NOTICE IS HEREBY GIVEN that a Regular Meeting of the Governing Board of the Texas School for the Deaf shall be held on **December 13, 2019 at 9:00 AM,** Texas School for the Deaf, Multipurpose Room of the Ford/CTE Bldg 1102 South Congress Ave Austin, Tx 78704.

If, during the course of the meeting, discussion of any item on the agenda should be held in closed meeting, the Board will conduct a closed meeting in accordance with the Texas Open Meetings Act, Texas Government Code, Chapter 551, Subchapters D and E or Texas Government Code section 418.183(f). Before any closed meeting is convened, the presiding officer will publicly identify the section or sections of the Act authorizing the closed meeting. All final votes, actions, or decisions shall be taken in open session.

The subjects to be discussed or considered, or upon which any formal action may be taken, are as follows (items do not have to be taken in the same order as shown on this meeting notice):

AGENDA

Item	**Call Roll of Board Members**
Information	Eric Hogue, President Shawn Saladin, Vice President Angie Wolf, Interim Secretary Sha Cowan David Saunders Christopher Moreland Keith Sibley Heather Withrow Dina Moore
Contact	Lindsey Kang
Action	Information only

Item	**Pledge of Allegiance**
Information	The Junior NAD students will lead the Pledge of Allegiance. "I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one Nation under God, indivisible, with liberty and justice for all."
Contact	Eric Hogue
Action	Information Only

Item	**Provide opportunity for public comment and introduction of visitors**
Information	The Open Meetings Act requires TSD to allow citizens (including parents of TSD students and TSD employees) to address the Board during Board meetings under procedures established by the Board. The Board may not deliberate or act on the item the citizen is addressing unless the item is on the agenda. If a citizen addresses an item that is not on the agenda, the Board President will acknowledge the citizen's comments. The item may be placed on an agenda of a future meeting or it may be deferred to the Superintendent to follow-up. Time allotted for speakers determined by the Board President at the meeting. Generally, it is 3 – 5 minutes per person.
Contact	Eric Hogue
Action	Information Only

Item	**Recognitions**
Information	The Board would like to recognize individuals who have made a significant contribution to TSD since the last Board meeting.
Contact	Claire Bugen and Eric Hogue
Action	Information Only

Item **Consent Agenda**

Information All matters listed under the Consent Agenda are considered to be routine by the Governing Board and will be enacted by one motion. There will not be separate discussion of these items. If discussion is desired, that item will be removed by a board member from the Consent Agenda and will be considered separately.

a. **Board Meeting Minutes of October 18th 2019** (Eric Hogue)
b. **Gifts and Donations** (Justin Wedel)
c. **Operating Budget FY20** (Justin Wedel)
d. **Operations Report** (Claire Bugen, Beth Polo)
e. **Appointment of SHAC Members (**Elizabeth Sterling**)**

Contact Eric Hogue

Action Approval

Governing Board Meeting
Meeting Minutes
October 18, 2019

Presiding Officer President Eric Hogue

A Governing Board Meeting of the Texas School for the Deaf was held at the Texas School for the Deaf campus, in Austin Texas October 18, 2019.

The Board found and determined that, in accordance with the policies and Order of this Board and with Chapter 551 (Open Meetings) of the Texas Government Code, as amended, the notice of the meeting has been properly complied with, including the posting of notice as to time, date, place of the meeting, and the subjects to be discussed at said meeting.

Call to Order
President Eric Hogue called the meeting to order at 10:45 am October 18, 2019. Board members attending are: Vice President Shawn Saladin, Sha Cowan, Keith Sibley and Heather Withrow. Other attendees: Claire Bugen, Julie Dodd, Stella Egbert, Mari Liles, Bobbie Beth Scoggins, Leonard Schwartz, Justin Wedel.

Pledge of Allegiance

The ASL students lead the Board and audience in the Pledge of Allegiance.

Public Comment
A request for visitors or public comment was made. Jon and Shelly Bergeron requested to discuss the new applied programs that is replacing the special needs program.

Jon spoke for he and Shelly. He thanked the Board for protecting deaf education and creating a protective and unique environment for deaf students. He stated that he and his wife love Texas School for the Deaf and have championed with legislation many years in support of the school. He let the Board know he is there with a heavy heart because of the new applied programs. He and his family have experienced a few issues with the new program. He is concerned and upset that there was no parental involvement in the implementation of this new program, nor any involvement or information during the roll out of the program. He and other parents did not know anything about the new program until late July. Even then there was not a lot of information given to them. All they knew, was their special needs student(s) were to be mainstreamed. They had no idea what kind of issues would arise from this drastic change. Nor did they know what kind of issues had been considered by the staff that decided to make this change without parental involvement. So, they were confused, and frustrated, they understood their special needs son would have an individual educational plan but were very worried at the thought he would be mainstreamed in with the regular students.

He feels this program has already put his son and other special needs students in danger. One example; his son was left alone with a pass to go to another area on campus. His son is not independent and needs help navigating the campus. Luckily his wife, Shelly, works at TSD and was close by. She explained the situation to the person giving her son the pass and was able to help him get to the area he needed to be. He said his son is very easily talked into doing things and he, as a parent, is uncomfortable with the lack of supervision in the new program. He also gave another issue where his son was sent to the bus all by himself. Because of his child's issues; it is so unsafe for him to be alone. He can be manipulated or hurt by not having the supervision he needs. Being a parent of a special needs child changes your life. You realize that the world is unsafe for your child and Jon said he was here to advocate for his son and other kids in the future. He said he and his wife are concerned that the special needs students are not getting the help and attention they had when there was a special staff that served these kids. He informed the Board of an eighteen-page document that addressed many issues the special needs children may have with this change in programs, which he says has been ignored. Mr. Bergeron requested the Board have some oversight for this new mainstreaming program of special needs children.

President Eric Hogue stated that he cannot go into great detail due to this specific issue is not on the agenda. He did let Mr. Bergeron know that there are areas the Texas School for the Deaf staff are being directed to look into to help with this transition. He let Mr. Bergeron know that there was a forum a few weeks ago and only four parents showed up to express their concerns about the new program.

Mr. Bergeron stated the forum was not well planned out and he understands about the poor parental involvement. He stated that he feels there is a process issue with dissolving the special needs department, and once again requests the Board and other staff look into the issues and the danger that special needs students are in.

Recognitions

The following people were recognized for their outstanding work and contributions at the Texas School for the Deaf:

Retiring Texas School for the Deaf Attorney, Leonard Schwartz

ASL Expressions: Lisa Cochran, Mary Ellen Graham, Linda Miller, and Sonia Bridges

Last Minute NRE /DRE working the weekend of Houston flooding: Student Life Staff

ASL Teachers for Deaf Awareness Week: Denise Egbert, Mark Holcomb, Ursa Rewolinski

Exiting Board Member: Ryan Hutchison

Consent Agenda Items

All matters listed under the Consent Agenda are considered to be routine by the Governing Board and will be enacted by one motion. There will not be separate discussion of these items. If discussion is desired, that item will be removed by a board member from the Consent Agenda and will be considered separately.

a. Board Meeting Minutes of April 12th 2019
b. Gifts and Donations
c. Operations Report
d. FY19 Operating Budget
e. 2019-20 Term and Probationary Contracts

The above Consent Agenda items were motioned by Sha Cowan to be accepted as is. Vice President Shawn Saladin seconded the motion. All were in favor of accepting the consent agenda items as is. Motion carries unanimously.

TFC Deferred Maintenance GMP 5.1 Update

The McKinney / York team along with Daniel Yen of Texas Facilities Commission updated the Board on the deferred maintenance plan.

Approval of Internal Audit Contract

Chief Financial Officer Justin Wedel informed the Board that Garza Gonzales were selected through the State of Texas bidding process to be contracted as the Board's Internal Auditors.

Vice President Shawn Saladin motioned to Garza / Gonzalez as the Board's Internal Auditors. Sha Cowan seconded the motion. All were in favor of accepting Garza / Gonzalez as the Board's Internal Auditors. Motion carries unanimously.

Policies Review and Approval

Sha Cowan requested Board approval for the following policies.

Motion as is:
FNCC Student Conduct Prohibited Organizations and Hazing
GKA Community Use of School Facilities Conduct on School Premises

Motion with minor changes:
DBAA Employment Requirements and Restrictions: Criminal History and Credit Reports
DC Employment Practices
DECB Leaves and Absences - Military Leave
FNAA Student Expression Distribution of Non-School Literature
FO Student Discipline

FOB Student Discipline Out of School Suspension
FOA Placement in Disciplinary Alternative Setting Removal by Teacher
DFBA Term Contracts: Suspension/Termination During Contracts
DFBB Term Contracts: Nonrenewal
GKC Visitors to the School

Motion to strike the original language and substitute with new language as is:
FNCE Student Conduct Telecommunication Devices

Motion to strike the original language and substitute with new language with minor changes:
FNCA Dress Code

All were in favor. Motion carries unanimously.

Recess
President Eric Hogue recessed for lunch at 11:38 am

Open Session
President Eric Hogue called the meeting back to order at 12:32 pm.

Superintendent's Report
Superintendent Claire Bugen informed the Board that enrollment status is 556 students with 223 being residential students. Other information she went over with the Board was Deaf Awareness Week which was a big success. Recent and future superintendent travel, Homecoming, 2019 smarter football grant, collaboration with Texas Workforce Commission on Robotics, Annual Report, the re-opening of TSD libraries, the parental forum on the new applied programs, and TSD townhall meetings.

CEASD Accreditation and Strategic Planning
Superintendent Claire Bugen informed the Board about the new accreditation and strategic plan. She reminded them that this is renewed every five years. There will be a school planning team on January 24 and 25, 2020 to work on plan development. Once the top priorities are decided the strategic goal teams will research each area identified, and then bring their ideas to the Board for approval.

Update on New Legislation
Superintendent Claire Bugen and ERCOD Director Bobbie Beth Scoggins went over the new legislation passed for the Deaf and Hard of Hearing. They explained HB 548 pertaining to language acquisition, HB 2255 on infant screening, and SB 281 for deaf and hard of hearing terminology.

SGT 2 Update: Academic and Personal Achievement
Director of Instruction Stella Egbert gave the Board an update on SG2 Academic and Personal Achievement.

Continuum of Services Update

Superintendent Claire Bugen and Director of Instruction Stella Egbert gave an update on continuum of services. They went over the issues and concerns the parents have shared about dissolving the special needs program and starting the applied programs. They said many people are optimistic about the change in mainstreaming the special needs students, including many of the special needs students themselves. One female student told Superintendent Bugen she was so excited because she was now part of the Texas School for the Deaf. The students now have a variety of classroom options that they didn't have before. They are included in so much more things with their other fellow Texas School for the Deaf students. Superintendent Bugen said they had more work to do, especially with parents. They need to help them see the benefits of the new program. She said that staff are meeting about things they have learned they are planning to make the new program even stronger by fixing the issues they find. She stated that they have been, and are addressing the issues of students who need the extra supervision like, parent Jon Bergeron, brought up in public comments earlier.

Adjournment

President Eric Hogue reminded the Board the next meeting will be December 12 and 13, 2019. He asked the members to remember it was important to have all eight members attend the meeting. He then adjourned The Texas School for the Deaf Governing Board meeting at 1:27 pm.

_____

Eric Hogue, President

_____

Angie Wolf, Secretary

Item **Gifts and Donations**

Information

Education Code §30.052 (I), states that the Board may accept and retain control of gifts, devises, bequests, donations, or grants, either absolutely or in trust, of money, securities, personal property, and real property from any individual, estate, group, association, or corporation. The funds or other property donated or the income from the property may be spent by the board for: (1) any purpose designated by the donor that is in keeping with the lawful purpose of the school; or (2) any legal purpose, if a specific purpose is not designated by the donor.

Additionally, Government Code §575.001-575.003 states that a state agency with a Governing Board may accept a gift of $500 or more only if a majority of the Board, in an open meeting, approves accepting the gift.

Donations received (October 4, 2019 – December 3, 2019) that require Board acceptance:

Date	Donor	Amount	Designated Purpose
10/9/19	NW Sertoma Club – Austin	$ 3,200.00	Earmolds / Audiology Supplies
10/28/19	Holloway Houston	$ 500.00	Christmas Party and Dinner Event
Total:		$ 3,700.00	

Contact Justin Wedel

Action Approval

Item	**FY20 Operating Budget**
Information	As of December 4, 2019 roughly 25% of the fiscal year has elapsed. To date, the School has executed 25% of its present budget allocation for FY20 activities. At the present time, adequate cash flow exists to cover expenses through the end of the fiscal year to end on August 31, 2020.
Information Contact	Justin Wedel
Action	Information Only

FY 2020
Balances by Org as of 12/04/2019

Strategy	Division Director	Org Code	Department Name	FY 2020 Budget	Amount Expended as of 12/04/2019	Balance	Percentage Expended
Technical Assistance	Bobbie Beth Scoggins	121	ERCOD	934,720	231,521	703,199	24.77%
Statewide Outreach	Bobbie Beth Scoggins	123	Discovery Retreat	60,000	4,052	55,948	6.75%
Statewide Outreach	Bobbie Beth Scoggins	124	PIP	400,792	107,641	293,151	26.86%
Technical Assistance	Bobbie Beth Scoggins	132	Distance Learning	75,178	22,651	52,527	30.13%
Statewide Outreach	Bobbie Beth Scoggins	790	Summer School GAA Summer Program	700,925	17,853	683,072	2.55%
Statewide Outreach	Bobbie Beth Scoggins	792	Family Weekend Retreat (FWR) GAA Summer Program	21,500	-	21,500	0.00%
Statewide Outreach	Bobbie Beth Scoggins	793	Communication Skills Workshop (CSW)	249,550	-	249,550	0.00%
Statewide Outreach	Bobbie Beth Scoggins	797	Outreach College Prep (TWC)	-	-	-	
Statewide Outreach	Bobbie Beth Scoggins	798	Outreach MS STEM (TWC)	-	-	-	
Technical Assistance	Bobbie Beth Scoggins	830	Deaf TEC Grant	72,247	13,492	58,755	18.68%
Technical Assistance	Bobbie Beth Scoggins	7941	Region XI Guide By Your Side	40,000	9,359	30,641	23.40%
Technical Assistance	Bobbie Beth Scoggins	7942	Region XI Special Projects	27,000	2,651	24,349	9.82%
Technical Assistance	Bobbie Beth Scoggins	7643	Region XI Online Resources	67,000	512	66,488	0.76%
Technical Assistance	Bobbie Beth Scoggins	7945	Mental Health Webinar Series	45,000	947	44,053	2.10%
Technical Assistance	Bobbie Beth Scoggins	8151	Parent Support	102,885	21,268	81,617	20.67%
Technical Assistance	Bobbie Beth Scoggins	8152	Guide By Your Side	131,115	28,145	102,970	21.47%
Technical Assistance	Bobbie Beth Scoggins	8153	Family Training and Support	18,000	-	18,000	0.00%
Technical Assistance	Bobbie Beth Scoggins	8154	Resources for Spanish Speaking Families	25,000	2,725	22,275	10.90%
Technical Assistance	Bobbie Beth Scoggins	8155	Resource Website	20,000	3,000	17,000	15.00%
Technical Assistance	Bobbie Beth Scoggins	8156	Family Signs	55,000	15,207	39,793	27.65%
Technical Assistance	Bobbie Beth Scoggins	8157	Parent Training on Transition	21,000	1,120	19,880	5.33%
Technical Assistance	Bobbie Beth Scoggins	8158	K-12 Mental Health Initiative	15,000	1,100	13,900	7.33%
				$ 3,081,912	**$ 483,244**	**$ 2,598,668**	**15.68%**
Central Administration	Claire Bugen	111	Superintendent's Office	570,703	154,198	416,505	27.02%
Central Administration	Claire Bugen	112	Governing Board	64,100	4,404	59,696	6.87%
Instruction/Residential	Mari Liles	131	Information Technology Services	752,630	193,630	559,000	25.73%
Classroom Instruction	Mari Liles	133	Software Maintenance Fees	117,000	9,931	107,069	8.49%
Classroom Instruction	Mari Liles	862	Title IV, Part A	10,000	300	9,700	3.00%
Classroom Instruction	Mari Liles	8261	Technology Services (Interagency Contract)	208,000	14,325	193,676	6.89%
Central Administration	Julie Dodd	141	Human Resources	606,956	163,768	443,188	26.98%
Other Support Services	Julie Dodd	142	Sign Language	112,833	32,576	80,257	28.87%
				$ 2,442,222	**$ 573,131**	**$ 1,869,091**	**23.47%**
Classroom Instruction	Stella Egbert	510	Director of Instruction	643,871	144,766	499,105	22.48%
Classroom Instruction	Stella Egbert	511	Curriculum	117,507	31,516	85,991	26.82%
Classroom Instruction	Stella Egbert	521	Elementary/ECE	2,617,093	757,332	1,859,761	28.94%
Related and Support Services	Stella Egbert	522	Elementary/ECE Support	619,514	170,560	448,954	27.53%
Classroom Instruction	Stella Egbert	541	Physical Education	399,535	121,362	278,173	30.38%
Classroom Instruction	Stella Egbert	542	Aquatics	53,961	14,676	39,285	27.20%
Classroom Instruction	Stella Egbert	561	High School	2,435,149	654,523	1,780,626	26.88%
Related and Support Services	Stella Egbert	562	High School/CTE Support	694,375	192,561	501,814	27.73%
Career and Transition	Stella Egbert	570	Ranger Press	100,440	16,310	84,130	16.24%
Career and Transition	Stella Egbert	571	Career Technology Education	1,265,720	330,859	934,861	26.14%
Career and Transition	Stella Egbert	572	ACCESS	1,049,056	251,702	797,354	23.99%
Career and Transition	Stella Egbert	573	ACC Dual Credit	25,000	11,368	13,632	45.47%
Classroom Instruction	Stella Egbert	581	Middle School	1,405,801	372,546	1,033,255	26.50%
Related and Support Services	Stella Egbert	582	Middle School Support	396,624	84,720	311,904	21.36%
Career and Transition	Stella Egbert	796	Outreach Acess 18+ (TWC)	-	-	-	0.00%

FY 2020
Balances by Org as of 12/04/2019

Strategy	Division Director	Org Code	Department Name	FY 2020 Budget	Amount Expended as of 12/04/2019	Balance	Percentage Expended
Classroom Instruction	Stella Egbert	821	IDEA-B Formula	276,610	73,097	203,513	26.43%
Career and Transition	Stella Egbert	824	Perkins Grant	23,933	491	23,442	2.05%
Classroom Instruction	Stella Egbert	841	IDEA-B Preschool	16,672	2,511	14,161	15.06%
Classroom Instruction	Stella Egbert	860	Title I, Part A	80,379	15,706	64,673	19.54%
Classroom Instruction	Stella Egbert	861	Title II, Part A	9,744	4,291	5,453	44.04%
Classroom Instruction	Stella Egbert	8263	DOI/Curriculum (Interagency Contract)	156,179	34,301	121,878	21.96%
Classroom Instruction	Stella Egbert	8264	Elementary/ECE (Interagency Contract)	27,500	3,299	24,201	12.00%
Classroom Instruction	Stella Egbert	8266	Physical Education/Aquatics (Interagency Contract)	8,000	137	7,863	1.71%
Classroom Instruction	Stella Egbert	8267	High School (Interagency Contract)	24,500	9,908	14,592	40.44%
Classroom Instruction	Stella Egbert	8268	Middle School (Interagency Contract)	13,500	2,314	11,186	17.14%
				$12,460,663	**$ 3,300,855**	**$ 9,159,808**	**26.49%**
Central Administration	Justin Wedel	211	Business Administration	391,558	95,894	295,664	24.49%
Other Support Services	Justin Wedel	213	Mailroom	23,000	10,883	12,117	47.32%
Central Administration	Justin Wedel	231	Accounting	326,126	87,388	238,738	26.80%
Other Support Services	Justin Wedel	241	Purchasing	156,381	38,151	118,230	24.40%
Other Support Services	Justin Wedel	245	Copy Machines	85,000	4,325	80,675	5.09%
Other Support Services	Justin Wedel	262	Workers Comp/Unemployment	110,000	81,997	28,003	74.54%
Other Support Services	Justin Wedel	281	Utilities	930,000	201,467	728,533	21.66%
Other Support Services	Justin Wedel	282	Cell Phones	70,000	11,083	58,917	15.83%
Other Support Services	Justin Wedel	299	Facilities AR	140,000	3,033	136,967	2.17%
Transportation	Justin Wedel	462	Transportation	941,558	270,915	670,643	28.77%
Related and Support Services	Justin Wedel	468	Food Services	1,012,408	308,875	703,533	30.51%
Other Support Services	Justin Wedel	491	Security	476,417	121,951	354,466	25.60%
Transportation	Justin Wedel	5904	Transportation Items - Capital	145,000	-	145,000	-
				$ 4,807,448	**$ 1,235,962**	**$ 3,571,486**	**25.71%**
Related and Support Services	Wilmonda McDevitt	411	Auditorium	15,000	214	14,786	1.43%
Transportation	Wilmonda McDevitt	463	Homegoing Expenses	1,463,376	248,545	1,214,831	16.98%
Residential Services	Wilmonda McDevitt	471	Athletics	437,728	119,191	318,537	27.23%
Residential Services	Wilmonda McDevitt	473	Coaching Stipends	96,425	7,776	88,649	8.06%
Residential Services	Wilmonda McDevitt	610	Director of Student Llife	172,023	35,633	136,390	20.71%
Residential Services	Wilmonda McDevitt	612	Residential Supervisors	445,301	121,401	323,900	27.26%
Residential Services	Wilmonda McDevitt	621	Residential Student Development	478,630	141,318	337,312	29.53%
Residential Services	Wilmonda McDevitt	641	Residential Services Staff	2,368,116	732,391	1,635,725	30.93%
Classroom Instruction	Wilmonda McDevitt	8269	Extracurricular Stipends (Interagency Contract)	20,000	-	20,000	0.00%
				$ 5,496,599	**$ 1,406,469**	**$ 4,090,130**	**25.59%**
Related and Support Services	Elizabeth Sterling	410	Student Support Services	1,487,622	431,385	1,056,237	29.00%
Related and Support Services	Elizabeth Sterling	416	Hearing Aids/Earmolds	12,500	505	11,995	4.04%
Related and Support Services	Elizabeth Sterling	417	Family Services	291,541	80,527	211,014	27.62%
Related and Support Services	Elizabeth Sterling	434	Interpreting Services	741,424	224,839	516,585	30.33%
Related and Support Services	Elizabeth Sterling	451	Health Services	775,366	233,566	541,800	30.12%
Classroom Instruction	Elizabeth Sterling	791	Extended Year Services (EYS) GAA Summer Program	73,300	-	73,300	0.00%
Related and Support Services	Elizabeth Sterling	795	State Supplemental (Visually Impaired)	5,397	290	5,107	5.38%
				$ 3,387,150	**$ 971,113**	**$ 2,416,037**	**28.67%**
			Grand Totals	**$31,675,994**	**$ 7,970,775**	**$23,705,219**	**25.16%**

Item **Operations Report**

Information We continue to be actively involved in Deferred Maintenance on the campus. We are nearing completion of the projects which were identified under GMP 4, and are beginning the initial projects assigned to GMP 5.

The GMP 4 Projects nearing completion include:

Clinger Gymnasium- repair work to an outside set of stairs, ramp, and handrails

R. L. Davis Auditorium- almost at completion with work remaining on the addition of stairs leading to Stage Left from backstage.

Koen Hall and Lewis Hall- the source of the roof leaks has been identified and this project will be completed under GMP 4

Elementary Playground- ADA hand railings have been ordered and will be installed upon arrival

The GMP 5 Projects:

The initial work on the GMP 5 Projects has begun and will continue for approximately the next 18 months. Projects currently underway include:

Football stadium- new LED stadium lights and power to time clocks

Sump pumps- installation of pumps in 37 communication manholes across campus to keep water from collecting in the lines

Cottage 570- demolition on interior and exterior including ADA upgrades, exterior water proofing, new windows, and interior improvements to serve as the new home for Human Resources

Information Contact Claire Bugen, Beth Polo

Action Information Only

Item **Appointment of SHAC Members**

Information A SHAC (School Health Advisory Committee) is a school board appointed advisory group of individuals who represent different segments of the community. By law, a majority of the members must be persons who are parents of students enrolled in the district and who are not employed by the district. The TSD SHAC is made up of parents, community members, students, and school staff working together to improve the health of all students and families though coordinated school health programs.

A minimum of five members must be appointed to serve on the SHAC by the Board of Trustees. We recommend that the Board appoint the following individuals:

Malibu Barron
Bobbie Jo Cardenas
Deborah Davison
Crystal Kelley Schwartz
Mallory Malzkuhn

Contact Elizabeth Sterling

Action Request for Approval

Item **Superintendent's Report**

Information At each Board Meeting the Superintendent prepares a high-level summary of what has transpired since her last communication with the Board. The Superintendent will respond to any questions and/or elaborate on any issues at the Board meeting.

Contact Claire Bugen

Action Information Only

TEXAS SCHOOL FOR THE DEAF

LEARN. GROW. BELONG.

DATE: DECEMBER 13, 2019

TO: GOVERNING BOARD

FROM: CLAIRE BUGEN

RE: FOR YOUR INFORMATION

A. Enrollment Update. The enrollment as of 11/27/19 is 568 (231 of these are residential students). Last year at this time enrollment was 542. Enrollment grid is attached.

B. Student Holiday Events. It's that time of year again when we plan holiday events for the students. A schedule of the student holiday events is attached. Special thanks is due to Lindsey for coordinating this complicated schedule.

C. Board Scholarship Fund Update. Both 2019 recipients have received their $500 scholarships. After the $126 profit from Homecoming Booth water sales the scholarship fund has a balance $442.58. If you elect to give two $500 scholarships to the Class of 2020, we'll need some monetary donations from the Board.

D. Superintendent Travel. I have been quite busy since the last Board meeting. October 27th-30th I was in Kentucky for the joint conferences of the Council of Administrators of Special Education (CASE) and National Association of State Directors of Special Education (NASDSE), and the Fall CEASD Board meeting. November 3rd-6th I chaired the Pennsylvania School for the Deaf accreditation team in Philadelphia, and December 2nd-4th both Chris Hamilton and I attended the National Deaf High School Athletics Summit at CSD-Riverside with 4 other schools (Maryland SD, CSD-Fremont, Indiana SD, Model Secondary SD). I happy to not have to travel again until February.

E. Lamar University. Enrollment for the master's program partnership with Lamar University will begin in the Fall of 2020. As you may recall this plan is to address the shortage of teaching professionals entering into special education/Deaf education. TSD will become an additional program site to provide classroom space and student housing for Lamar's Deaf education degree candidates. Press Release is attached and we have a short video of news coverage to share. Link

F. Master Plan Update. Phase I of the TSD Master Plan provides for a Central Administration/Welcome Center and Early Learning Center. Plans are at 100% completion and we have entered the bidding phase with groundbreaking occurring in early 2020.

The new Central Services building will feature an open Deaf Space design lobby, which will serve as the Welcome Center and as a space for campus social functions. The building will house the Central Administration offices, Governing Board suite, the Business Services division, as well as having multiple flex space conference rooms that can be configured to accommodate large or small gatherings.

The Early Learning Center will support our PIP and ECE students ages 2 – 5. The classrooms are arranged in pairs separated by see-through pocket doors which enable the space to be used as a large team-teaching space, or separated into more individualized learning groups. The play area will feature spaces that are appropriate for 2 – 3 year-olds and 4 – 5 year-olds, as well as incorporating elements of nature play.

Phase II of the Master Plan was recently funded by the 86th Legislative Session and includes funding for campus security and traffic circulation as well as a new Culinary Arts expansion. We will be adding card readers to buildings and pedestrian gates, adding traffic arms to the Congress Avenue entrance and relocating the security booth to a center island, and modifying classroom door locks. The Culinary Arts expansion will allow for upgrades to state-of-the-art commercial kitchen equipment and a larger classroom space to meet the needs of our ever expanding and exceedingly talented Culinary Arts students and department.

G. Pancake Breakfast. The 16th Annual All-You-Can-Eat Pancake Breakfast is scheduled for Saturday, February 1st from 7:30am – 1:00pm. We would love for you to attend if you are in Austin. Proceeds from this benefit TSD student projects.

H. NRSC National VEX-IQ Robotics Competition.

Middle School Robotics: TSD is partnering up with NTID Regional STEM Center (NRSC) to host nationwide VEX IQ robotics competition on TSD campus for 15+ deaf schools with approximately 40 teams this coming February 6-9, 2020.

Middle School 8th Graders - a total of 8 teams, but only four teams will compete in local competitions and travel to Alabama Institute for Deaf and Blind in late February.

Middle School 7th Graders - a total of 3 teams and all will compete in local competition and participate with the NRSC's VEX IQ competition on TSD campus.

Total of 20-24 middle school students (roster is not finalized yet) with 7 teams. VEX Robotics teams have lower student per team ratio.

High School Robotics: Twenty students are participating on the Blue Chargerbots team this year. This year, the (For Inspiration and Recognition in Science and Technology) FIRST Tech Challenge (FTC) competitions are focused on the Star Wars theme, and the name of the competition is Skystone for our FTC team. We are in the Austin Metro League division, which is considered the toughest division in Texas, if not nationwide (think Westlake, Vandegrift, LASA, and so on). We recently had our first qualifying competition in November and will have three more weekend competitions before the Championship competition.

Below are a few pictures to help understand the difference between three robotics competitions. It's helpful to see the robotics and the level of competition.

FTC Team - you create and customize nearly every part, via lathe, milling, 3D-print etc. - less limitations.

VEX EDR - has many metal/aluminum parts and more limitations on being able to use parts outside of the VEX bundle kits.

VEX IQ - mainly uses plastic and Lego-based parts.

I. **Betty Bounds' Memorial.** Former TSD assistant superintendent Betty Bounds passed away November 6, 2019. Starting out as a middle school teacher, then curriculum coordinator, Betty worked at TSD from 1994 to 2008. Her husband, Larry Evans, is having a memorial/celebration of life service at TSD on January 18th in the Deaf Smith Center. A draft of the program is attached.

J. City of Austin Employee of the Year Award. On Friday, November 8th I was awarded the 2019 Employee of the Year from the Mayor's Committee for People with Disabilities. TSD residential staff Taurean Burt is one of the Mayor's committee members. Photo attached.

K. EPA MOU. After several months of planning TSD and the Environmental Protection Agency (EPA) had a signing ceremony on November 5th regarding a collaboration on environmental education activities. Elementary students can become members of the Planet Protectors Club and learn how to reduce, reuse, and recycle. Middle School and High School students can participate in Environmental Education and consider service projects to help our community "go green." High School students can consider internships or making a career of protecting the environment with the EPA. A group of students were on hand for the signing ceremony. A copy of the MOU is attached.

TEXAS SCHOOL FOR THE DEAF ENROLLMENT

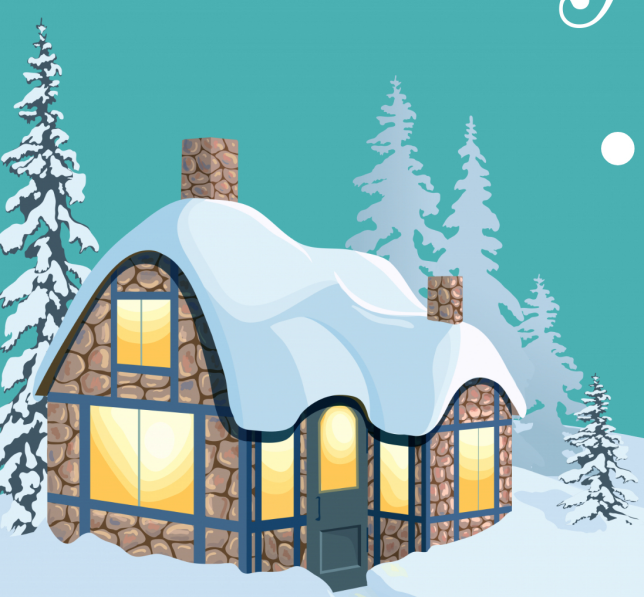
REGULAR SCHOOL YEAR PROGRAMS	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019
Parent Infant Program	18	19	18	28	20	23	21	22
Pre-Kindergarten	10	19	19	11	9	18	18	11
Pre-School	12	22	18	19	25	22	26	30
K-5 Elementary	98	94	104	120	115	110	118	124
Special Needs	81	59	64	61	54	57	72	75
Middle School	106	104	98	82	94	96	101	84
High School	173	178	208	197	201	192	201	185
ACCESS	28	55	52	66	65	44	44	40
TOTAL	**526**	**550**	**581**	**584**	**583**	**562**	**601**	**571**
Residential Enrollment	**241**	**242**	**274**	**262**	**248**	**214**	**247**	**226**

SUMMER PROGRAMS	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017 - 2018	2018-2019
Extended Year Services Program	52	40	30	32	30	16	29	62
Summer Camps and Programs	248	203	66	122	126		67	69
Summer Camps and Programs Non-TSD	99	110	101	109	135		53	82
Early Childhood Education	16	23	17	14	14		16	9
Parent Infant Program	2	3	12	13	15	10	14	15
Accelerated Instruction						17	7	27
Other Short-Term Programs	145	179	233	159	146	162	180	248
TOTAL	**461**	**445**	**459**	**449**	**436**	**205**	**366**	**512**

TOTAL SERVED	1086	995	1040	1033	1019	767	967	1083

Texas School for the Deaf

Annual Holiday Celebrations



12/17: Elementary to Epic Fun
12/18: Middle School to EVO
12/19: PIP & ECE to Catch Air
12/20: ACCESS to Main Event
12/20: High School to Austin's Park & Pizza

*Lunch and Transportation Provided

If you would like your child to opt out of the celebration please contact your child's teacher.

For more information call 512.462.5303 or email lindsey.kang@tsd.state.tx.us

TSD & EPA MOU SIGNING

Texas School for the Deaf 2019


TEXAS
BASKETBALL

The students were so excited that they made a video!

TEXAS SCHOOL FOR THE DEAF PRESS RELEASE

Contact: Gabriel Cardenas
Phone: 512-462-5372
Email: Gabriel.Cardenas@tsd.state.tx.us

FOR IMMEDIATE RELEASE

LAMAR UNIVERSITY PARTNERS WITH TEXAS SCHOOL FOR THE DEAF TO ADDRESS SHORTAGE OF TEACHERS ENTERING SPECIAL EDUCATION

November 15, 2019 - Austin, Texas – Lamar University will expand its' Master of Sciences (M.S.) degree program(s) in Deaf Education and Deaf Studies through a partnership with the Texas School for the Deaf (TSD) in an effort to address a shortage in the number of teaching professionals entering into Deaf Education.

Recently agreed to by the Southern Association of Colleges and Schools Commission on Colleges, TSD will become an additional program site to provide classroom space, Wi-Fi and student housing for Lamar's Deaf Education degree candidates who may reside outside of the Austin area.

Currently, classes for Lamar University's Deaf Studies and Deaf Education (DSDE) students are only offered on weekends at the main campus in Beaumont, Texas.

Plans for the TSD site to be up and running will start for university students enrolling in classes for the Fall 2020 semester.

TSD Superintendent, Claire Bugen, welcomed the news and affirmed the unique partnership as an innovative way to help address the shortage of highly qualified deaf education teachers.

"This announcement could not have come at a better time, Bugen says. We look forward to sharing this news with our statewide partners in Deaf Education as well as schools for the deaf across the nation.

"Our Texas Lieutenant Governor recently asked the Senate Education Committee to look at ways to recruit, prepare and retain highly effective teachers.

"This partnership with Lamar University is a perfect example of collaboration by two educational institutions to find innovative solutions and maintain an adequate pipeline of qualified educators ready for our future generations."

DSDE chair, M. Diane Clark, believes that offering the program on the TSD campus will permit potential students who were unable to attend the program on the Lamar campus, due to family constraints, to earn their Masters and obtain teacher certification. As noted by the TSD superintendent, Claire Bugen, we have to creatively develop programs to increase the number of Deaf Education teachers.

Lamar and TSD began working on this partnership two years ago. Clark commented that the two are perfect partners as both as both "support a bilingual educational philosophy; access to both ASL and English to support academic as well as social emotional development where Deaf children can thrive."

##

ABOUT THE TEXAS SCHOOL FOR THE DEAF: The Texas School for the Deaf (TSD) is the oldest continuous operating public school in Texas. Educating deaf and hard of hearing students of Texas since 1856, the campus also provides outreach and educational resources for students, their families and professionals in the field throughout the state of Texas. With educational excellence and a strong belief in a culture and community at TSD, students form a unique identity based on their individual strengths and talents. TSD is an environment where students learn, grow, and belong. For more information about the Texas School for the Deaf, visit www.tsd.state.tx.us.

ABOUT THE DEPARTMENT OF DEAF STUDIES AND DEAF EDUCATION AT LAMAR UNIVERSITY: The department of Deaf Studies and Deaf Education (DSDE) cultivates and inspires students with research base innovative learning opportunities to become scholars, service providers, and allies who revolutionize the field of ASL/English bilingual Deaf education, ASL, and Deaf Studies. DSDE also promotes effective communication that allows partnerships and collaboration within a diverse community, including deaf and hearing populations. Lamar University is a member of the Texas State University System, and is nationally recognized as a Carnegie Doctoral Research University. It is rated as one of the best educational values in the state of Texas, and in North America, based on its average cost to students. For more, please visit: https://www.lamar.edu/fine-arts-communication/deaf-studies-deaf-education/index.html.

Contact information:
Contact Name: Gabriel Cardenas
Contact email: gabriel.cardenas@tsd.state.tx.us
Phone: (512) 462-5372
Website: www.tsd.state.tx.us

TEXAS SCHOOL FOR THE DEAF

presents:

PANCAKE BREAKFAST

Est. 2004

SUNDAY February 1st

7:30 am - 1:00 pm

All You Can Eat!

Includes:
pancakes
scrambled eggs
bacon
coffee & OJ

#SHARETHEWILL

LIVE MUSIC @10

featuring

Gary Knippa & Friends

ROUND ROCK BALLET FOLKLORIO @ 11

Performance

Austin Roasting Company
AUSTIN · TEXAS

Tickets:
$7 each or
4 for $25

In loving memory of

BETTY BOUNDS-EVANS

March 5th, 1942 - November 6th, 2019

Celebration of Life
held at the
Texas School for the Deaf
Deaf Smith Student Center

1:00 PM // January 18th, 2020

BETTY BOUNDS-EVANS

Introduction
Co-Hosts Claire Bugen (TSD Superintendent)
and Mark Seeger (former CSD/Sprint employee)
Opening Remarks by Selected Guests
Clips from the Silent Network
Selected Bugen & Bounds Show Videos
Open Mic for Visitors
Closing Remarks by Betty's Family
Gratitude
Closing song
Refreshments

We invite you to sign and share your thoughts in the memorial book in the back of the Deaf Smith Student Center (Kathryn Caldcleugh)

We also encourage you to donate to TSD Middle School in her memory at the TSD Foundation table or donate to:

https://tsdfoundation.org/how-you-can-help/#donate (Holly Hawk)

(Photo: Lily bouquet taken at the Sodalis Memory Care Community)

Mayor's Committee for People with Disabilities
Employee of the Year
Presented To:
Claire Bugen
NOVEMBER 08, 2019
Jonathan Franke, Chair

Item	**CEASD Accreditation and Strategic Planning**
Information	Our self-study for CEASD accreditation is in full swing. We have tons of data that we have collected, Standards Focus groups are meeting and we are preparing on internal and external analysis of current trends and influences. We will present you with an overview of the process and timeline.
Contact	Claire Bugen
Action	Information Only

2019-2020

TSD Strategic Planning

TIMELINE

2019-2020 TSD Strategic Planning and Accreditation Process

September – December 2019

INTERNAL/EXTERNAL ASSESSMENT

- Student Performance, Demographic Data
- Technology Impact, Economic Impact
- Political Landscape, Stakeholder Views
- Local, State, National Trends
- CEASD Standards Surveys
- Mission, Vision, and Beliefs Survey

February – March 2020

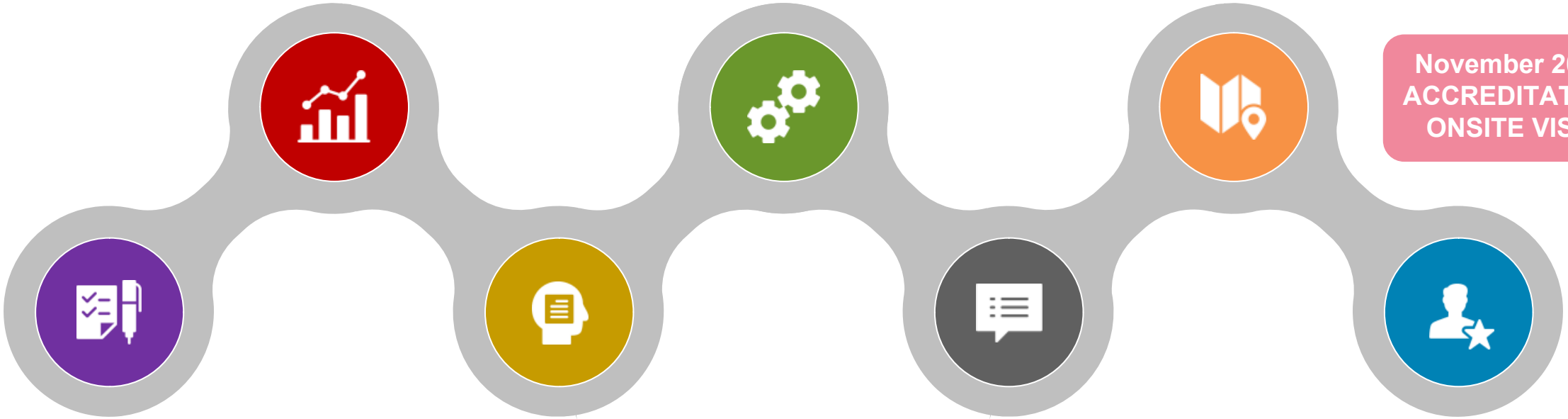
ESTABLISH STRATEGIC GOAL TEAMS (SGTs)

- Feb 6th – Training
- SGTs Meet and Conduct Research on Critical Issues

May – July 2020

FORMALIZE PLANS

- Five-Year Strategic Plan Developed
- District Improvement Plan (DIP) Development
- Begin Compiling CEASD Self Study



November 2020
ACCREDITATION ONSITE VISIT

June – September 2019

CONDUCT SURVEYS

- CAYCI Surveys
- UT Employee Engagement

January 24th and 25th, 2020

SCHOOL COMMUNITY PLANNING TEAM MEETING

- 25 Members
- Review Mission, Vision, Belief Statements
- Review Internal/External Assessment (Survey Data)
- Identify Critical Issues

April 2020

SGT REPORTS

- SGT Reports Due (April 17th)
- SGT Chairs present final report at CEASD Core Meeting
- SGT Reports/Critical Issues Approved by Board

August – October 2020

BOARD REVIEW & APPROVAL

- Board approves Strategic Plan
- Board approves DIP
- Self Study Assembly in Final Stages
- Preparation of Evidence for Exhibit Room
- Develop Schedule for Site Visit

Item **Update on Strategic Goal Teams**

Information

A. SGT 1 Update: Communication (Claire Bugen, Mari Liles)

Year 4 updates and highlights for SGT Goal #1 objectives.

B. SGT 4 Update: Data Driven Decision Making (Donna Altuna, Karl Hummel)

Year 4 updates and highlights for SGT Goal #4 objectives.

Contact Claire Bugen

Action Information Only

SGT #4 – Data Driven Decision Making

- **PowerSchool Accomplishments**
  - PowerSchool now central source for all contact information
  - PowerScheduler installed – will be fully implemented by 20-21
  - PowerSchool Registration – all Admission forms in PS will field test in January
  - PowerSchool Medical and Guardian Alerts – in place
  - Migration from Grade Book to Power Teacher Pro by Aug. 1, 2020
  - PowerSchool Substitute System – purchased and up and running in January 20
- **PowerSchool Pending**
  - Investigating Residential Barcoding/Scanning for bed checks
  - Forming sub committee to determine if a FTE needs to be allocated to PS needs
  - Investigating need/feasibility of sending 1-3 staff to PS University (Edge)
  - Forming sub committee to investigate how PowerSchool compares with eSped for our ARD needs

SGT #4 – Data Driven Decision Making

- **Archival System Needed**
  - Retention Schedule Draft complete, needs superintendent's approval
    - Pending approval – will post for Records Manager
  - Sub Committee selected Archival System: ImageNet
  - Sub Committee selected Scanning Company (old documents): Rainmaker
- **SHARS**
  - All new service providers trained – going well
- **SNAP**
  - Training complete and transition to use taking place
- **LMS**
  - Currently investigating Schoology and Canvas to meet our various campus needs
- **Incident Reports (IRs)**
  - Developing sub committee to investigate FERPA access and revisions of reporting form

SGT #1 - Communication
Year 4 – Update
Claire Bugen and Mari Liles

Communication Goal:

Implement an integrated approach to communication that represents progressive technologies, a knowledge and appreciation of our audiences and a respectful and transparent culture.

SGT 1: Communication - CB

Obj 1 - Engage and involve families in their children's education to create shared responsibilities for student success.

• Department principals are identifying training topics that are relevant to their families. CTE will provide a training on Medicaid waivers, guardianship & alternatives. Elementary is providing Family Story Time. Middle school sent a survey to their parents and is organizing an evening parent group.

• We received a mini grant to expand the number of teachers to provide online Parent Classes and were also able to expand the budget by 5K to serve additional families.

• Residential supervisors helped to identify strong parent reps by city, and stops were prioritized by those with the largest numbers of families. We will eventually hit all 6 buses; San Antonio, Spring, Mesquite, San Angelo, Sugarland, & Saginaw.

Obj 2 - Promote a culture of mutual respect, support, and responsibility to achieve shared goals.

• Malibu Barron was hired as the Equity, Diversity and Inclusion Coordinator. Dirk and Malibu are establishing a training schedule for this year.

SGT 1: Communication Cont. – ML

Obj 3 - Mobilize resources to advance our use of technology and social media to communicate with internal and external stakeholders and to advance our bilingual mission.

- Continue to engage with the public through Social Media. A new account as created for Student Life. We had a successful use of our Social Media Rangers during homecoming and spirit week.

- A NEW webpage design is in preliminary stages. We are compiling examples of good web designs to apply to TSD's Homepage. We are purging old content and doing new re-organization of content.

Obj 4 - Create a workplace culture of trust and transparency.

- PPfT orientation was provided for instructional staff. Two Town Hall meetings have been conducted on Emergency Drills and CEASD Accreditation & Five Year Planning. We will hold a Master Planning Town Hall in Jan/Feb, and another CEASD in the Spring

- Three Trust and Transparency trainings were provided to Supervisors in Student Life

SGT 1: Communication Cont. - CB

<u>Obj 5</u> - Prepare for the next 5 Year Plan and upcoming CEASD Accreditation.

- Data collection for CEASD Internal/External Analysis is 99% complete
- CEASD Standards survey results have been reviewed by Focus Groups
- Invitations to the School Community Planning Team (January 24th/25th) are being finalized
- Parent, Student, and Staff survey results have been submitted to the Community and Youth Collaborative Institute CAYCI for analysis
- Community survey results have been received and analyzed
- School leaders are preparing reports on external influences in Student Demographics, Student Achievement, Political and Economic Climate, Finance, Technology, Human Resources, and General and Special Education trends

Item **SAO Cybersecurity Audit Update**

Information IT Staff will update the Board on the progress that has been made on the SAO Cybersecurity Audit findings. We will share the new documentation that has been developed in response to the findings and provide a general update on items that have been completed, are in progress, and are still pending completion.

Contact Mari Liles and Craig DeBellis

Action Information Only

Cybersecurity Audit
State Auditor's Office

Update Report to
TSD's Governing Board
12.14.19

Background Info for New Board Members:

- Oct. 2018 – Jan 2019 – SAO conducted a Cybersecurity Audit at TSD.
- Feb. 2019 – State Auditor's Office released (2) reports of their findings.

Where We Are Today:

- The State Auditor's Office requested an update from TSD on **November 4, 2019**.
- Our responses are due to SAO on **December 13, 2019.**

We are required to submit 2 separate reports:

- A status update of the recommendations in the Public Audit Report on Cybersecurity at the School for the Deaf (SAO Report No. 19-031; Released 2/26/2019).
- A status update of the recommendations in the Confidential Information Technology Report (dated February 26, 2019).

Timelines for corrections and improvements:

- Each finding in the (2) audit reports has a Target/Implementation Date which must be addressed and improved by **November 4, 2024.**

Legislative and Other Influences Guiding Cybersecurity Requirements

- **SB 820: Effective 9.1.19**
  - SB 820 requires school districts to adopt a cybersecurity policy.
    TASB recently released on 10.24.19, a new cybersecurity policy (CQB).
    TASB's policy does **NOT** meet all of the requirements recommended and required by DIR.
  - SB 820 requires school districts to ensure all employees who use district computer systems or databases, as well as elected board members, have **annual cybersecurity training** certified by DIR.
- **HB 3834: Effective 9.1.19**

  - HB 3834 requires that certain state and local government employees and state contractors complete a cybersecurity training program certified by the Department of Information Resources.
- **Growing Concerns About Cybersecurity and the Need for Training Include:**
  - Awareness of the different forms of cybersecurity threats
  - The importance of password security
  - Protecting agency, school, and student data
  - Email, internet and social media habits
  - Identifying agency security weaknesses

SAO Summary of Findings and Issue Ratings

Chapter/ Subchapter	Title	Issue Rating [a]
1-A	The School Should Establish and Document Its Information Security Policies, Standards, and Procedures, and It Should Implement a Process to Identify and Manage Its Information Security Risks	Priority
1-B	The School Should Strengthen Its Processes and Controls to Ensure That External Service Providers Meet Its Information Security Requirements	High
2-A	The School Should Establish and Document Its System Configurations and Its Processes for Systems Development and Change Management	Medium
2-B	The School Should Strengthen Access Controls over Its Information Systems	High
3	Although the School Implemented Network and Physical Security Controls, It Should Strengthen Certain Controls over Its Incident Detection, Response, and Recovery Planning	Medium

Update on SAO Findings in Public Report

- **SAO Finding #1-A**

1-A	The School Should Establish and Document Its Information Security Policies, Standards, and Procedures, and It Should Implement a Process to Identify and Manage Its Information Security Risks	Priority

- **TSD's Response:**
  - We have developed TSD Information Security Guidelines using an Information Security Policy template created by the Texas Education Agency and a Data Use Agreement Form from DIR.
  - These guidelines have been shared with ALL TSD Staff as recommended by the SAO.
  - We will create a TSD Policy from these guidelines within the coming year.
  - We have started researching cybersecurity training programs and materials that could be used to train TSD staff. '**KnowBe4' is one of the programs we are researching.**

- **TSD's Status:** *Substantially Implemented*: Successful development of the guidelines. We will use TASB's Cybersecurity Policy and TSD's Information Security Guidelines to create TSD's Cybersecurity Policy.

New Guidelines, Procedures and Policies Developed to Support and Manage Risks

- Data Use Agreement Form
- Information Security Guidelines
- TASB's New CQB Cybersecurity Policy

Update on SAO Findings in Public Report

- **SAO Finding #1-B:**

1-B	The School Should Strengthen Its Processes and Controls to Ensure That External Service Providers Meet Its Information Security Requirements	High

- **TSD's Response:**
  - We have a new procedure in place to review Service Organization Control Reports from external providers which are audit reports of how they secure and protect TSD's data.
  - TSD's Health Center has started migrating to Professional Software for Nurses, Inc.'s SNAP Health Portal to confidentially secure and manage student data.

- **TSD's Status:** *Substantially Implemented*

Update on SAO Findings in Public Report

- **SAO Finding #2-B:** *(detailed in the SAO's confidential report)*

2-B	The School Should Strengthen Access Controls Over Its Information Systems	High

- **TSD's Response:**
  - The database team modified the HR Core and added nightly scripts to identify possible findings when they occur and to alert IT staff to user account mismatches. We have made significant changes in the IT server room to enhance security.

- **TSD's Status:** *Substantially Implemented*: Successful progress with access controls and security enhancements but we are still making some configuration changes. There are more significant changes that will take place this summer when there are fewer programs in session at TSD.

Questions or Comments?

TSD Data Use Agreement

Please read the following agreement carefully and completely before signing

This Agreement applies to employees of Texas School for the Deaf (hereafter referred to as “agency”) who handle confidential and sensitive information, including financial, medical, personnel, or student data and pertains to all state-owned or controlled Information Resources. The purpose of this Agreement is to inform you of your principal obligations concerning the use of agency Information Resources, and to document your Agreement to abide by these obligations.

"Information Resources" has the meaning defined in Texas Government Code § 2054.003(7): “. . .the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.” Additionally, data impacted by the aforementioned is included as Information Resources.

Under Texas Administrative Code §202.22(3), the user of an information resource has the responsibility to:

- (A) use the resource only for the purpose specified by the agency or information-owner;
- (B) comply with information security controls and agency policies to prevent unauthorized or accidental disclosure, modification, or destruction; and
- (C) formally acknowledge that they will comply with the security policies and procedures in a method determined by the agency head or his or her designated representative.

Confidential and Sensitive Information

As an employee of agency, you may have access to confidential or sensitive information through use of agency Information Resources or through your associated activities with agency information systems. Confidential and sensitive information includes identifying information, federal tax information, personal health information, criminal justice information, or any information that is classified as confidential or sensitive by federal or state law, by agency policy, or is defined as “Personal Identifying Information” under Texas Business and Commerce Code §521.002(a)(1) or “Sensitive Personal Information” as defined by Texas Business and Commerce Code §521.002(a)(2).

As a user of agency systems, you are required to conform to applicable laws and agency policies governing confidential and sensitive information.

Your principal obligations in this area are outlined below. You are required to read and to abide by these obligations.

I understand that:

- In the course of my job, I may have access to confidential and sensitive information related to:
    - Customers, employees, users, contractors, and volunteers (e.g., records, conversations, applications, financial information). This may include any information by which the identity of a person can be determined, either directly OR indirectly.
    - Agency functions (e.g., information protected by the attorney-client and attorney work product privilege, financial information, employment records, contracts, federal tax information, internal reports, memos and communications.).
    - Third parties (e.g., vendor information, customer information, contracts).

I agree that:

- I will, at all times, safeguard and retain the confidentiality, integrity and availability of confidential and sensitive information.
- I will only access confidential and sensitive information for business needs.
- I will not in any way divulge, copy, release, sell, loan, review, alter, or destroy any confidential or sensitive information except as authorized.
- I will not misuse or carelessly handle confidential and sensitive information.
- I will encrypt confidential and sensitive information when appropriate, including when emailing such information outside the agency and when storing such information on portable electronic devices and portable storage devices.
- I will safeguard and will not disclose my password or other authorization I have that allows me to access confidential and sensitive information, except as permitted by law.
- I will report activities by any other individual or entity that I suspect may compromise the confidentiality, integrity or availability of confidential and sensitive information.
- My privileges hereunder are subject to periodic review, revision, and if appropriate, renewal.
- I have no right or ownership interest in any confidential or sensitive information referred to in this Agreement. The agency may revoke my access to confidential and sensitive information at any time and without notice.

Authorized Use – I agree that:

- I will use Information Resources only for official state-approved business.
- I will not use Information Resources for personal reasons unless there are specific limited use exceptions permitted by the agency division to which I am assigned.
- I have no right to expect privacy in my use of agency Information Resources or in the content of my communications sent or stored in agency Information Resources. All user activity is subject to monitoring, logging, and review.

Personal Security Identification Codes (User ID’s and Passwords) - I agree that:

- I will receive and will be required to use a personal security identification code (User ID and Password) to gain access to and to use Information Resources.
- My user ID and password are security measures that must be used only by me and I will not disclose my password to anyone.
- I will be held personally responsible for any transactions initiated, actions taken, or for any harm, loss, or adverse consequences arising from the use of my user ID and password, including any unauthorized use by a third party if such party gains access to my user ID and password due to my misconduct or failure to abide by agency policy.

Software - I agree that:

- I will only install or use software on agency computers that has been properly licensed and approved for my use in accordance with agency policies and procedures.
- If installing or authorizing the installation of software on agency computers, I will be responsible for ensuring that such software is only used in a manner that complies with the terms of the applicable software license agreement and all applicable agency policies and procedures.

Access to Data - I agree that:

- Proper authorization is required for access to all data owned by agency, except data that has been authorized by the agency for public access.
- I will not attempt to access or alter any data that I am not authorized to access in the performance of my job duties.
- I will not use agency Information Resources to review, alter, or otherwise act to obtain access to information about myself, or any relative, friend, or business associate.
- I will use appropriate measures to prevent others from obtaining access to agency data, such as securing my workstation either by logging off or using a password-protected screen saver.
    - Before leaving a workstation with access to files containing confidential or sensitive information, I will log-off or activate a password-protected screen saver.
    - If I receive a request for the release of agency information or data, I will follow agency's policies and procedures for the release of information.

Security of Equipment - I agree that:

- I will not remove Information Resources from agency property without proper prior authorization and approval of staff with appropriate authority.
- I will immediately report all security incidents, including the loss or theft of any Information Resources or data, to agency management and to the agency Information Security Officer.

I agree that:

- I am required to be aware of, read, and comply with the information in the agency Information Security Policy found at afp://soco.tsd.state.tx.us/Cybersecurity
- I must comply with the policies concerning Information Resources set out in the agency Policies and Procedures Manual, as well as any changes to those policies.
- I must comply with the information security policies, standards, and guidelines of the agency division that employs me, including any changes to those policies, standards, and guidelines.
- My failure to comply with this Agreement may result in loss of access privileges to agency Information Resources or other disciplinary action up to and including termination for employees; termination or alteration of employment relations in the case of temporaries, contractors, or consultants; or dismissal for interns and volunteers. Additionally, individuals could also be subject to additional civil liability, and/or criminal charges.

Your Full Name	
Your Email	
DO you agree to the Data Use Agreement above?	☐ Yes
After downloading and reviewing the TSD Information Security Guidelines, DO you agree to be in compliance with these guidelines? To download, click TSD Information Security Guidelines	☐ Yes

Submit

Information Security Guidelines
Texas School for the Deaf

Revised Date: December 2, 2019

Table of Contents

An internal email address, ***information.security@tsd.state.tx.us*****,** has been established for reporting information security issues.

INTRODUCTION

The possibility that electronic information could be lost, corrupted, diverted, or misused represents a real threat to mission performance for the Texas School for the Deaf (TSD) and other government agencies. Today, TSD is more dependent than ever on information technology. Information technology has gone from being important to being essential in the performance of these missions. However, even as TSD's dependence on information technology has grown, so too has the vulnerability of this technology and the range of external threats to it.

Information security is a key aspect of the interaction among many important societal issues—defense, terrorism, commerce, privacy, intellectual property rights, and computer crime. Information technology resources also consume a growing share of the State's budget and are becoming increasingly important to daily life. As a result, a considerable body of applicable guidelines is in place, consisting of laws, statutes, regulations, Executive Orders, and other directives. TSD's Information Security Program, as well as those of other agencies, must operate within these complex guidelines landscape to ensure that the State, and in particular, TSD meets its obligations to its citizens and customers. Providing for the security of information resources is not only a difficult technical challenge, it is also a human challenge. Ultimately information security is a human endeavor that depends heavily on the behavior of individual people.

PURPOSE OF THESE GUIDELINES

By information security we mean protection of the ***Texas School for the Deaf's***, hereinafter referred to as the ***TSD,*** data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose of the information security guidelines is:

- To establish an ***TSD***-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of ***TSD*** data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of the ***TSD*** and allow the ***TSD*** to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with these guidelines.

GENERAL GUIDELINES

Throughout the document the terms *must* and *should* are used carefully. The term *must* is not negotiable; the term *should* is a goal for the ***TSD***.

- The ***TSD*** will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the ***TSD***'s data, network and system resources.
- Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.
- Vulnerability and risk assessment tests of external network connections must be conducted on a regular basis. At a minimum, testing should be performed annually, but the sensitivity of the information secured may require that these tests be done more often.
- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual: network administrator, system administrator, data custodian, and users.
- Violation of the Information Security Guidelines may result in disciplinary actions as authorized by the ***TSD*** in accordance with ***TSD*** and disciplinary policies, procedures, and codes of conduct.

OWNERSHIP

The Information Security Policies are owned by the ***TSD*** Information Resources Manager (**IRM**). The **IRM**, or designate, is the only authority that can approve modifications to the Security Policies.

Support Information
These Guidelines are supported by the Security Policy Standards.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the ***TSD.***

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

SECURITY GUIDELINES DEVELOPMENT AND MAINTENANCE GUIDELINES

Introduction

The ***TSD*** Information Security Policies provides the operational detail required for the successful implementation of the Information Security Program. These security policies were developed based on, and cross referenced to, the Security Guidelines Standards. In addition, these policies have been developed by interpreting Health Insurance Portability and Accountability Act of 1996 (HIPAA), Texas Administrative Code, Chapter 202 (TAC 202) and other legislation and legal requirements, understanding business needs, evaluating existing technical implementations, and by considering the cultural environment.

Purpose
The business, technical, cultural, and legal environment of ***TSD***, as it relates to information resources use and security, is constantly changing. These policies are technology neutral and apply to all aspects of information resources. Emerging technologies or new legislation, however, will impact these Information Security Policies over time. The Security Policies will be revised as needed to comply with changes in federal or state law or rules promulgated there under or to enhance its effectiveness.

Security Guidelines Development and Maintenance Guidelines

A number of factors could result in the need or desire to change the Security Policies. These factors include, but are not limited to:

- Review schedule
- New federal or state legislation
- Newly discovered security vulnerability
- New technology
- Audit report
- Business requirements
- Cost/benefit analysis
- Cultural change

Updates to the ***TSD*** Information Security Policies, which include establishing new policies, modifying existing policies, or removing policies, can result from three different processes:

- At least annually, the Information Security Officer (**ISO**), or designee, will review the Policies for possible addition, revision, or deletion. An addition, revision, or deletion is created if it is deemed appropriate.

- Every time new information resource technology is introduced into the ***TSD,*** a security assessment should be completed. The result of the security assessment could necessitate changes to the Security Policies before the new technology is permitted for use at the ***TSD***.

Any User may propose the establishment, revision, or deletion of any practice standard at any time. These proposals should be directed to the **ISO** who will evaluate the proposal and make recommendations to the Information Resource Manager **(IRM)**.

Once a change to the Security Policies has been approved by the **IRM**, or designee, the following steps will be taken as appropriate to properly document and communicate the change:

- The appropriate **IT** Security web pages will be updated with the change
- Training and compliance materials will be updated to reflect the change

The changes will be communicated using standard ***TSD*** communications methods such as: announcements, web page notification, newsletters, and communications meetings.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

SECURITY GUIDELINES STANDARDS

Introduction

The Information Security Guidelines Standards apply to all information obtained, created, or maintained by the ***TSD****'s* automated Information Technology. These Guidelines Standards are based on the interpretation of Texas Administrative Code, Title 1, Part 10, Chapter 202 (TAC 202) and other reference material and apply equally to all levels of management and to the personnel they supervise. Further, these Guidelines Standards apply to all information generated by the ***TSD****'s* Information Technology functions, through the time of its transfer to ownership external to the ***TSD*** or its proper disposal/destruction.

Audience

These Guidelines Standards apply equally to all personnel including, but not limited to, the ***TSD***'s employees, agents, consultants, volunteers, and all other authorized users granted access to information resources.

Definitions

Information: Any and all data, regardless of form, that is created, contained in, or processed by, Information Technology facilities, communications networks, or storage media.

Information Resources: any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Key Roles & Responsibilities

Information Resources Manager (IRM): Responsible to the ***TSD*** and the State of Texas for management of the ***TSD***'s information resources. The designation of an ***TSD*** **IRM** is intended to establish clear accountability for setting guidelines for information resources management activities, provide for greater coordination of the state ***TSD***'s information activities, and ensure greater visibility of such activities within and between state agencies. The **IRM** has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the information resources of the ***TSD.***

Information Security Officer (ISO): Responsible to the **IRM** for administering the information security function within the ***TSD***. The **ISO** is the ***TSD***'s internal and external point of contact for all information security matters. The **ISO** duties are include but are not limited to:

- Assuring the information security guidelines is updated on a regular basis (at a minimum annually) and published as appropriate.
- Appropriate training is provided to data owners, data custodians, network and system administrators, and users.
- Appoints a person, if applicable, to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

Technology Management Team (TMT): Designated as a coordinating group comprised of information personnel from the ***TSD***, chaired by the **IRM** and chartered with the task to establish procedures to implement these policies within their areas of responsibility, and for monitoring compliance.

Program Manager: Assigned information resource ownership; responsible for the information used in carrying out program(s) under their direction and provides appropriate direction to implement defined security controls and procedures.

Technical Manager (TM): Assigned custodians of information resources; provide technical facilities and support services to owners and users of information. **TM**'s assist Program Management in the selection of cost-effective controls used to protect information resources. **TM**'s are charged with executing the monitoring techniques and procedures for detecting, reporting, and investigating breaches in information asset security.

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the use of the information. Where appropriate, ownership may be shared by managers of different departments.

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For server applications Information Technology is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

User: Has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.

Information Technology (IT): The name of the ***TSD*** department responsible for computers, networking, and data management.

Internal Auditor: Ensures that the ***TSD***'s information resources are being adequately secured, based on risk management, as directed by the **IRM** acting on delegated authority for risk management decisions.

System Administrator: Person responsible for the effective operation and maintenance of information resources, including implementation of standard procedures and controls to enforce an organization's security guidelines. Whereas each ***TSD*** will have one Information Security Officer, technical management may designate a number of system administrators.

Security Guidelines Standards

The ***TSD*** will protect the information resource assets of the Texas School for the Deaf and the in accordance with Standards and Guidelines as published by Your State and Federal regulations.

Specifically, the ***TSD*** will apply policies, procedures, practice standards, and guidelines to protect its **IT** functions from internal data or programming errors and from misuse by individuals within or outside the ***TSD***. This is to protect the ***TSD*** from the risk of compromising the integrity of shared data, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public's safety.

All ***TSD*** information security programs will be responsive and adaptable to changing technologies affecting information resources.

Guidelines Standard	Detail based on Best Practices
Reference #	
1	Information Technology Security controls must not be bypassed or disabled.
2	Security awareness of personnel must be continually emphasized, reinforced, updated and validated.
3	All personnel are responsible for managing their use of information resources and are accountable for their actions relating to information resources security. Personnel are also equally responsible for reporting any suspected or confirmed violations of these guidelines to the appropriate management immediately.
4	Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management immediately.
5	Access to, change to, and use of information resources must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as at each job status change such as: a transfer, promotion, demotion, or termination of service.
6	The use of information resources must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of information resources utilization, the establishment of effective use, and reporting of performance to management.

Guidelines Standard, continued	Detail based on Best Practices
Reference #	
7	Any data used in an information resources system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.
9	On termination of the relationship with the ***TSD*** users must surrender all property and information resources managed by the ***TSD***. All security policies for information resources apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, these guidelines survive the terminated relationship.
10	The owner must engage the **IRM**, or designate, at the onset of any project to acquire computer hardware or to purchase or develop computer software. The costs of acquisitions, development and operation of computer hardware and applications must be authorized by appropriate management. Management and the requesting department must act within their delegated approval limits in accordance with the ***TSD*** authorization guidelines. A list of standard software and hardware that may be obtained without specific, individual approval will be published.
11	The department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian.

Guidelines Standard, continued	Detail based Best Practices
Reference #	
12	The information resource network is owned and controlled by **IT**. Approval must be obtained from **IT** before connecting a device that does not comply with published guidelines to the network. **IT** reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.
13	The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all ***TSD*** legal and fiscal policies and procedures.
14	The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.
15	All changes or modifications to information resource systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.
17	All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the ***TSD*** is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

Guidelines Standard, continued	Detail based on TAC 202 and Best Practices
Reference #	
18	All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized ***TSD*** officer and must contain terms approved as to form by the Legal Department.
19	Information resources computer systems and/or associated equipment used for ***TSD*** business that is conducted and managed outside of ***TSD*** control must meet contractual requirements and be subject to monitoring.
20	External access to and from information resources must meet appropriate published ***TSD*** security guidelines.
21	All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The **IRM** through **IT** reserves the right to remove any unlicensed software from any computer system.
22	The **IRM** through **IT** reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to: games, instant messengers, pop email, music files, image files, freeware, and shareware.
23	Adherence to all other policies, practice standards, procedures, and guidelines issued in support of these guidelines statements is mandatory.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

VIOLATIONS AND DISCIPLINARY ACTIONS GUIDELINES

Introduction

All **TSD** information resources are subject to certain rules and conditions concerning official and appropriate use as specified.

Purpose

Any event that results in theft, loss, unauthorized use, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denied services of information resources constitutes a breach of security.

Violations Guidelines

Violations may include, but are not limited to any act that:

- exposes the ***TSD*** to actual or potential monetary loss through the compromise of information resources security,
- involves the disclosure of sensitive or confidential information or the unauthorized use of ***TSD*** data or resources,
- involves the use of information resources for personal gain, unethical, harmful, or illicit purposes, or results in public embarrassment to the ***TSD***.

Disciplinary Actions Guidelines

Violations of these Information Security Policies may result in immediate disciplinary action that may include, but may not be limited to:

- formal reprimand,
- suspended or restricted access to ***TSD*** information resources,
- restitution or reimbursement for any damage or misappropriation of any ***TSD*** property,
- suspension without pay,
- termination of employment,
- termination of contract,
- civil prosecution or state and/or federal criminal prosecution.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

ACCEPTABLE USE GUIDELINES

Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus these guidelines is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of the ***TSD*** are the property of the ***TSD***.

Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the ***TSD*** are not private and may be accessed by ***TSD*** **IT** employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

Acceptable Use Guidelines

The ***TSD*** must have guidelines on appropriate and acceptable use that includes these requirements:

- ***TSD*** computer resources must be used in a manner that complies with ***TSD*** policies and State and Federal laws and regulations. It is against ***TSD*** guidelines to install or run software requiring a license on any ***TSD*** computer without a valid license.
- All software must be authorized by the ***TSD* IT** prior to use. A list of authorized software will be maintained in Appendix A of these Guidelines. Individuals may request written approval for software use through the ***TSD* IRM**. Unauthorized software is subject to removal upon discovery.
- Use of the ***TSD***'s computing and networking infrastructure by ***TSD*** employees unrelated to their ***TSD*** positions must be limited in both time and resources and must not interfere in any way with ***TSD*** functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.
- Uses that interfere with the proper functioning or the ability of others to make use of the ***TSD***'s networks, computer systems, applications and data resources are not permitted.
- Use of ***TSD*** computer resources for personal profit is not permitted.
- Files, images, emails or documents which may cause legal action against or embarrassment to the ***TSD,*** may not be sent, received, accessed in any format (i.e. auditory, verbal or visual), downloaded or stored on ***TSD*** information resources.
- All messages, files and documents – including personal messages, files and documents – located on ***TSD*** information resources are owned by the ***TSD***, may be subject to open records requests, and may be accessed in accordance with these guidelines.
- Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations.
- Use of network sniffers shall be restricted to system administrators who must use such tools to solve network problems. Network sniffers may be used by auditors or security officers in the performance of their duties. All use of network sniffers shall be approved by the **IRM.** They must not be used to monitor or track any individual's network activity except under special authorization as defined by ***TSD*** guidelines that protects the privacy of information in electronic form.
- Users must not download, install or run any programs or utilities on their systems except those authorized and installed by the ***TSD* IT** and specifically designed to conduct the business of the ***TSD***. Examples of non-business related software or files include, but are not limited to: unauthorized peer-to-peer (P2P) file-sharing software, games, unauthorized instant messengers (IM), pop email, music files, image files, freeware, and shareware. Unauthorized software may be removed upon discovery.

Incidental Use

As a convenience to the ***TSD*** user community, incidental use of information resources may be permitted. The following restrictions apply:

- Incidental use must not interfere with the normal performance of an employee's work duties.
- Storage of personal email messages, voice messages, files and documents within ***TSD***'s information resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on ***TSD*** information resources are owned by ***TSD***, may be subject to open records requests, and may be accessed in accordance with these guidelines.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

Appendix *A* to the Acceptable Use Guidelines
Approved *TSD* Software

Approved ***TSD*** Software is comprised of three categories; Level I, Level II, and Level III as listed and defined below:

TSD Level I Software

Operating Systems, networking and application software which is ***TSD*** licensed, fully supported, and IT pre-installed (imaged) on all ***TSD*** workstations.

MacOS 10.12, 10.13, 10.14, 10.15
Microsoft Office 2019 for Mac
Sophos Antivirus
Alertus Desktop
Apple Keynote, Pages, Numbers
Convo VRS Application for Mac
Purple P3 VRS Application for Mac

Sorenson VRS Application for Mac
ZVRS Application for Mac
JAMF Self Service
All others available in JAMF Self Service

TSD Level II software

Application software which is IT installed, fully supported and ***TSD*** licensed on an as needed basis for requested ***TSD*** workstations. **Level II** software requires a written Supervisor/Team Leader authorization request to the ***TSD IRM*** for approval prior to installation**.**

Parallels Desktop 15
Microsoft Windows 7, 8 and 10
Microsoft Office 2019 for Windows
Adobe Creative Suite
NutriKids

TSD Level III Software

Application software which IT verifies the license, installs the software on requested ***TSD*** workstations, but is not IT supported (personal production/organizational software i.e. an individually purchased Palm Pilot or Blackberry). If there is an issue with the installation of **Level III** software or the workstation performance after the installation, the workstation will be re-imaged.

Level III software requires a written Supervisor/Team Leader authorization request to the ***TSD IRM*** for approval prior to installation.

Rocket BlueZone (USAS, USPS)
AutoDesk AutoCAD
Software installed in Austin Community College's PCs, servers
Texas Facilities Commission's PCs and installed software (OnSSI, S2)
All others not listed

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

ACCOUNT MANAGEMENT GUIDELINES

Introduction
Computer accounts are the means used to grant access to ***TSD*** information resources. These accounts provide a means of providing accountability, a key to any computer security program, for Information Technology usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose
The purpose of the ***TSD*** Account Management Security Guidelines is to establish the rules for the creation, monitoring, control and removal of user accounts.

Account Management Guidelines

- All accounts created must have an associated **Helpdesk** request and approval that is appropriate for the ***TSD*** system or service.
- All users must sign the ***TSD*** Data Use Agreement before access is given to an account.
- All accounts must be uniquely identifiable using the assigned user name.
- All default passwords for accounts must be constructed in accordance with the ***TSD*** Password Guidelines.
- All accounts must have a password expiration that complies with the ***TSD*** Password Guidelines.
- Accounts of individuals on extended leave (more than 30 days) will be disabled.
- All new user accounts that have not been accessed within 30 days of creation will be disabled.
- Supervisors are responsible for immediately notifying Information Security of individuals who change roles within ***TSD*** or are separated from their relationship with ***TSD***
- System Administrators or other designated staff:
  - are responsible for removing the accounts of individuals that change roles within ***TSD*** or are separated from their relationship with ***TSD***
  - must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
  - must have a documented process for periodically reviewing existing accounts for validity
  - are subject to independent audit review
  - must provide a list of accounts for the systems they administer when requested by authorized ***TSD*** management
  - must cooperate with authorized ***TSD*** management investigating security incidents.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

DATA CLASSIFICATION GUIDELINES

Introduction

Agreed information security classification definitions are an essential pre-requisite for many information security policies. They provide a consistent method for assessing and applying a sensitivity level to the important information assets of the ***TSD***. These classification "labels" can then be used as the basis for evaluating the appropriate protective measures (technical and non-technical) needed to ensure the risk to these assets is minimized.

Purpose

It is essential that all ***TSD*** data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. To assure proper protection of the ***TSD***'s information resources, various levels of classifications will be applied.

Data Classification Guidelines

The ***TSD*** has specified three classes below:

High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements.
These guidelines recognize that other data may need to be treated as high risk because it would cause severe damage to the ***TSD*** if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.
Confidential – Data that would not expose the ***TSD*** to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.
Public - Information that may be freely disseminated.
All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the ***TSD***.

- Owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.
- No ***TSD***-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.
- High risk data must be encrypted during transmission over insecure channels.
- Confidential data should be encrypted during transmission over insecure channels.

- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

EMAIL USE GUIDELINES

Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus these guidelines is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of email.
- To educate individuals using email with respect to their responsibilities associated with such use.

Purpose

The purpose of the ***TSD*** Email Guidelines is to establish the rules for the use of ***TSD*** email for the sending, receiving, or storing of electronic mail.

Definitions

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Email Use Guidelines

- The following activities are prohibited by guidelines:
  - Sending email that is intimidating or harassing.
  - Using email for purposes of political lobbying or campaigning.
  - Violating copyright laws by inappropriately distributing protected works.
  - Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
  - The use of unauthorized e-mail software.
  - Excessive personal use. Personal Use of email is a privilege which is revocable at any time.

- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
  - Sending or forwarding chain letters.
  - Sending unsolicited messages to large groups except as required to conduct ***TSD*** business.
  - Sending or forwarding email that is likely to contain computer viruses.
- All sensitive ***TSD*** material transmitted over external network must be encrypted.
- All user activity on ***TSD*** information resource assets is subject to logging and review.
- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of ***TSD*** or any unit of the ***TSD*** unless appropriately authorized to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the ***TSD***. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."
- Individuals must not send, forward or receive confidential or sensitive ***TSD*** information through non-***TSD*** email accounts. Examples of non-***TSD*** email accounts include, but are not limited to: Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

Individuals must not send, forward, receive or store confidential or sensitive ***TSD*** information utilizing non-***TSD*** accredited mobile devices. Examples of mobile devices include, but are not limited to: Personal Data Assistants, two-way pagers and cellular telephones.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

MALICIOUS CODE GUIDELINES

Introduction

The number of computer security and malicious code incidents linked with the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

The purpose of the Malicious Code Guidelines is to describe the requirements for dealing with computer virus, spyware, worm and Trojan Horse prevention, detection and cleanup.

Malicious Code Guidelines

- The willful introduction of computer viruses or disruptive/destructive programs into the ***TSD*** environment is prohibited, and violators may be subject to prosecution.
- All workstation systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to **IT**'s recommendations.
- All servers that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that it is kept updated. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.
- All incoming data including electronic mail must be scanned for viruses where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
- Where feasible, system or network administrators should inform users when a malicious code threat has been detected.
- Virus scanning logs should be maintained whenever email is centrally scanned for viruses.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

NETWORK ACCESS GUIDELINES

Introduction

The ***TSD*** network infrastructure is provided as a central utility for all users of ***TSD*** information resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet ***TSD*** demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the ***TSD*** Network Access Guidelines is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of ***TSD*** information.

Network Access Guidelines

- Users are permitted to use only those network addresses issued to them by ***TSD*** **IT**.
- All remote access (dial in services) to ***TSD*** will be either through an approved modem pool or via an approved Internet Service Provider (ISP).
- Remote users may connect to ***TSD*** information resources only through methods and using protocols approved by ***TSD***.
- Users inside the ***TSD*** firewall may not be connected to the ***TSD*** network at the same time a modem is being used to connect to an external network.
- Users must not install network hardware or software that provides network services without written approval from the **IRM**. This includes wireless access points, modems, and remote access software.
- Non ***TSD*** computer systems that require network connectivity must conform to ***TSD*** **IT** Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, ***TSD*** users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the ***TSD*** network infrastructure without written approval from the **IRM**.
- Users are not permitted to alter network hardware in any way.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

PASSWORD GUIDELINES

Introduction

User authentication is a means to control who has access to an Information Technology system. Controlling the access is necessary for any information resource. Access gained by an unauthorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to the ***TSD***.

Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- Something you know – password, Personal Identification Number (PIN)
- Something you have – Smartcard
- Something you are – fingerprint, iris scan, voice

A combination of factors – Smartcard and a PIN

Purpose

The purpose of the ***TSD*** Password Guidelines is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the ***TSD*** user authentication mechanisms.

Password Guidelines

- All passwords, including initial passwords, must be constructed and implemented according to the following ***TSD*** Information Technology rules:
  - it must adhere to a minimum password standard as established by Appendix A of these Guidelines
  - it must be routinely changed to adhere to the password aging standard as established in Appendix A of these Guidelines
  - it must not be anything that can easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
  - it must not be dictionary words or acronyms
  - password history must be kept to prevent the reuse of a password
- Stored passwords must be encrypted.
- User account passwords must not be divulged to anyone. ***TSD*** **IT** and **IT** contractors must not ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with the ***TSD***.
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Guidelines for the sake of ease of use.
- Users must not circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the ***TSD*** **ISO**. In order for an exception to be approved there must be a procedure to change the passwords.
- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- **IT** Helpdesk password change procedures must include the following:

- authenticate the user to the helpdesk before changing password
- change to a strong password
- the user must change password at first login

- In the event passwords are found or discovered, the following steps must be taken:
  - Take control of the passwords and protect them
  - Report the discovery to the ***TSD*** Help Desk

Transfer the passwords to an authorized person as directed by the ***TSD*** **ISO**

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

Appendix *A* to the Password Guidelines

TSD minimum password standard

The following minimum standard for password creation applies to users of ***TSD*** information systems.

Use a minimum of eight characters and a combination of alpha and numeric characters.

Users are encouraged to use a more complex password structure including at least one character from the following four classes:

- English upper case letters
- English lower case letters
- Numerals (0,1,2,...)
- Non-alphanumeric (special) characters such as punctuation symbols (!@#$%^&*_+=?/~`;:,<>|\).

- Very important passwords (e.g. password for any privileged or administrative account) should be at least 10 characters long;
- Do not base PIN or passwords on any of the following details:
  - Months of the year, days of the week or any other aspect of the calendar;
  - Family names, initials or car registration numbers;

- A proper name or any word in the dictionary without altering it in some way;
- Can be derived from a dictionary word, e.g. by reversing letters;
- Department or faculty names, identifiers or references;
- Telephone numbers or similar all numeric groups;
- User ID, user name, group ID or other system identifier;
- More than two consecutive identical characters;
- All-numeric or all-alphabetic groups;
- Obvious phrases or sequences such as "TSD123" or "123456";

- Do not reuse a password: construct a new password each time it is changed.
  The following strategies will help users to generate a password that is easy to remember, is hard to guess and complies with the ***TSD*** guidelines.

- Use a mixture of upper and lower case, numerals and punctuation e.g. **Keep0ut!**
- String several words or parts of words together e.g. **it'sCold**
- Choose a phrase, perhaps a line from a poem or song and form passwords by concatenating words from the phrase along with digits and/or punctuation. e.g. **Tw1nkL3*** (from twinkle, twinkle, little star)
- Invent phrases like car registration plates e.g. **one4you!**

TSD password aging guidelines

- Passwords must be changed at least every 90 days

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

PORTABLE COMPUTING GUIDELINES

Introduction

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

Purpose

The purpose of the ***TSD*** Portable Computing Security Guidelines is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of ***TSD*** information.

Definitions

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from ***TSD*** information resources. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and cell phones.

Portable Computing Guidelines

- Only ***TSD*** approved portable computing devices may be used to access ***TSD*** information resources.
- Portable computing devices **must** be password protected.
- Sensitive ***TSD*** data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive ***TSD*** data should be encrypted using approved encryption techniques.
- ***TSD*** data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- TSD mobile devices including, but not limited to PDA's and smart phones and will be used only for TSD business and must be used in accordance to the guidelines established by ***Appendix A*** of these Guidelines.
- All remote access (dial in services) to the ***TSD*** network must be through an approved method as established in the network access guidelines.
- Non ***TSD*** computer systems that require network connectivity must conform to ***TSD*** **IT** Standards and must be approved in writing by the ***TSD*** **ISO**. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

APPENDIX A to PORTABLE COMPUTING GUIDELINES

TSD Mobile Device Acceptable Use Guidelines

TSD mobile devices including but not limited to PDA's, smart phones and Blackberry's will be used only for *TSD* business. No personal email may be stored on TSD devices.

All mobile devices must be password protected.

TSD owned devices will be connected via *TSD* approved access methods.

The following four requirements apply to *TSD* employees wishing to use a personal device to access your TSD mail account:

1) employee must use Outlook Web Access or VPN access
2) employee must enable a pass code on the device
3) employee must enable the option to wipe the device after 10 failed attempts to enter the pass code
4) employee must receive written authorization from ***information.security@tsd.state.tx.us*** – which can be GRANTED based on compliance with requirements 1,2, and 3

Phone service may only be used to call another TSD owned device. All TSD mobile devices are part of an TSD pool of phone minutes. Calls between *TSD* owned devices do not impact the TSD pool of minutes or accrue charges. All other phone calls will use minutes from the TSD pool. Only users specifically authorized for additional phone services may initiate non-emergency calls to phone numbers other than to another TSD owned mobile device.

Users must report lost or stolen mobile devices **IMMEDIATELY**. During normal business hours, the report should be made to the TSD Help Desk. After normal business hours and on weekends, lost or stolen devices should be reported to the IT Director or ***information.security@tsd.state.tx.us***.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

PRIVACY GUIDELINES

Introduction

Privacy Policies are mechanisms used to establish the limits and expectations for the users of ***TSD*** information resources. Internal users should have no expectation of privacy with respect to information resources.

Purpose

The purpose of the ***TSD*** Information Privacy Guidelines is to clearly communicate the ***TSD*** Information Technology privacy expectations to information resource users.

Definitions

Webserver: A computer that delivers (*serves up*) web pages.

Web page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape Navigator, and Microsoft Internet Explorer.
Website: A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.

Privacy Guidelines

- Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of ***TSD*** are not private and may be accessed by ***TSD*** **IT** employees, for business reasons at any time without knowledge of the information resource user or owner.
- To manage systems and enforce security, the ***TSD*** may log, review, and otherwise utilize any information stored on or passing through its **IT** systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. For these same purposes, the ***TSD*** may also capture User activity such as IP addresses and web sites visited.
- A wide variety of third parties have entrusted their information to ***TSD*** for business purposes, and all workers at the ***TSD*** must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.
- Users must report any weaknesses in ***TSD*** computer security, any incidents of possible misuse or violation of this agreement to the proper authorities. An internal email address, ***information.security@tsd.state.tx.us*****,** has been established within the ***TSD*** for reporting information security issues.
- Users must not attempt to access any data or programs contained on ***TSD*** systems for which they do not have authorization or explicit consent.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

SECURITY AWARENESS GUIDELINES

Introduction

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

Purpose

The purpose of the Security Awareness Guidelines is to describe the requirements that will ensure each user of ***TSD*** information resources receives adequate training on information security awareness issues.

Security Awareness Guidelines

- All new users must complete an approved Security Awareness orientation prior to, or at least within 90 days of, being granted access to any ***TSD*** information resources.
- All users must sign an acknowledgement stating they have read and understand ***TSD*** requirements regarding computer security policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect ***TSD*** information resources.
- **IT** must prepare, maintain, and distribute one or more information security manuals that concisely describe ***TSD*** information security policies and procedures.
- **IT** must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest as approved by the **ISO**.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

SOFTWARE LICENSING GUIDELINES

Introduction

End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

Purpose

The purpose of the Software Licensing Guidelines is to establish the rules for licensed software use on ***TSD*** information resources.

Software Licensing Guidelines

- The ***TSD*** provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.
- Third party copyrighted information or software, that the ***TSD*** does not have specific approval to store and/or use, must not be stored on ***TSD*** systems or networks. All software on ***TSD*** computers will be procured, maintained and installed by **IT** unless specific written approval is granted. System administrators may remove unauthorized material.
- Third party software in the possession of the ***TSD*** must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

EXCEPTION GUIDELINES

Introduction

The ***TSD*** Information Security Policies provide the techniques and methodology to protect ***TSD*** information resource assets. While these Policies are technology independent they are more closely linked to the technology than the Guidelines Standards and are hence more likely to be impacted by changing technology, legislation, and business requirements. As with most policies there may be a need for exception.

Purpose

An exception is a method used to document variations from the rules

Exception Guidelines

In certain cases, compliance with specific guidelines requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- Required commercial or other software in use is not currently able to support the required features;
- Legacy systems are in use which do not comply.
- Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, a written explanation of the compliance issue must be developed and a plan for coming into compliance with the ***TSD***'s Information Security Guidelines in a reasonable amount of time. Explanations and plans should be submitted according to the process for approval:

The steps for permitting and documenting an exception are:

- A request for an exception is received by the **ISO** along with a business case for justifying the exception
- The **ISO** analyzes the request and the business case and determines if the exception should be accepted, denied, or if it requires more investigation
- If more investigation is required the **ISO** and **TMT** determine if there is a cost effective solution to the problem that does not require an exception
- If there is not an alternate cost effective solution, and the risk is minimal, the exception may be granted
- Each exception must be re-examined according to its assigned schedule. The schedule can vary from 3 months to 12 months depending on the nature of the exception

Any exception request that is rejected may be appealed to the **IRM**.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

ADMINISTRATION/SPECIAL ACCESS GUIDELINES

Introduction

Technical support staff, security administrators, system administrators and others may have special access account *privilege* requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

Purpose

The purpose of the ***TSD*** Administrative/Special Access Practice Standard is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege.

Administrative/Special Access Guidelines

- ***TSD*** departments must submit to **IT** a list of administrative contacts for their systems that are connected to the ***TSD*** network.
- All users of Administrative/Special Access accounts must sign the ***TSD*** Information Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization.
- Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the **ISO**.
- Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Each account used for administrative/special access must meet the ***TSD*** Password Guidelines.
- The password for a shared administrator/special access account must change when an individual with the password leaves the department or ***TSD***, or upon a change in the vendor personnel assigned to the ***TSD*** contract.
- In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
  - Must be authorized by the **ISO**, must be created with a specific expiration date and must be removed when work is complete.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Actions

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

BACKUP/DISASTER RECOVERY GUIDELINES

Introduction

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, data entry errors, system operations errors or other data corruption.

Purpose

The purpose of the ***TSD*** Backup/DR Guidelines is to establish the rules for the backup and storage of electronic ***TSD*** information.

Backup/Disaster Recovery Guidelines

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- The ***TSD*** Information Technology backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for ***TSD*** must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest ***TSD*** sensitivity level of information stored.
- A process must be implemented to verify the success of the ***TSD*** electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Procedures must be reviewed at least annually.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action
Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

CHANGE MANAGEMENT GUIDELINES

Introduction

The Information Technology infrastructure at the ***TSD*** is expanding and becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Technology infrastructures grows, the need for a strong change management process is essential. Managing these changes is a critical part of providing a robust and valuable Information Technology infrastructure.

Purpose

The purpose of the Change Management Guidelines is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of information resource.

Definitions

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the use of the information. Where appropriate, ownership may be shared by managers of different departments.

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications Information Technology is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that information is protected against improper modification before, during, and after system implementation.

Change:

- any implementation of new functionality
- any interruption of service
- any repair of existing functionality
- any removal of existing functionality

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure, the discovery of security vulnerability or other emergency.

Emergency Change: When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

Change Management Guidelines

- Every change to an ***TSD*** **IT** resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Guidelines and must follow the Change Management Procedures.
- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) should be reported to or coordinated with the leader of the change management process.
- The **TMT** Committee will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.
- A formal written change notification must be submitted for all changes, both scheduled and unscheduled.
- All scheduled change notifications must be submitted in accordance with change management procedures so there is time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- The appointed leader of the **IRM** may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year end accounting, or if adequate resources cannot be readily available.
- A Change Review shall be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
    - Date of submission and date of change
    - Owner and custodian contact information
    - Nature of the change
    - Indication of success or failure

All ***TSD*** information systems must comply with an **IT** change management process that meets the standards outlined above.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

INCIDENT MANAGEMENT GUIDELINES

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources, as outlined in the Email Guidelines and the Acceptable Use Guidelines.

Definitions

Computer Incident Response Team (CIRT): Personnel responsible for coordinating the response to computer security incidents in an organization

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Trojan Horse: Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

Security Incident: In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent**.**

Vendor: someone who exchanges goods or services for money.

Incident Management Guidelines

- ***TSD*** CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The **ISO** is responsible for notifying the **IRM** and the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
- The **ISO** is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The **ISO**, working with the **IRM**, will determine if a widespread ***TSD*** communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The **ISO** is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
- The ***TSD*** **ISO** is responsible for reporting the incident to the:
  - **IRM**
  - Department of Information Resources as outlined in TAC 202
  - Local, state or federal law officials as required by applicable statutes and/or regulations
- The **ISO** is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the **ISO** will recommend disciplinary actions, if appropriate, to the **IRM**.

- In the case where law enforcement is involved, the **ISO** will act as the liaison between law enforcement and ***TSD***.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

INTRUSION DETECTION GUIDELINES

Introduction

Intrusion detection plays an important role in implementing and enforcing an organizational security guidelines. As information technologies grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

Purpose

Intrusion detection provides two important functions in protecting information resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

Intrusion Detection Guidelines

- Intruder detection must be implemented for all servers containing data classified as high risk.
- Operating system and application software logging processes should be enabled on all critical server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems should be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

NETWORK CONFIGURATION GUIDELINES

Introduction

The ***TSD*** network infrastructure is provided as a central utility for all users of ***TSD*** information resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the ***TSD*** Network Configuration Security Guidelines is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of ***TSD*** information.

Network Configuration Guidelines

- ***TSD*** Information Technology (**IT**) owns and is responsible for the ***TSD*** network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent ***TSD*** network infrastructure capable of exploiting new networking developments, all cabling must be installed by ***TSD*** **IT** or an approved contractor.
- All network connected equipment must be configured to a specification approved by ***TSD*** **IT**.
- All hardware connected to the ***TSD*** network is subject to ***TSD*** **IT** management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of ***TSD*** **IT**.
- The ***TSD*** network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by ***TSD*** **IT**.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by ***TSD*** **IT**.
- All connections of the network infrastructure to external third party networks are the responsibility of ***TSD*** **IT**. This includes connections to external telephone networks.

- ***TSD* IT** Firewalls must be installed and configured following the ***TSD*** Firewall Implementation Standard documentation.
- The use of departmental firewalls is not permitted without the written authorization from ***TSD* IT**.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the ***TSD*** network without ***TSD* IT** approval.
- Users must not install network hardware or software that provides network services without ***TSD* IT** approval.
- Users are not permitted to alter network hardware in any way.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

PHYSICAL ACCESS GUIDELINES

Introduction

Technical support staff, security administrators, system administrators, and others may have Information Technology physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Technology facilities is extremely important to an overall security program.

Purpose

The purpose of the ***TSD*** Physical Access Guidelines is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Technology facilities.

Physical Access Guidelines

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Information Technology restricted facilities must be documented and managed.
- All **IT** facilities must be physically protected in proportion to the criticality or importance of their function at the ***TSD***.

- Access to **IT** facilities must be granted only to ***TSD*** support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to **IT** facilities must include the approval of the person responsible for the facility.
- Each individual that is granted access rights to an **IT** facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
- Requests for access must come from the applicable ***TSD*** data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Technology facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the **IT** facility immediately.
- Cards and/or keys must not have identifying information other than a return mail address.
- All **IT** facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for **IT** facilities must be kept for routine review based upon the criticality of the information resources being protected. The person responsible for the **IT** facility must remove the card and/or key access rights of individuals that change roles within ***TSD*** or are separated from their relationship with ***TSD***.
- Visitors must be escorted in card access controlled areas of **IT** facilities.
- The person responsible for the **IT** facility shall review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the **IT** facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

SYSTEM DEVELOPMENT GUIDELINES

Introduction

The development of new systems, applications or major enhancements to existing systems is often the result of significant changes made to the processes they support. Ideally, the efforts to simplify business processes will be done by the functional office in conjunction with the technical staff, so that current technologies can be considered as the processes are reviewed. Ultimately, the most important criteria for development is to create changes that are best for the ***TSD*** as a whole.

Purpose

The purpose of the System Development Guidelines is to describe the requirements for developing and/or implementing new software within the ***TSD***.

Definitions

System Development Life Cycle (SDLC): a set of procedures to guide the development of production application software and data items. A typical SDLC includes design, development, maintenance, quality assurance and acceptance testing.

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or use of the information. Where appropriate, ownership may be shared by managers of different departments

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications, Information Services is the custodian; for micro and mini applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

User: Has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.

Production System: The hardware, software, physical, procedural, and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

System Development Guidelines

- Information Technology **(IT)** is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for ***TSD*** system development projects. All software developed in-house which runs on production systems should be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality

assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical ***TSD*** information.

- All production systems must have designated Owners and Custodians for the critical information they process. **IT** must perform periodic risk assessments of production systems to determine whether the controls employed are adequate.
- All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. A designated access control administrator (who is not a regular user on the system in question) must be assigned for all production systems.
- Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Migration of code between SDLC environments must comply with the Change Management Guidelines. All production software testing must utilize sanitized information.
- All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

SECURITY MONITORING GUIDELINES

Introduction

Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as but not limited to the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Help desk logs
- Other log and error files.

Purpose

The purpose of the Security Monitoring Guidelines is to ensure that Information Technology security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measurement, Limitation of Liability, and Capacity Planning.

Security Monitoring Guidelines

- Automated tools will be used by the ***TSD* IT** to provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
  - Internet traffic
  - Electronic mail traffic
  - LAN traffic, protocols, and device inventory
  - Operating system security parameters

- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
  - Automated intrusion detection system logs
  - Firewall logs
  - User account logs
  - Network scanning logs
  - System error logs
  - Application logs
  - Data backup and recovery logs
  - Help desk trouble tickets

- The following checks will be performed at least quarterly by assigned individuals:
  - Password strength
  - Unauthorized network devices
  - Unauthorized personal web servers
  - Unsecured sharing of devices
  - Operating System and Software Licenses

Any security issues discovered will be reported for follow-up investigation. An internal email address, ***information.security@tsd.state.tx.us*,** has been established within the ***TSD*** for reporting information security issues.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

SYSTEM SECURITY GUIDELINES

Introduction

Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Purpose

The purpose of the ***TSD*** System Security Guidelines document is to describe the requirements for installing a new system in a secure fashion and maintaining the security of the server and application software.

System Security Guidelines

All systems introduced on the ***TSD*** network should be made secure before placing them into production. This is known as "hardening" the systems. This process should be a combination of vendor recommendations, and industry best practices and procedures as deemed appropriate.

- Installing the operating system from an **IT** approved source.
- All systems connected to the ***TSD*** network should have a vendor supported version of the operating system installed.
- All systems connected to the ***TSD*** network should be current with security patches, hot fixes or updates for operating systems and applications. Security patches, hot fixes or updates must be applied in a timely manner, as approved by the **TMT,** to protect ***TSD*** information resources**.**
- Setting security parameters, file protections and enabling audit logging.
- Warning banners must be established, as appropriate, on all system access points. The approved ***TSD*** warning banner is included in Appendix A of these guidelines.
- All unnecessary services should be disabled.
- Systems in the final stages of hardening may be placed on the ***TSD*** network in an isolated segment such as a segmented lab environment to minimize exposure.

- Vulnerability scans or penetration tests must be performed on all Internet-facing applications and systems before placement into production. At a minimum, quarterly audits must be conducted to re-evaluate the risk potential of applications and systems.
- System integrity checks of server systems housing high risk ***TSD*** data should be performed.

Support Information

These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

Appendix *A* to the System Security Guidelines

Approved *TSD* Warning Banner

********** WARNING! **********

Unauthorized use of this system is prohibited and may be subject to criminal prosecution. The System Administrator may monitor any activity or communication on the system and retrieve any information stored within the system. By accessing this system, you are consenting to such monitoring and information retrieval. You should have no expectation of privacy as to any communication on or information stored within this system except as explicitly stated in officially approved system privacy policies. Unauthorized or improper use of this system is a violation of law and may be prosecuted resulting in criminal, civil, and/or administrative penalties.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

VENDOR ACCESS GUIDELINES

Introduction

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems; they can monitor and fine tune system performance; they can monitor hardware performance and errors; they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to the ***TSD***.

Purpose

The purpose of the ***TSD*** Vendor Access Guidelines is to establish the rules for vendor access to ***TSD*** information resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and the protection of ***TSD*** information.

Vendor Access Guidelines

- Vendors must comply with all applicable ***TSD*** policies, practice standards and agreements, including, but not limited to:
  - Safety Policies
  - Privacy Policies
  - Security Policies
  - Auditing Policies
  - Software Licensing Policies
  - Acceptable Use Policies
- Vendor agreements and contracts must specify:
  - The ***TSD*** information the vendor should have access to
  - How ***TSD*** information is to be protected by the vendor
  - Acceptable methods for the return, destruction or disposal of ***TSD*** information in the vendor's possession at the end of the contract
  - The Vendor must only use ***TSD*** information and information resources for the purpose of the business agreement
  - Any other ***TSD*** information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- The ***TSD*** will provide an **IT** point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these guidelines.
- Each vendor must provide the ***TSD*** with a list of all employees working on the contract. The list must be updated and provided to the ***TSD*** within 24 hours of staff changes.
- Each on-site vendor employee must acquire an ***TSD*** identification badge that will be displayed at all times while on ***TSD*** premises. The badge must be returned to the ***TSD*** when the employee leaves the contract or at the end of the contract.
- Each vendor employee with access to ***TSD*** sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate ***TSD*** personnel.
- If vendor management is involved in ***TSD*** security incident management, the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable ***TSD*** change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate ***TSD*** management.

Support Information
These Guidelines are supported by the Security Policy Standard.

Disciplinary Action

Violation of these guidelines may result in disciplinary action which may include termination. Additionally, individuals are subject to loss of ***TSD*** information resources access privileges, as well as civil and criminal prosecution. Violations of these guidelines or aggregate security policies are subject to the guides established in the Violations and Disciplinary Actions Guidelines of the TSD.

Revision History

Version	Author	Date	Comments	Approved by	Approved Date
v 1.0	Craig DeBellis	12/02/19		Mari Liles	12/02/19

Cybersecurity Policy

Each district shall adopt a cybersecurity policy to:

1. Secure district cyberinfrastructure against cyber attacks and other cybersecurity incidents; and
2. Determine cybersecurity risk and implement mitigation planning.

A district's cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources (DIR) under Government Code Chapters 2054 and 2059.

Cybersecurity Coordinator

The superintendent shall designate a cybersecurity coordinator to serve as a liaison between the district and the Texas Education Agency (TEA) in cybersecurity matters.

Report to TEA

The district's cybersecurity coordinator shall report to TEA any cyber attack or other cybersecurity incident against the district cyberinfrastructure that constitutes a breach of system security as soon as practicable after the discovery of the attack or incident.

Report to Parent

The district's cybersecurity coordinator shall provide notice to a parent of or person standing in parental relation to a student enrolled in the district of an attack or incident for which a report is required to TEA involving the student's information.

Definitions

For purposes of the district's cybersecurity policy, the following definitions apply:

Breach of System Security

"Breach of system security" means an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action.

Cyber Attack

"Cyber attack" means an attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.

Cybersecurity

"Cybersecurity" means the measures taken to protect a computer, computer network, or computer system against unauthorized use or access.

Education Code 11.175

Cybersecurity Training

At least once each year, a district shall identify district employees who have access to a district computer system or database and require those employees and board members to complete a cybersecurity training program certified under Government Code 2054.519 (state-certified cybersecurity training programs) or offered by the

district as described at District Training Program, below. *Gov't Code 2054.5191(a-1)*

The board may select the most appropriate state-certified cybersecurity training program or district training program for employees of the district to complete. The board shall:

1. Verify and report on the completion of a cybersecurity training program by district employees to the DIR; and
2. Require periodic audits to ensure compliance with these provisions.

Gov't Code 2054.5191(b)

District Training Program

A district that employs a dedicated information resources cybersecurity officer may offer to its employees a cybersecurity training program that satisfies the requirements described by Government Code 2054.519(b). *Gov't Code 2054.519(f)*

Security Breach Notification

A district that owns, licenses, or maintains computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the district determines that the breach occurred, except as provided at Criminal Investigation Exception, below, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

To Individuals

Resident of Other State

If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person that owns or licenses computerized data to provide notice of a breach of system security, the notice of the breach of system security required under Notice, below, may be provided under that state's law or under Notice, below.

To the Owner or License Holder

A district that maintains computerized data that includes sensitive personal information not owned by the district shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notice

A district may give the required notice to individuals or the owner or license holder by providing:

1. Written notice at the last known address of the individual;
2. Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001 (electronic records and signatures); or
3. If the district demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the district does not have sufficient contact information, by:
    a. Electronic mail, if the district has electronic mail addresses for the affected persons;
    b. Conspicuous posting of the notice on the district's website; or
    c. Notice published in or broadcast on major statewide media.

Information Security Policy

A district that maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice described above complies with the notice requirements if the district notifies affected persons in accordance with that policy.

To the Attorney General

A district that is required to disclose or provide notification of a breach of system security under these provisions shall notify the attorney general of that breach not later than the 60th day after the date on which the district determines that the breach occurred if the breach involves at least 250 residents of this state. The notification must include:

1. A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;
2. The number of residents of this state affected by the breach at the time of notification;
3. The measures taken by the district regarding the breach;
4. Any measures the district intends to take regarding the breach after the notification described at Notice, above; and
5. Information regarding whether law enforcement is engaged in investigating the breach.

To a Consumer Reporting Agency

If a district is required to notify at one time more than 10,000 persons of a breach of system security, the district shall also notify each consumer reporting agency, as defined by 15 U.S.C. 1681a,

that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The district shall provide the notice without unreasonable delay.

Criminal Investigation Exception

A district may delay providing the required notice to individuals or the owner or license holder at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.

Business and Commerce Code 521.053; Local Gov't Code 205.010

Definitions

For purposes of security breach notifications, the following definitions apply:

Breach of System Security

"Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner*. Business and Commerce Code 521.053(a)*

Sensitive Personal Information

"Sensitive personal information" means:

1. An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
    a. Social security number;
    b. Driver's license number or government-issued identification number; or
    c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
2. Information that identifies an individual and relates to:
    a. The physical or mental health or condition of the individual;
    b. The provision of health care to the individual; or

c. Payment for the provision of health-care to the individual.

"Sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

Business and Commerce Code 521.002(a)(2), (b)

Cybersecurity Information Sharing Act

A district may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-federal entity or the federal government a cyber threat indicator or defensive measure in accordance with the Cybersecurity Information Sharing Act, 6 U.S.C. Subchapter I (sections 1501–1510). *6 U.S.C. 1503(c)*

Removal of Personal Information

A district sharing a cyber threat indicator pursuant to these provisions shall, prior to sharing:

1. Review such indicator to assess whether it contains any information not directly related to a cybersecurity threat that the district knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

2. Implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the district knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

6 U.S.C. 1503(d)(2)

Definitions

For purposes of the Cybersecurity Information Sharing Act, the following definitions apply:

Cybersecurity Purpose

"Cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. *6 U.S.C. 1501(4)*

Cybersecurity Threat

"Cybersecurity threat" means an action, not protected by the First Amendment to the United States Constitution, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement. *6 U.S.C. 1501(5)*

Cyber Threat Indicator

"Cyber threat indicator" means information that is necessary to describe or identify:

1. Malicious reconnaissance, as defined in 6 U.S.C. 1501(12), including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
2. A method of defeating a security control or exploitation of a security vulnerability;
3. A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
4. A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
5. Malicious cyber command and control, as defined in 6 U.S.C. 1501(11);
6. The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
7. Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
8. Any combination thereof.

6 U.S.C. 1501(6)

Defensive Measure

"Defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. The term does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure or another entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure. *6 U.S.C. 1501(7)*

Information System

"Information system" has the meaning given the term in 44 U.S.C. 3502 and includes industrial control systems, such as supervisory

control and data acquisition systems, distributed control systems, and programmable logic controllers. *6 U.S.C. 1501(9)*

Security Control — "Security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information. *6 U.S.C. 1501(16)*

Security Vulnerability — "Security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control. *6 U.S.C. 1501(17)*

Access to Electronic Communications

Electronic Communication Privacy Act

Except as otherwise provided in the Electronic Communication Privacy Act, 18 U.S.C. 2510–22, a person commits an offense if the person:

1. Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication;

2. Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

    a. Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

    b. Such device transmits communications by radio, or interferes with the transmission of such communication; or

    c. Such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

    d. Such use or endeavor to use takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

    e. Such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

3. Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information

was obtained through the prohibited interception of a wire, oral, or electronic communication;

4. Intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the prohibited interception of a wire, oral, or electronic communication; or

5. Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by 18 U.S.C. 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518; knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation; having obtained or received the information in connection with a criminal investigation; and with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

It shall not be unlawful for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state.

18 U.S.C. 2511(1), (2)(d)

Stored Wire and Electronic Communications and Transactional Records Access Act

A district must comply with the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. 2701–12.

Whoever intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system commits an offense. *18 U.S.C. 2701(a)*

Exceptions

This section does not apply with respect to conduct authorized:

1. By the person or entity providing a wire or electronic communications service;

2. By a user of that service with respect to a communication of or intended for that user; or

3. By sections 18 U.S.C. 2703, 2704, or 2518.

18 U.S.C. 2701(c)

Definitions

Electronic Communication

"Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. *18 U.S.C. 2510(12), 2711(1)*

Electronic Storage

"Electronic storage" means:

1. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

2. Any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

18 U.S.C. 2510(17), 2711(1)

The term encompasses only the information that has been stored by an electronic communication service provider. Information that an individual stores to the individual's hard drive or cell phone is not in electronic storage under the statute. *Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012)*

Electronic Communications System

"Electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. *18 U.S.C. 2510(14), 2711(1)*

Electronic Communication Service

"Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications. *18 U.S.C. 2510(15), 2711(1)*

Facility

"Facility" includes servers operated by electronic communication service providers for the purpose of storing and maintaining electronic storage. The term does not include technology, such as cell phones and computers, that enables the use of an electronic communication service. *Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012)*

Person

"Person" means any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation. *18 U.S.C. 2510(6), 2711(1)*

Item	**Approval of Annual Report**
Information	In accordance with our Memorandum of Understanding on Accountability with TEA we publish an Annual Report describing the educational performance of the School; The Annual Report is disseminated to parents of enrolled students, districts that have students attending TSD, Regional Education Service Centers, and other state offices. The Report is provided for public discussion at the December board meeting.
Contact	Claire Bugen
Action	Request for Approval

TEXAS SCHOOL FOR THE DEAF

ANNUAL REPORT 2018-2019

kids Matter

TEXAS SCHOOL FOR THE DEAF
Est. 1856
LEARN. GROW. BELONG.

www.tsd.state.tx.us

Our Mission

Texas School for the Deaf ensures students learn, grow and belong in a language- rich environment while supporting students, families and professionals through statewide outreach services.

Our Vision

The Texas School for the Deaf aspires to be a premier leader in bilingual education that challenges each student to reach their full potential.

Table of Contents

A Reflection from the Board and the Superintendent

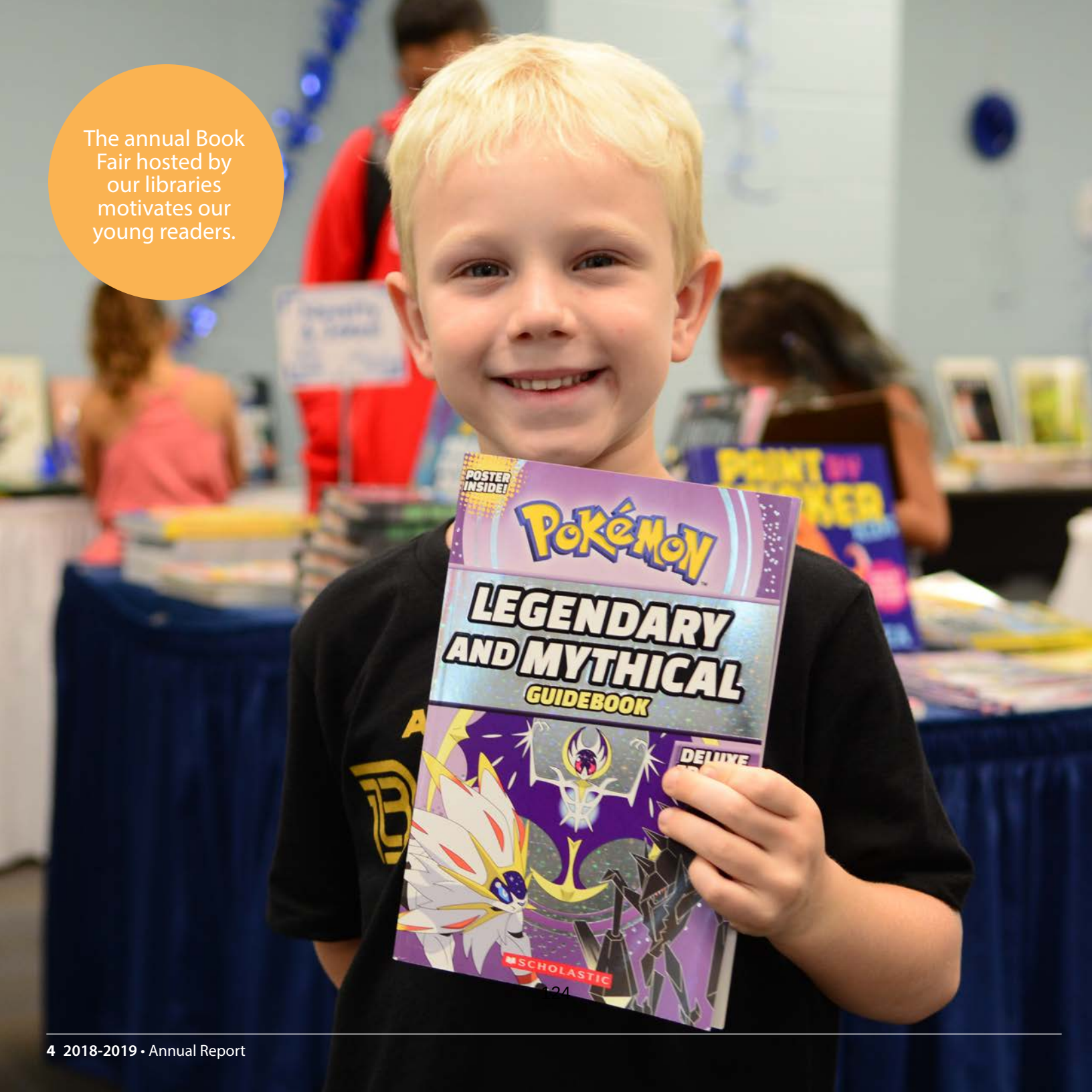
In 2018 – 2019, Texas School for the Deaf continued to make great strides on implementing our Strategic Plan for school improvement. Our goal to ensure that KIDS MATTER, not only here on campus in Austin, but statewide, was manifested in every aspect of our work. This work could not have been accomplished without our amazing partners. In this report, you will learn more about the wonderful staff, students, parents and community members that have helped us ensure that deaf and hard of hearing students thrive.

With the 86th Legislative Session behind us we are proud of our advocacy efforts with our parents, Texas Association of the Deaf and leaders who testified and supported the passage of bills that will advance language equality and acquisition for students who are deaf and hard of hearing, more resources for families with infants identified as deaf and improved culturally sensitive language to identify students who are deaf and hard of hearing. TSD also successfully secured funding in the session for Phase 2 of its Master Plan to include a new commercial Culinary Arts kitchen and café as well as safety, security and infrastructure upgrades for the campus.

This annual report will share highlights of our work offering a look inside the way in which we provide living and learning opportunities that integrate academic, social and emotional development that help each and every student to succeed.

Eric Hogue, Board President

Claire Bugen, Superintendent



The annual Book Fair hosted by our libraries motivates our young readers.

BUILDING A POSITIVE LEARNING ENVIRONMENT

- We've had a successful year with our **ACC Dual Credit Welding class**, further supporting our students by adding a more concentrated content mastery class in addition to the dual credit course. We also committed to two additional ACC Dual Credit courses for the 2019-2020 school year, working with **ACC** and **Texas Workforce Commission.**

45%
of the ACCESS students (18-22) had a successful work placement.

- There were 72 business partnerships between the **ACCESS** and CTE programs, and 21 of them were new businesses. Students gained employability skills through internships or paid work opportunities.

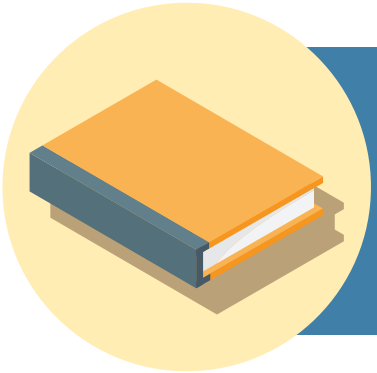
- The **CTE Culinary Arts** program took home the **championship trophy** in Las Vegas, showcasing their extraordinary culinary expertise.

- The **Middle School Battle of Books** reached to the National Level at Gallaudet University and the Middle School Math Counts participated in the national competition for the 12th year at the Rochester Institute of Technology.

- All across campus, we participated in the **Hour of Code**—doing a variety of activities, such as using the Sphero, using coding software via iPads, and participating in coded activities in Physical Education.

Automotive Technology will be a new ACC Dual Credit class for the upcoming school year.

- The **Elementary K-2** program began its first year in the K-2 **Bilingual Language Arts program**, focusing on strengthening both, American Sign Language and English literacy skills.



40%
increase in students checking out books at our Libraries.

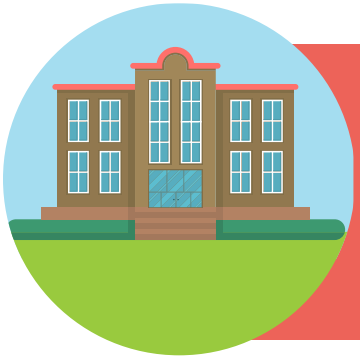
- The **Middle School** received a Technology Lending Grant for a **one-on-one iPad initiative**, enhancing instruction in the classroom and extending learning after hours.

Honor Graduates from left to right are Jakiya Murphy, Leila Sicoli, Salutatorian, Sunita Schmidjorg, Valedictorian, Precious Schwartz and Jaida Scott.

- The **ECE teachers and staff partnered with our ECE-Elementary librarian** to guide parents with reading and building activities after reading throughout the year. The project increased school and home connection and each family who came to the storytelling activities brought home a kit including the book they read.

- **Gallaudet University** recognized our many students' **literacy projects in ASL and English** in the Spring.

- The High School **BLUE Chargerbots Robotics Team** grabbed the TAPPS Championship!



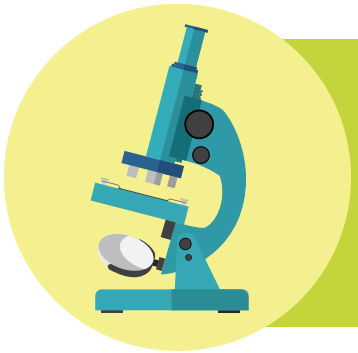
31

Seniors were accepted to either 4-year and 2-year colleges and community colleges.

- The **ACCESS** program had a successful **Fall and Spring Bazaars**, where students used skills learned in the program to learn the business aspects of the bazaars and sell products they designed.

- **ACCESS** program received awesome **grants** to help support our students: ACCESS wears Prada (Fashion Show), Measure Twice, Cut Once (Wood making skills) and Mother Hubbard's Cupboard (Corner Market).

- The **PE** Program revived the **Splash and Dash** event for the Elementary PE Classes.



25

25 Students enrolled in a dual-credit Forensics science class.

- The **Middle School service learning** continues: students went to the Central Texas Food Bank, The Ronald McDonald House, and sponsored the Annual Thanksgiving Food Drive on campus.

- **High School** students **exceeded MAP growth** projections.

- The **Summer Reading Project** funded by our Foundation complete its 5th year.

- **Academic Intervention** strategies continued to reduce failure rates in high school.

20

Students took College Algebra and 10 attempted to earn CLEP credit.

Mission Accomplished! Spike Out Champions!

ADVANCING SOCIAL AND EMOTIONAL DEVELOPMENT

"It was an exciting, memorable and record-breaking Athletic year!"

Winter Cheerleading

- placed second in Leopard Classic
- placed third in Clerc Classic

Cross Country

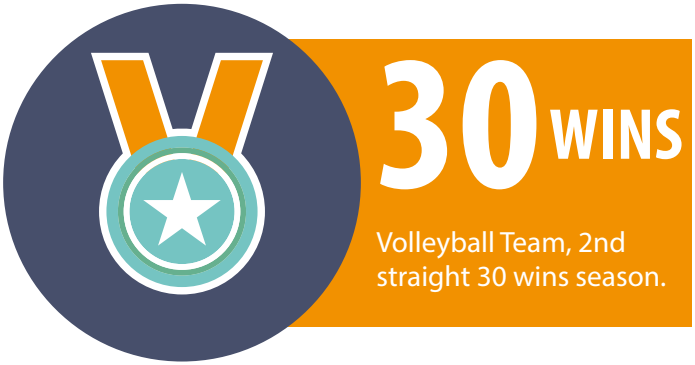
- Boys - NDIAA Team of the Year - 3rd consecutive year
- Girls - Best Team among Schools for the Deaf - 3rd consecutive year
- Girls - NDIAA Runner of the Year - Jaida Scott
- Girls achieved 29 personal and season bests in the 2 miler and 5K distances combined
- Boys achieved 37 personal and season bests in the 2 miler and 5K distances combined

Football

- Posted a winning, 8-win season
- Team Offense - Highest points scored (471) since 2007
- 5 players selected TAPPS All-State
- Preston Garrett was chosen as NDIAA Player of the Year

Volleyball Team

- won District Championship
- 3rd appearance in Spike Out Championship Game
- Sunita Schmidjorg selected as NDIAA Co-Player of Year & District Co-MVP



Boys Basketball Team

- posted a winning (11th straight winning season)
- placed FIRST in the Southwestern Classic (13th straight Southwestern title)
- qualified for state playoffs

Girls Basketball Team

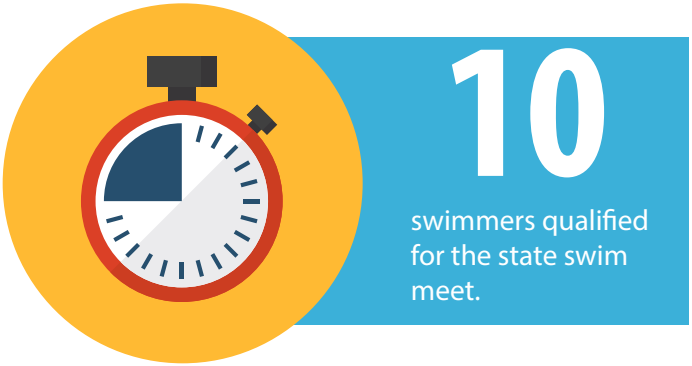
- DeafDigest & NDIAA Team of the Year
- NDIAA Player of the Year (Sunita Schmidjorg)
- NDIAA Coach of the Year (Brian Sipek)

Clerc Classic Repeat Champions!

- 33 wins: Most wins in the history of deaf school basketball (boys or girls)
- TAPPS 4A Final Four Appearance (back-to-back)
- TAPPS 4A District 4 Champions
- TAPPS 4A District 4 MVP (Sunita Schmidjorg)

Swim Team

- Boys - best youngest swim team of Freshman and Sophomore swimmers (very close to breaking records)
- Girls - achieved 60 personal and season bests
- Boys - achieved 50 personal and season bests



Wrestling Team

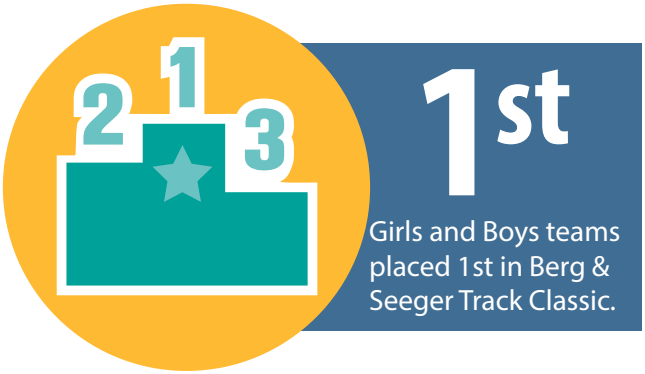
- posted a winning, 10 win season
- placed 2nd in Willigan Tournament

Baseball Team

- placed 3rd in Hoy Tournament

Softball Team

- placed 2nd in Hoy Tournament



Track Team

- 15 athletes qualified for the state track meet
- Ashley Harlicker won bronze in 800m
- Anabelle Weaver won silver in 3200m

International Studies Students admire the world's largest 4,086 mile salt flat at 11,995 feet above sea level.

- **Student Life** hosted its first **Holiday Open House** in December for teachers, staff and families.

- **Dorms** continue to receive **refurbishing** including living rooms, bedrooms and common areas.

9

Students took full-year credit course focusing on Bolivia.

- **International Studies students** had the opportunity to travel to **Bolivia** visiting 5 deaf schools and exploring their culture for 2 weeks.

- **Service-Learning** opportunities with **Healing Horses** helps students build independence and resilience.

Healing Horses helps students build independence and resilience.

- Students attended the **"Imagination Celebration"** in Ft. Worth hosted by Regional Day School Programs for the Deaf.

- **Sunshine 2.0** traveling theater troupe based at RIT's National Technical Institute for the Deaf (NTID), came to work with our students, providing workshops after school hours.

- Class Poster Competition during **Spirit Week** showcased our students' creative talents!

Spirit Week Posters.

Rendering of the Early Learning Center and Central Services Building.

FACILITIES, SAFETY AND FINANCE

Deferred Maintenance Projects were completed across the campus as we near the end of GMP 4 including:

- **Clinger Gymnasium** improvements included a new roof, reengineering of the gym floor for improved structural support, installation of an HVAC system, window replacement, new bleachers, and fire suppression sprinkler system.

- **R. L. Davis Auditorium** underwent installation of an elevator for ADA compliant access to the dressing rooms, renovation of the dressing rooms to make them more accessible and add restrooms, upgrading the house lights, upgrading the HVAC system, and carpet replacement.

- **Master Plan Phase 1** achieved 75% design completion for the new Central Administration/ Welcome Center, and Early Learning Center.

- **We became a 100% locked campus** and implemented a new Standard Response Protocol (SRP) for the safety of our staff and students.

- **We continued to partner with the Texas Facilities Commission** in the maintenance, upkeep, and operation of our campus serving staff, students, as well as supporting outside and community events.

- **A new Risk Manager** was hired during the 18/19 school year to further enhance campus safety and security efforts.

- **The Business Services Division successfully migrated to a new financial software system**, replacing a state-issued legacy system that had been in use since the 1990's.

- **TSD was graciously appropriated $14.6M by the Texas Legislature** during the 85th Legislative Session for construction of a new Toddler Learning Center and Central Services Administrative Building, with groundbreaking scheduled for the 19/20 school year.

- **School Safety Bill** provides an annual allotment for school districts based on a formula.

$4000

approximated pay increase for the biennium for teachers, librarians, counselors, and nurses based on experience.

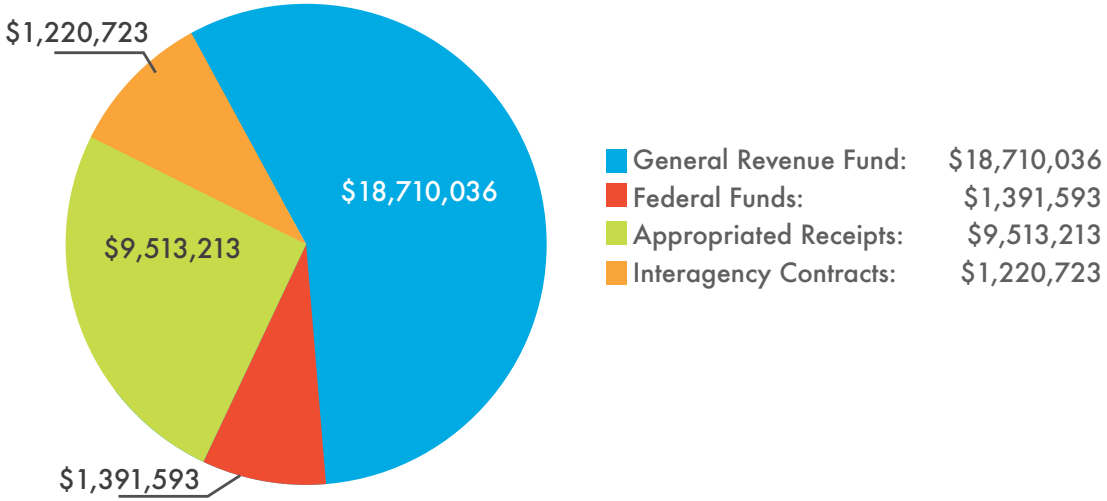
Legislative Success and Bills Passed

- **1 Behavior Health Specialist:** $63,864
- **3 Special Education staff:** $317,507
- **4% pay increase** for certain staff: $464,628
- **2 buses and 1 utility truck:** $270,000
- **Campus security infrastructure and CTE culinary:** $5,066,797
- **HB 2255:** Screening results must be shared with TSD.
- **SB 81:** Elimination of term ("hearing impaired", "hearing loss", "auditory impairment" and "speech impairment").
- **HB 548:** MOU with TEA, HHSC and TSD to ensure that the language acquisition of each deaf child under eight years of age is assessed and monitored regularly.

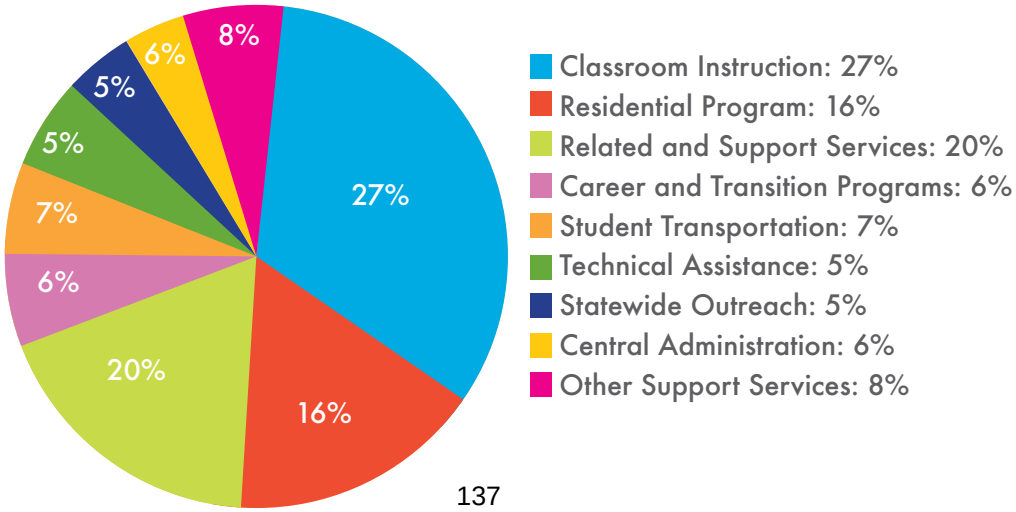
Second grade student demonstrates his Sphero Robot with Legislators at the Texas Capitol School House.

FINANCIAL DATA

FY 2019 REVENUE (APPROPRIATED)



FY 2019 APPROPRIATIONS BY FUNCTION



137

K-2 students engaged in TSD's Hour of Code!

ACADEMIC ACHIEVEMENT

TSD ACCOUNTABILITY DATA
A TWO-YEAR COMPARISON

OUTCOME MEASURES: STUDENT PROGRESS	Actual 2018	Actual 2019
% Academic Courses Passed	94.20%	88.20%
% Of Graduates Accepted in Postsecondary Education	82%	55%
% Career/Work Courses in Which Students Obtain a Passing Grade	99.38%	99.58%
% Of Life Skills Courses in Which Students Obtain a Passing Grade	99.38%	99.45%
% Grad under SBOE Rules for Sp Ed	100%	100%
% All Statewide Assessments – State Passing Standard is Met/Exceeded	37%	30%

For students in grades 3 – high school, the State of Texas Assessments of Academic Readiness (STAAR) are administered. All students who participate in the STAAR take assessments at their enrolled grade level. Students who have significant cognitive disabilities and who are receiving special education services participate in the STAAR Alternate 2 STAAR assessment

Type of State Assessments taken at TSD	Number of Students Tested	Percent of Students Tested
STAAR: Grades 3–8 and High School EOCs	317	91%
STAAR Alternate 2: Grades 3–8 and High School EOCs	33	9%

Percentage of students who passed STAAR (Grades 3 – 8)

Grade	2017-2018 Reading/ELA	2018-2019 Reading/ELA	2017-2018 Math	2018-2019 Math
3rd	19%	25%	31%	40%
4th	6%	14%	24%	11%
5th	20%	11%	65%	16%
6th	14%	17%	48%	52%
7th	9%	20%	53%	41%
8th	32%	32%	49%	63%

Percentage of students who passed STAAR Alternate 2 (Grades 3 – 8)

Grade	2017-2018 Reading/ELA	2018-2019 Reading/ELA	2017-2018 Math	2018-2019 Math
3rd	100%	100%	100%	100%
4th	100%	100%	100%	100%
5th	83%	N/A	100%	N/A
6th	100%	100%	100%	100%
7th	88%	83%	100%	100%
8th	100%	100%	83%	100%

Percentage of students who passed STAAR EOCs

Subject	2017-2018	2018-2019
English I	9%	9%
English II	13%	11%
Algebra I	44%	41%
Biology	48%	42%
US History	47%	38%

Percentage of students who passed STAAR Alternate 2 EOCs

Subject	2017-2018	2018-2019
English I	100%	100%
English II	100%	86%
Algebra I	100%	100%
Biology	100%	100%
US History	100%	100%

MEMORANDUM OF UNDERSTANDING WITH TEXAS EDUCATION AGENCY

Texas School for the Deaf (TSD) has a Memorandum of Understanding (MOU) with the Texas Education Agency (TEA) on Accountability. Although no one assessment is specified in the MOU, TEA approved TSD's request to move from giving the SAT 10 (a non-standards-based assessment) to the Measures of Academic Progress (MAP), which is a normed, state-aligned computer adaptive assessment program. MAP was not developed for students who meet eligibilities for Special Education.

MAP provides educators with a RIT (Rasch Unit) score which is an estimation of a student's instructional level. Through fall, winter and spring testing events, students, parents, educators and administrators can track student progress. After fall MAP assessments, NWEA (Northwest Evaluation Association - makers of MAP) provides a projected RIT growth score for each student in grades 3 – 10 in math and in reading. This score is a projected amount of "growth" for that academic school year. When asked how many students typically meet their predicted growth scores annually, NWEA stated,

"Since each student's growth goal is the mean (or average) normative growth, in a very general sense, one could reasonably expect that about 50% of students meet their growth goals."

Students with the most significant cognitive disabilities are included in the overall MOU results as well; however, these students are evaluated on report card results, which reflect mastery of IEP objectives, and not on MAP scores.

Department	Achieved Projected Growth
High School	57%
Middle School	61%
Elementary	29%
Percent of TSD Students Meeting or Exceeding Projected Academic Indicators	52%

On February 20 TSD welcomed then U.S. Department of Education Assistant Secretary Johnny Collett to TSD. He spent an event filled day with us which included snack time with our Parent Infant students, some frolicking with the kindergarteners in ASL class and time with high school students discussing their future educational and career goals.

STUDENT ENROLLMENT

Regular School Year Programs	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19
Parent Infant	18	19	18	28	20	23	21	22
Pre Kindergarten	10	19	19	11	9	18	18	11
Pre School	12	22	18	19	25	22	26	30
K5 - Elementary	98	94	104	120	115	110	118	124
Special Needs	81	59	64	61	54	57	72	75
Middle School	106	104	98	82	94	96	101	84
High School	173	178	208	197	201	192	201	185
ACCESS (Transitional)	28	55	52	66	65	44	44	40
TOTAL	526	550	581	584	583	562	601	571
Residential Enrollment	241	242	274	262	248	214	247	226

Summer Programs	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19
Extended Year Services Programs	36	52	40	32	30	16	29	62
Summer School	248	203	66	122	126	0*	67	75
Summer Enrollment Non-TSD	99	110	101	109	135	0*	53	85
Early Childhood	16	23	17	14	14	0*	16	9
Parent Infant	2	3	12	13	15	10	14	15
AI						17	7	27
STEM						11	5	
Other Short-Term Programs	145	179	233	159	146	151	175	248
TOTAL	461	445	459	449	436	205	366	521

TOTAL SERVED	1086	995	1040	1033	1019	767*	967	1092

** Summer programs were suspended in 2017 due to financial constraints.*

Summer STEM Camp students adjust their robot wheels.

ENGAGING STUDENTS, FAMILIES AND PROFESSIONALS STATEWIDE

- **25,239 students, families, pre-professionals and professionals received Outreach services** in the form of shared resources, consultations, training, tours, observations, retreats, short term programs, internships, classes, and summer camps.

- **ERCOD** expanded resources on the **Crossroads webpage for the Mental Health Initiative for Deaf Youth** and helped establish an advisory group to steer the future of this important work.

- **ERCOD** created a livestreamed celebration of **Deaflympians** with accompanying classroom activities that was accessed by 271 students and teachers statewide.

- Through live, interactive videoconferencing, **ASL Storytelling** offered weekly classes to 247 students statewide.

- Over the course of three **Discovery Retreats,** 87 students enjoyed learning that coding matters!

- **160 students** participated in a new model of **Summer Programs** focusing on Specialty Camps. One example, Deaf That! Camp – spotlighting Deaf Culture, Language and Identity received a lot of positive feedback from students who left feeling empowered by the experience.

- **Texas Deaf/Hard-of-Hearing Mentor Program** pilot program launched with 12 participants as first step toward full program start up in Fall 2019.

- **Guide by Your Side** matched 114 parents with Guides for their journey of parenting a deaf or hard-of-hearing child. GBYS also hosted 32 family events with 1,267 family members attending.

146

parents/guardians, their 120 children and 26 interns embodied the theme that "Families Matter" at the annual Family Weekend.

- Through videoconferencing, the **Family Signs** program brought free sign language instruction to 60 parents in the Fall, 66 in the Spring, and 31 throughout the summer.

- In its second year, the **DeafTEC** math conference saw international visitors included in the 98 participants who attended from across the nation.

- 577 attended **Communication Skills Workshops** to improve their sign communication skills.

- **National Deaf Education Conference** hosted by TSD brought 374 participants to campus to learn about best practices for improving educational outcomes.

Post-Secondary ACCESS students spread joy at their annual Holiday Bazaar.

YOUR SUPPORT MATTERS, THANK YOU!

- Alabama Institute for Deaf and Blind
- Alamo Drafthouse Cinema
- American Society for Deaf Children
- Applebee's
- The Art Alterations
- The City of Austin
- Austin Alumnae Delta Zeta
- Austin American-Statesman
- Austin Animal Clinic
- Austin Community College
- Austin Community College - Gallaudet University Regional Center
- Austin Duck Adventures
- Austin Habitat for Humanity Re-Store
- Austin Humane Society
- Austin ISD - Science Health Resource Center
- Austin Jeep People
- Austin Parks and Recreation
- Austin Public Library
- Austin Roasting Company
- Austin Sertoma
- Austin's Park & Pizza
- Barca Academy
- Barton Creek Square
- Ben White Florist
- Benevity Community Impact Fund
- BGK Architects
- Bicycle Sport Shop
- Birds Barbershop
- Bouldin Creek Cafe
- CAAG
- Rick Cantu
- Capital Metro Project Connect
- Terrence Casey
- Castle Hill Fitness
- Catholic Charities - Hope Donation
- Chaparral Ice
- Chick-Fil-A
- Chili's
- Clark Travel
- Clubhouse Cadets at TSD
- Communication by Hand
- Communication Services for the Deaf - CSD
- Convo
- Craig O's
- Crepe Crazy
- Crowne Plaza Austin
- Crux Climbing Center
- Michael Curtiss
- The Daily Moth
- DeafTEC
- The Deaf Network
- DME, LLC
- Doc's Backyard
- Downtown Austin Alliance
- Dawn Douglas
- Dress For Success Austin
- Early Childhood Intervention Services
- Ellis and Salazar ProCare
- Embassy Suites
- Endeavor Real Estate Group
- Enterprise Rental Car
- FlintCo
- Flower House
- Gallaudet University
- Georgetown Sertoma
- Goodwill Computer Works
- The Great Outdoors
- Hair O'The Dog Salon
- Harris Communications
- H-E-B Stores
- Hiland Dairy Foods
- Hilton Austin
- Hippo Insurance
- Holland Photo Imaging
- HomeGoods
- Hudson Meats
- Interntal Revenue Service
- Jo's Coffee
- JOANN Fabric & Craft Stores
- JW Marriott
- K & K Welding
- The Kallina Family
- KEYE
- Kimpton Hotel Van Zandt
- Gary Knippa & Friends
- KTBC Fox 7 Austin
- KVUE
- KXAN
- Labatt Food Service
- Lamar University
- Lone Star Pediatric Dental
- Lone Star Riverboat
- Lucky Robot
- Magnolia Café
- Main Event Austin
- McKinney-York Architects
- The Meadows Center/Tx State University
- Mindy's Bake Shop
- Moojo
- Moonlight Bakery
- MSD Capital
- National Association of the Deaf
- National Deaf Center
- National Technical Institute for the Deaf | RIT
- National Technical Institute for the Deaf Regional STEM Center
- National Tire & Battery
- North Austin Optimist Club
- Northwest Sertoma
- The Oasis
- Old Navy
- Open Door Preschools
- Orange Theory Fitness
- Parkhill Smith & Cooper
- Paz Veterinary
- PCSI
- PETCO
- Point Collision Center
- Pt. Venture Lions Club
- PSAV
- Relay Texas
- Round Rock Ballet Folklorico
- Round Rock Community Foundation
- The Round Rock Express
- Round Rock Serteens
- Round Rock Sertoma
- Scan Mailboxes
- Schlitterbahn New Braunfels
- Mark Seeger & Jeff Harper
- Share the Will Foundation
- Skull Mechanix Brewing
- Snarf's
- Socialisssima
- Sorenson Communications
- Noelle Sorenson
- The Soup Peddler
- Spectrum News Austin
- Spillar Custom Hitches
- Sprint
- Dawn and Jeffrey Steele
- StoryBuilt
- StreetLeverage
- Sun Moon Stars Learning Center
- T. J. Maxx
- Texas A&M Colonias Program
- Texas Association of Parents and Educators for the Deaf-TAPED
- Texas Association of the Deaf
- Texas Department of Public Safety
- Texas Early Hearing Detection and Intevention-TEHDI
- Texas Education Agency
- Texas Education Service Center Region 11
- Texas Education Service Center Region 13
- Texas Facilities Commission
- Texas Facilities Commission State Surplus Store
- Texas General Land Office
- Texas Hands & Voices/ Guide by Your Side
- Texas Health and Human Services
- Texas Legislature
- Texas School for the Blind and Visually Impaired
- Texas School for the Deaf Alumni Association
- Texas School for the Deaf Foundation
- Texas School for the Deaf PTSO
- Texas Workforce Commission
- Thundercloud Subs
- Todd Pilates
- Top Drawer Thrift Store
- TopGolf
- Torres Hair Design
- Trade Graphic Services
- Trader Joe's
- Tricycle Creative
- Trudy's Tex Mex
- TV Dinners
- Twomey Auto Works
- Typhoon Texas
- Ucki + Uchiko
- University Co-op
- The University of Texas
- The University of Texas Child Development Center
- The University of Texas Housing & Dining
- Veterans Colleague Resource Group
- VYPE
- Westlake High School Seniors
- Wheatsville Co-op
- Wild Foods
- Will Williams
- Word of Mouth Bakery
- Work & Woof
- Wurstfest
- YMCA of Austin
- Yoga Yoga
- Z-VRS/Purple Communications
- Zachary Scott Theater

Governing Board of the Texas School for the Deaf

From the left to right: Christopher Moreland, Heather Withrow, Board President Eric Hogue, Ryan Hutchison, Board Secretary Angie Wolf, David Saunders, Sha Cowan, Keith Sibley, and Board Vice President Shawn Saladin.

www.tsd.state.tx.us

1102 South Congress Avenue, Austin, Texas 78704 • (512) 462-5353 (v/tty) • Facebook/Instagram: @texasschoolforthedeaf • Twitter: @TSD_Main

Printed by TSD students at Ranger Press www.rangerpress.org

Item	**Continuum of Services Update**
Information	For our 2019-2020 school year, our students previously assigned to the Special Needs Department are now in classes across the campus in elementary, middle and high school. We refer to the programming for these students as "Applied Programming". Each individual student will be assessed and placed in appropriately challenging curriculum based on their academic needs. Students also have varying levels of academic, behavioral, transition, and social emotional support. The Continuum of Services Core Team continues to address the Applied Programming issues in the Middle and High Schools. We will provide you with an update on our work.
Contact	Stella Egbert
Action	Information Only

TEXAS SCHOOL FOR THE DEAF

APPLIED PROGRAMMING
PARENT AND FAMILY
HOLIDAY GATEHRING

December 17, 2019

Please join us for a holiday gathering in the Ford Multiple Purpose Room from 1 to 2pm.

High School Open House 2 - 3PM
Residential Open House 3 - 4PM

LIGHT REFRESHMENTS WILL BE SERVED

Applied Programming, Upper School Action Plan 2019-2020

The core team meets every 4 to 6 weeks, starting 11/19/2019. The core team ensures that the action plan are being met, consider input from parent seminars that are scheduled for the remaining year, and work together in ensuring the merge would be optimal for students, families, and program staff. The core team members are Claire Bugen (Superintendent), Stella Egbert (Director of Instruction), Wilmonda McDevitt (Director of Student Life), Elizabeth Sterling (Special Education Director), Karl Hummel (HS Principal), Megan Scarboro (CTE Principal), Lisa Svenningsen (HS Assistant Principal), and Brian Sipek (MS Principal).

Communication and Planning	Programming	Students
Quarterly Seminars with Parents: December 17, 2019, 1-2pm *Including HS Open House, 2-3pm* *Residential Open House, 3-4pm* ***Solicit feedback on when seminars would be preferred by parents from the above seminar and topics that parents would like to have.*** January/February 2020 March/April 2020 May 2020	HS Teachers have met on November 20th to discuss challenges and highlights of the past three months. MS Teachers have already been a part of the department meetings in MS. HS Teachers have had separate department meetings to focus on specific needs within the merge as well as they participate in the HS general department meetings. MS and HS Teachers and staff will meet with the MS and HS Administrative Team to begin discussing the first semester highlights and challenges since the Fall merge. Team will meet monthly going forward to solicit feedback and ensure support is in place as we continue to discuss the full merge.	ARD areas of focus highlighting needs of students are being individually discussed prior to REED ARDs or Annual ARDs. Such focuses: personal care page to identify level of supervision. Ensuring this is also being communicated/shared with the residential program as well. Ensure students' eligibilities and services are highlighted to prepare for future needs such as obtaining support after graduation.
Flyer for December 17th Parent Seminar and letter containing this chart will be sent the week of December 2nd. HS will have their Open House on December 17th to allow families to see the classroom setting and the Residential program will have its open house the same afternoon.	Professional Development Focuses in November and December are on Transition Plans, Personal Graduation Plans, and the like.	Discuss after school programming for students such as SOTX and other activities that would need supervision and support with the Residential/ Student Life/Athletic programs.
Picture Directory from MS and HS Programs went out prior to Fall Break.	HS will fill the vacant Assistant Principal to ensure they have the administrative team personnel to support all students within the high school program. The position will be posted within the month of December.	

Applied Programming, Upper School Action Plan 2019-2020

Communication and Planning	Programming	Students
HS Program personnel will personally be contacting parents upon return from Fall Break throughout the three weeks prior to Winter Break. Questions will stem towards individual student needs, progress, concerns and/or feedback.		

Academic Affairs

3 December 2019

Dear Parents, Guardians, and Families:

I hope this letter finds you well and you enjoyed your recent fall break with your family. I'm writing to follow up on our earlier forum meeting. In spite of many technical difficulties, and we apologize for that, we were able to gain some valuable insight from the parents who attended.

You'll see a flyer inviting you to come to campus on December 17th, just when we will have our Open House for the High School program. That same afternoon, the residential program has their open house and we thought it'd be a great opportunity to have you see the classrooms and the residential program space and meet the individuals who have worked with your child since August. We hope to get your feedback on future bimonthly gatherings as well—your input on what dates may work best for you will be reviewed during the gathering. If you find that you are unable to come on campus for this gathering and would like to participate remotely, please email me at stella.egbert@tsd.state.tx.us and we will make arrangements with you in ensuring you may be able to participate.

You will also find our action plan based on the feedback from the initial parent forum in October. This action plan is a living document—there is a core team that meets every 4 to 6 weeks to review the plan and continuously modify it as we learn from you, our teachers and staff, and what students have shared and experienced to best respond to this merge and that services for your child continues to be responsive and optimal.

I look forward to continuing this work with you and hope to see you on December 17th,

Stella F Egbert, Director of Instruction

1102 South Congress Avenue Austin, Texas 78704-1728 512 462-5781 FAX 512/462-5620 www.tsd.state.tx.us

Item	**Student Code of Conduct**
Information	The student code of conduct provides information to parents and students regarding standards of conduct, consequences of misconduct, and procedures for administrating discipline. Because the Student Code of Conduct is adopted by the Governing Board, it has the force of policy; therefore, in case of conflict between the code and student handbook, the code will prevail. A high-level overview of the changes to the Code of Conduct will be provided.
Contact	Stella Egbert
Action	Information Only

2019-2020

Texas School for the Deaf
2019-2020

Student Code of Conduct

Texas School for the Deaf

Dear Parent/Guardian/Families:

One of the important priorities for TSD is providing a safe learning environment for all students. In order to help us meet this goal, please read and review the revised and updated 2019-2020 Student Code of Conduct. This Code provides important information for parents/legal guardians and students about the rights and responsibilities of all members of the TSD community. It outlines expectations for student behavior to foster a safe, positive and supportive learning environment.

The formatting of our updated Code of Conduct is new to all of us. The purpose of updating our Code is to ensure we share more about our practices at TSD in terms of supporting all our students. You will find some descriptives of programs we are doing at TSD to support our community. Enclosed is also references to specific policies that the TSD Governing Board has reviewed and approved, which are available for you on our TSD website The Code refers to specific policies that the TSD Governing Board approved, which are all listed in our TSD website (https://www.tsd.state.tx.us/apps/pages/index.jsp?uREC_ID=348273&type=d&pREC_ID=760910).

After you have reviewed this guide with your child, please sign and date the enclosed Acknowledgement of Electronic Distribution of Student Code of Conduct form on page 3. An electronic copy of this Code is available on the TSD website. Please refer to it as needed throughout the school year.

Thank you in advance for your support in helping to make your child's school a safe place for all our school community members,

Stella Egbert
Director of Instruction

Acknowledgement of Electronic Distribution of Student Code of Conduct

Dear Students and Parent(s)/Legal guardian(s):

We know that you share TSD's priority of providing a safe school environment. In order to help us reach this goal we ask you to please read and review this Student Code of Conduct (Code).

In our continued efforts to be as efficient as possible, the TSD website is the primary source for access to the Code. Families who do not have Internet access can receive a copy at their campus upon request at any time during the school year. To ensure that every district student has had the opportunity to access the information contained within the Code, we are requiring that a parent or legal guardian of every student complete the requested information below and return it to your child's teacher and/or the school's administrative team. This form will remain in your child's cumulative folder.

_____ I acknowledge that I can electronically access the TSD Student Code of Conduct.

_____ I acknowledge that I can obtain a paper copy by visiting the administrative office of my child's school. A copy of the Student Code of Conduct will be available through my child's department.

You are responsible for reading the rules, expectations and other information contained herein and signing and returning the attached acknowledgement form. All students will be held accountable for their behavior and will be subject to disciplinary consequences outlined in the Student Code of Conduct. Failure to read the Code does not excuse the student from any consequences if they are in violation of the Code.

Each school year, a paper copy of the Code will be available to you in the administrative office of your child's school. Please visit this office to obtain the most recent copy of the Code.

Student Name: _____Dept: _____Grade: _____

Student Signature:

_____Date: _____

Parent/Legal guardian Signature:

_____Date: _____

Teacher Signature:

_____Date: _____

Table of Contents

Texas School for the Deaf Student Code of Conduct

TSD Mission Statement

Texas School for the Deaf ensures students learn, grow and belong in a language-rich environment while supporting students, families and professionals through statewide outreach services.

In order to achieve this mission, all TSD personnel will demonstrate the attitude and skills to model and support responsible, fulfilling and respectful lives. To ensure that students' learning environment is socially and emotionally safe and free from disruption, each educator is expected to:

- Develop positive relationships in the school community.
- Look for opportunities for proactive intervention before disciplinary action.
- Model courtesy and respect.
- Take a holistic approach to conflict and problem solving.
- Be an active listener.
- Communicate with all pertinent stakeholders.
- Keep equity (see glossary) in mind.

Parents* as Partners

(*Parents includes a person standing in parental relation but does not include a person as to whom the parent-child relationship has been terminated or a person not entitled to possession of or access to a child under court order [Education Code §26.002].)

Students, parents and school personnel all have a role in making schools safe and the benefit of collaborating with one another to achieve this goal. is essential. School staff should keep parents informed of their child's behavior and enlist parents as partners in addressing areas of concern. Outreach to parents can include, but is not limited to, a phone call and/or a written communication. As role models, parents and school staff should exhibit the behaviors that they would like to see students emulate.

Parents must be familiar with the Student Code of Conduct (Code) to ensure that they become active and involved partners in promoting a safe and supportive environment. School officials are responsible for sharing the information in this document with students, parents and staff. Schools are encouraged to provide workshops for parents about understanding the Code and how best to work with the school to support their child's social-emotional growth. Educators are responsible for informing parents about their child's behavior and for nurturing the skills students need to succeed in school and in society. Parents are encouraged to discuss with their child's teacher and other school staff issues that may affect and strategies that may be effective toward student behaviors.

Maximum consultation and communication between the school and the home is important. A variety of conferences (including ARDs) attended by the principal or principal's designee, a guidance counselor, the student's parent(s) and one or more of the student's teachers are an effective means of encouraging parental input and should be held with the student when appropriate. Parents who want to discuss concerns should contact the school.

In the event a student engages in inappropriate behavior, the principal or principal's designee must report the behavior to the student's parent. When a student is believed to have committed a crime the police must be summoned, and the parent must be contacted.

Parents who have questions or concerns about student discipline decisions arising from violations of the code should contact the campus principal or Director of Instruction.

Promoting Positive Student Behavior

School culture and climate have a profound impact on students' academic progress and their relationships with peers and adults. Each school is expected to promote a positive school culture that provides students a supportive environment that helps them grow socially and academically. Student connections to school through opportunities to participate in a wide range of pro-social (see glossary) activities and to bond with caring, supportive adults, coupled with a comprehensive program of prevention and intervention, provides students with the experiences, strategies, life skills and support they need to thrive.

Social-Emotional Learning (SEL) is a basic component of a school's program of universal prevention for all students. Schools are expected to take a proactive role in nurturing students' pro-social behavior. Providing a range of positive behavioral supports as well as meaningful opportunities for SEL fosters resiliency. Effective SEL helps students develop fundamental life skills, including recognizing and managing emotions, developing caring and concern for others, establishing positive relationships, making responsible decisions and constructively and ethically handling challenging situations. When students develop SEL skills, they experience more positive relationships with peers, engage in more positive social behaviors and are less likely to engage in misconduct.

The establishment of a school-wide, tiered framework of behavioral supports and interventions is essential to implementing progressive discipline. The goal of behavioral supports is to foster resiliency, help students understand and follow school rules and support students in developing the skills they need to meet behavioral expectations. School staff members are also responsible for addressing inappropriate student behaviors that disrupt learning.

Administrators, teachers, counselors and other school staff are expected to engage all students in intervention and prevention strategies that address a student's behavioral issues and discuss these strategies with the student and his/her parent(s).

Intervention and prevention strategies include but are not limited to: support and services that address personal and family circumstances; SEL; conflict resolution; peer mediation; collaborative negotiation; restorative circles; anger management; stress management; collaborative problem-solving; communication skills acquisition; the use of alternative instructional materials and/or methods; enrichment services; alternative class placement; development or review of functional behavioral assessments and behavioral intervention plans, which should be developed and/or reviewed as an early

intervention strategy.

Through the use of interventions and prevention strategies that engage students and give them a clear sense of purpose, school staff members facilitate students' academic and social-emotional growth and assist them in following school rules and policies.

Positive Behavior Supports

Understanding discipline as a "teachable moment" is fundamental to a positive approach to discipline. Positive behavior supports uses incremental interventions to address inappropriate behavior with the ultimate goal of teaching pro-social behavior. Positive behavior supports does not seek punishment. Instead, positive behavior supports seeks concurrent accountability and behavioral change.

The goal of positive behavior supports is prevention of a recurrence of negative behavior by helping students learn from their mistakes. Positive behavior supports helps students who have engaged in unacceptable behavior to:

- Understand why the behavior is unacceptable and the harm it has caused; understand what they could have done differently in the same situation;
- Take responsibility for their actions;
- Be given the opportunity to learn pro-social strategies and skills to use in the future; and
- Understand the progression of more stringent consequences if the behavior reoccurs.

Every reasonable effort must be made to correct student behavior through guidance interventions and other school-based strategies such as restorative practices.

Guidance interventions are essential because inappropriate behavior or violations of the Code may be symptomatic of more serious problems experienced by students. School personnel must be sensitive to issues that may influence the behavior of students and respond in a manner that is most supportive of their needs.

Appropriate disciplinary responses should emphasize prevention and effective intervention, foster resiliency, prevent disruption to student's education and promote positive school culture. When a student's misconduct results in a placement out of the classroom, the school should consider using a peer mediation or the restorative circle process as an effective strategy to support a successful return to the student's regular program.

For students whose behavior impedes the student's participation in school, a functional behavior assessment (FBA) is an essential tool to understand the causes of the student's behavior. A behavioral intervention plan (BIP) after an FBA provides specific approaches to address the student's behavior may be developed and reviewed in an ARD.

Addressing the Behavioral Needs of Pre-K Thru Second Grade Children

A student enrolled in a grade level below grade three is prohibited from being placed in out-of-school suspension, unless while on school property or while attending a school-sponsored or school-related activity on or off school property, the student engages in: conduct that contains the elements of an

offense related to weapons (unlawful carrying weapons or prohibited weapons); conduct that contains the elements of a violent offense (assault (see glossary), sexual assault, aggravated assault or aggravated sexual assault); or selling, giving or delivering or another person or possessing, using or being under the influence of: any amount of marihuana or a controlled substance, a dangerous drug, or an alcoholic beverage. [Texas Education Code §37.005]

There is no simple solution to complex student needs. At the core of our response to PK-2 students, we should ask the following questions: What do we see when the student is in front of us? What is the root cause of the behavior? What does the student need?

We do not ask: What is wrong with the student? Instead, we do ask: What is going on with the student?

TSD Strives to ensure that we respond to students' needs through a tiered approach. Having a tiered approach allows us to support our students on all levels, and for those who benefit from tailored and supplemental and/or intensive services beyond Tier 1.

Tier I Prevention

Positive Behavioral Interventions and Supports (PBIS): A broad range of systemic and individualized strategies with emphasis on proactive interventions for promoting, teaching, reinforcing and monitoring positive student behaviors by all adults on campus while preventing problem behavior with all students.

Restorative Practices: A continuum of responsive practices available to a campus to focus on developing a campus culture and climate that supports the needs of each individual student and their family.

Social and Emotional Learning (SEL): A fundamental research-driven approach where students learn critical life skills such as recognizing and managing emotions, solving problems effectively and establishing positive relationships through explicit instruction and adult-modeling. TSD is moving into the next stage of implementation that includes a deep integration of SEL into core teaching and learning in every classroom, maximizing implementation on every campus and ensuring seamless delivery systems of intervention and support.

Trust-Based Relational Interventions (TBRI): TSD is committed to becoming a more trauma-informed campus and learning essential strategies to best support our students through this knowledge. TBRI is a trauma-informed intervention designed to meet the needs of children who have experienced abuse, neglect and/or trauma and students who are not responding to the learning environment.

Tier II Targeted Response

Assessment and Monitoring

- Campus and/or campus reflection questions
- Child Study Team Meeting, Core Meetings, Student Staffing Team
- Conference with parents or legal guardians and campus support personnel
- Development or monitoring of an academic or behavior plan in partnership with the student, teacher, and school personnel
- Restorative circle (with support as needed by district staff)

Supports

- Classroom and peer observations from campus administration by specific personnel to offer reflection and support
- Counseling with school counselor or by service provider (based on capacity)
- Development of a classroom calming areas if age approrpiate
- Development of a campus SEL program
- Support for families in terms of external referrals to community based resources to support students and families further

Tier III Intensive Response

Assessment and Monitoring

- Consistent mointoring in support plan within a Student Staffing Team and Additional and Comprehensive Support Services

Supports

- Additional resources provided within the school system as agreed in the ARD, such as behavior support, counseling, and other related service needs
- Referral to community partners and service providers

Summary

This Student Code of Conduct (Code), reviewed and approved by the TSD Governing Board, provides information and direction to students and parents regarding behavioral expectations and consequences for code of conduct violations. Parents/legal guardians and students are encouraged to read and regularly review the district's Code to ensure a successful and productive school year for all.

The district has the authority to handle discipline and give consequences when:

- The interest of the school is involved on or off school grounds in conjunction with or independent of classes and school-sponsored activities.
- Students violate the code of conduct during the school day while attending or participating in a school-related or school-sponsored activity, including in any vehicle owned by the district.
- Students post threatening messages on social media towards another student, staff or district property, regardless of time or location.
- Students engage in specific criminal activity, as determined by law enforcement, regardless of time or location.

Determining consequences:

- As required by law, our Special Education Director, Elizabeth Sterling, will serve as the District Behavior Coordinator (DBC). The DBC is primarily responsible for maintaining student discipline policies and procedures. The department principals and administrative teams will determine appropriate consequences based on these policies and procedures.
- Before the DBC and department administration recommend a suspension or the student's removal to an alternative school setting, they must consider:
    - If the student acted in self-defense;
    - The student's intent or lack of intent at the time the student engaged in the conduct;
    - The student's disciplinary history;
    - Whether the student has a disability that substantially impairs the student's capacity to appreciate the wrongfulness of their conduct, regardless of whether the decision involves a mandatory or discretionary action.
    - A student's status in the conservatorship of the Department of Family and Protective Services or a student's status as a student who is homeless.
- The DBC and department administration can offer students the following options to restore order, help students with their social and emotional development and keep students engaged with their academic progress at their home campus:
    - Parent/teacher conference;
    - Conflict resolution;
    - Classroom circles (used to establish a respect agreement, build school community, repair harm and teach decision-making strategies and/or content);
    - Behavior coaching;
    - Behavior improvement plan;
    - Referral to the school's student support team;
    - Referral to social services in the community;

    - Transfer student to another classroom;
    - In School Suspension or Out-of-School Suspensions.

- The district may recommend a student to obtain alternative education services for serious or persistent misconduct or when the student breaks local or state law:
    - Students have the right to participate in a due-process conference before they are removed from their regular school setting.
    - Students can be removed to a district alternative education program (DAEP).
    - Students may not be allowed to attend or participate in any extracurricular activities.

Purpose

The Code is the district's specific response to requirements of Chapter 37: Discipline; Law and Order of the Texas Education Code.

The Code provides clear guidance and reliable information to students, parents and staff, so everyone knows what to expect if disciplinary issues arise. This Code also aligns with TSD's goals and philosophy of respect, success, prevention, guidance and early intervention.

The law requires the district to define misconduct that may or must result in a range of specific disciplinary consequences.

Rules of conduct and discipline shall not have the effect of discriminating on the basis of race, color, religion, gender, gender identity, gender expression, sexual orientation, national origin, disability, age, immigration status, or any other basis prohibited by law.

This Code is an outgrowth of collaboration among district, campus staff, parents and other community members. This Code, adopted by the TSD Governing Board, provides information and direction to students and parents regarding standards of behavior as well as consequences of misconduct. In the case of conflict between the Code and board policy, the Code will prevail.

References are made throughout this document to Chapter 37 of the Texas Education Code (TEC), which governs various aspects of the Code. TEC and AISD policies, regulations and exhibits concerning discipline and behavior management can be accessed on-line:

TEC: http://www.statutes.legis.state.tx.us/?link=ED

TSD policies, regulations, and exhibits: https://www.tsd.state.tx.us/apps/pages/index.jsp?uREC_ID=348273&type=d&pREC_ID=889409

I. Expectations for Student Behavior

In order to achieve TSD's mission, all students will demonstrate the attitude and skills to lead responsible, fulfilling and respectful lives; all students will understand the components of a healthy lifestyle. To ensure that students learn in a psychologically-, physically- and emotionally safe environment free from disruption, each student is expected to:

- Demonstrate courtesy and respect for others;
- Behave responsibly;
- Attend all classes regularly and on time;
- Avoid Code violations;
- Prepare for each class and take appropriate materials and assignments to class;
- Cooperate with or assist the school staff in maintaining safety, order and discipline;
- Be well-groomed and dress appropriately according to district or campus dress code;
- Respect the property of others, including district property and facilities;
- Respect the rights and privileges of other students, teachers and other district staff.

A student whose behavior shows disrespect for others, including interference with a person's access to a public education and/or a safe environment, will be subject to disciplinary action. The district or individual schools may impose campus or classroom rules in addition to those found in the Code. These

rules may be listed in the campus student handbooks or posted in classrooms and may or may not constitute violations of the Code.

In general, discipline will be designed to correct the misconduct and to encourage all students to adhere to their responsibilities as citizens of the school community. Disciplinary action and the length of the assignment will draw on the professional judgement of teachers and administrators and on a range of discipline management techniques. Disciplinary action will be related to, but not limited to, the seriousness of the offense, the student's age and grade level, the frequency of misbehavior, the student's attitude, whether the student was acting in self-defense, the effect of the misconduct on the school environment, intent or lack of intent at the time the student engaged in the conduct, whether a student has a disability that substantially impairs the student's capacity to appreciate the wrongfulness of their conduct (as required by law, IDEA, 504), and a student's status in the conservatorship of the Department of Family and Protective Services or a student's status as a student who is homeless. Because of these factors, varying techniques and responses may be considered for discipline for a particular offense (unless otherwise specified by law).

The following techniques may be used alone or in combination for Code and non-Code violations, such as campus or classroom rules:

- Verbal correction;
- Cooling-off time;
- Seating changes in the classroom or in vehicles owned or operated by the district;
- Counseling by teachers, counselors or administrative personnel;
- Parent-teacher conferences;
- Confiscation of items that disrupt the educational process;
- Behavioral contracts;
- Sending the student to the office or other assigned area, or to Student Support Centers (in-school suspension);
- Assignment to another classroom;
- Detention;
- Restriction or revocation of bus district transportation privileges;
- Assigned school duties other than class tasks;
- Withdrawal of privileges, such as participation in extracurricular activities and eligibility to seek and hold honorary offices;
- Techniques or penalties identified in individual student organizations' codes of conduct;
- School-assessed and school-administered probation;
- Grade reductions for cheating, plagiarism and as otherwise permitted by policy;
- Referral to an outside agency and/or legal authority for criminal prosecution in addition to disciplinary measures imposed by the district;
- Other strategies and consequences as specified by the Code or deemed appropriate by the campus administrators, such as suspension, removal or expulsion.

Note: Corporal punishment is not permitted at TSD.

When disciplinary consequences require a conference or ARD meeting, the DBC or principal will make valid attempts to inform the student and the student's parent or legal guardian of the time and place of the conference. The district may hold the meeting if attempts to schedule it has been fulfilled.

Discipline Authority

School rules and the district's authority to administer discipline apply whenever the interest of the school is involved on or off school grounds in conjunction with or independent of classes and school-sponsored activities. The district has disciplinary authority over a student:

- During the regular school day, when the student is within 300 feet of the school's real property boundary line, and while the student is going to and from school on district transportation.
- During lunch periods in which a student is allowed to leave campus.
- While the student is in attendance at any school-related activity, including summer school, regardless of time or location.
- For any school-related misconduct, regardless of time or location.
- When criminal mischief is committed on or off school property or at a school-related event.
- When retaliation against a school employee or volunteer occurs or is threatened, regardless of time or location.
- When the student commits a felony offense in the community, as provided by the Texas Education Code.
- Pursuant to any code of conduct adopted at the campus level relating to participation in a student club, organization or extracurricular activity.
- When the student is required to register as a sex offender.

Note: In addition to disciplinary consequences, misdemeanor and felony offenses committed on campus will be reported to and handled by the appropriate law enforcement agency. Please see district policy FNF for information on searches.

District Behavior Coordinator (DBC)

As required by law, a person at each district must be designated to serve as the DBC. This person may be the principal of the campus or any other campus administrator selected by the principal. The DBC is primarily responsible for maintaining student discipline. TSD's DBC is Elizabeth Sterling, our Special Education Director. Department Principals work with Ms. Sterling in supporting our district behavior program.

Due Process

A student will be afforded due process consistent with this Code and state law before a decision is made to suspend a student from school or remove a student to the District Alternative Education Program (DAEP). Although this Code describes in detail the specific procedures applicable to disciplinary consequences, these general provisions apply any time a student is removed from a class or school setting for disciplinary reasons. The student will be given a notice of the allegations against them. If the student denies those allegations, school officials will provide an explanation specifying the reasons they believe misconduct has occurred. The student will be offered to present their side of the story.

No later than the third-class day after the day on which a teacher or campus administrator removed the student from class, the DBC shall schedule a conference with the campus administrator, a parent or legal guardian of the student, the teacher who removed the student from class (if applicable) and the student.

At the conference, the student will receive an explanation of the reasons for their removal and will have an opportunity to respond. The student may not return to their regular classroom pending this conference. The DBC or department administrative team will make good-faith attempts to invite the parent and student to the removal conference but may proceed with the disciplinary placement regardless of whether the student and parent are in attendance.

Before ordering a student's suspension, removal to DAEP, the DBC and the department administrative team will consider whether mitigating factors exist; that is, whether the student acted in self-defense, the intent or lack thereof at the time the student engaged in the misconduct, the student's disciplinary history, whether the student has a disability that substantially impairs the student's capacity to appreciate the wrongfulness of the student's conduct, and a student's status in the conservatorship of the Department of Family and Protective Services or a student's status as a student who is homeless.

Following the conference, the DBC or department administration will provide the parent or legal guardian with written notice of the hearing's outcome, consistent with the appropriate provisions of the Code.

II. General Misconduct

A. Definition of General Misconduct

General misconduct is unacceptable or improper behavior of a student; that is, not following the policies of TSD, state laws and/or the Code.

At school, in vehicles owned or operated by the district and at all school-related activities, prohibited conduct and items include, but are not limited to, the following:

General Violations or Rules/Miscellaneous

- Cheating or copying another person's work.
- Violating the district or campus dress code.
- Inappropriate discharge of a fire extinguisher.
- Violating safety rules.
- Disobeying rules for conduct on school buses.
- Repeatedly violating communicated campus or classroom standards of behavior.
- Failure to comply with directives given by school personnel.
- Behaving in any way that disrupts the school environment or educational process.
- Leaving school grounds or school-sponsored events without permission.
- Damaging or vandalizing property owned by others.
- Defacing or damaging school property—including textbooks, lockers, furniture and other equipment—with graffiti (see glossary) or by other means.
- Falsification of paper or computer records, passes or other school related documents.

- Gambling.
- Stealing, theft or robbery.
- Engaging in conduct that constitutes criminal mischief.
- Engaging in any behavior that gives school officials reasonable cause to believe that such conduct will substantially disrupt the school program or incite violence.
- Violating any local, state or federal laws.
- Inappropriate Physical or Verbal Conduct, committing extortion, coercion or blackmail (obtaining money or another object of value from an unwilling person) or forcing an individual to act through use of force or threat of force.
- Recording the voice or image of another person(s) without that person(s)'s prior consent to be recorded or recording in any way that disrupts the educational environment or invades the privacy of others.
- Use of profanity, vulgar language or obscene gestures.
- Name-calling, using ethnic or racial slurs or giving derogatory statements that school officials have reason to believe will disrupt the school program or incite violence.
- Engaging in conduct that constitutes sexual- or gender-based harassment or sexual abuse, whether by word, gesture or any other sexual conduct, including request for sexual favors.
- Engaging in inappropriate physical or sexual contact.
- Harassment (see glossary).
- Dating violence (see glossary).
- Bullying (see glossary).
- Cyberbullying (see glossary).
- Hazing (see glossary).
- Throwing objects that can cause bodily injury or property damage.
- Fighting.
- Aggressive, disruptive actions or group demonstrations that substantially disrupt or materially interfere with school activities.
- Making false accusations or perpetuating hoaxes regarding school safety.
- Engaging in threatening behavior toward another student or district employee or property, including creating a hit list, defined as a list of people targeted to be harmed, using a firearm (see glossary), a knife, or any other object with the intent to cause bodily harm.
- Engaging in Assassin, or any other organized mock killing or elimination game which involves but is not limited to carrying out strikes, kills or hit lists, regardless of method (for example, toy guns or markers).

Threats

The District takes all threats seriously. Threats of any nature are taken seriously and investigated to the full extent allowable by law and district policy. Threats of any kind against a school, students or staff are not tolerated. All school threats are investigated by school officials and law enforcement.

Threats that result in evacuations, lockdowns, investigations by an official or agency organized to deal with emergencies, will result in the application of discipline policy. Any disciplinary action taken will be in accordance with TEC Chapter 37 and federal and state laws regarding students with disabilities, and the Student Code of Conduct. Please emphasize to your children that all such threats—made verbally or over any social media channel—are investigated immediately. Students may be detained or arrested on a charge of making a terroristic threat, even if the threat is not credible.

Harassment and Bullying

The district believes that all students learn best in an environment free from dating violence, discrimination, harassment and retaliation and that their welfare is best served when they are free from this prohibited conduct while attending school. Students are expected to treat other students and district employees with courtesy and respect, to avoid behaviors known to be offensive and to stop those behaviors when asked or told to stop. District employees are expected to treat students with courtesy and respect.

The board has established policies and procedures to prohibit and promptly respond to inappropriate and offensive behaviors that are based on a person's race, color, religion, sex, gender, gender identity, gender expression, sexual orientation, national origin, disability, age, immigration status or any other basis prohibited by law. [See policy FFH.]

Upon receiving a report of prohibited conduct as defined by policy FFH, the district will determine whether the allegations, if proven, would constitute prohibited conduct as defined by that policy. If not, the district will refer to policy FFI to determine if the allegations, if proven, would constitute bullying, as defined by law and that policy. If the alleged prohibited conduct, if proven, would constitute prohibited conduct and would also be considered bullying as defined by law and policy FFI, an investigation of bullying will also be conducted.

To the extent possible, the district will respect the privacy of the student; however, limited disclosures may be necessary to conduct a thorough investigation and to comply with law. Allegations of prohibited conduct, which includes dating violence, discrimination, harassment and retaliation, will be promptly investigated.

During the investigation and when appropriate, the district will take interim action to address the alleged prohibited conduct.

If the district's investigation indicates that prohibited conduct occurred, appropriate disciplinary action and, in some cases, corrective action will be taken to address the conduct. The district may take disciplinary and corrective action even if the conduct that is the subject of the complaint was not unlawful.

David's Law and Discipline

A student may be removed from class and placed in a disciplinary alternative education program or expelled (Section 37.0052) if the student engages in "Bullying" or "Cyberbullying" as defined in Section 37.0832 that encourages a student to commit or attempt to commit suicide; or incites violence against a student through group bullying; or releases or threatens to release intimate visual material of a minor or student who is 18 years of age or older without the student's consent.

Schools have authority to apply discipline for bullying that occurs on or is delivered to school property or to the site of a school-sponsored or school-related activity on or off school property; bullying that occurs on a publicly or privately owned school bus or vehicle being used for transportation of students to or from school or a school-sponsored or school-related activity; and cyberbullying that occurs off school property or outside of a school-sponsored or school-related activity if the cyberbullying: interferes with a student's educational opportunities; or substantially disrupts the orderly operation of a classroom, school, or school-sponsored or school-related activity.

Prohibited Items to Distribute, Possess, Sell or Use

- Pornographic materials.
- Published or electronic material designed to promote or encourage illegal behavior or that could threaten school safety; this includes e-mail or Web sites used at school to encourage illegal behavior or threaten school safety.
- Glue or aerosol paint containing volatile chemicals and/or able to be abused.
- Alcoholic beverages (includes consumption before arriving at or while on school premises); committing a serious act or offense while under the influence of alcohol.
- Medicine available without a prescription in a manner inconsistent either with the medicine's intended use as indicated on the manufacturer's labeling or with district policy concerning the handling of such medicines.
- Prescription or over-the-counter drugs taken in violation.
- A student's own prescription drugs when given to another student or possessing or being under the influence of another person's prescription drug.
- Drug paraphernalia.
- Look-alike drugs or items imitating or mimicking drugs and contraband.
- Matches or lighters.
- Tobacco products, including cigarettes, cigars, cigarillos, dissolvable tobacco products, traditional smokeless tobacco products including chewing tobacco and moist snuff
- Vape products, including electronic cigarettes (e-cigarettes) (see glossary), electronic vaping devices, personal vaporizers (PV) or electronic nicotine delivery systems, their accessories, and e-liquids.
- Selling, giving, delivering, possessing, using or being under the influence of any amount of marihuana or a controlled substance, or a dangerous drug.
- Any articles generally not considered weapons, including school supplies, when the principal or designee determines that a danger exists.
- Razors, box cutters, chains or other objects used in a way that threatens or inflicts bodily injury to another person.

- Knives, bladed instruments, switchblade knives, air guns, toy guns, chemical dispensing devices (see glossary), mace/pepper spray, fireworks, replica firearms, electronic stunning devices, ammunition and other dangerous items.
- A firearm (see glossary); a machine gun; a short-barrel firearm; a firearm silencer; armor-piercing ammunition; a zip gun; a location-restricted knife, defined as a knife with a blade over five-and-a-half inches; a butterfly knife; a club (see glossary); a prohibited weapon, such as an explosive weapon (see glossary); knuckles.
- Any item, other than those defined as firearms (see glossary) under state and federal, capable of propelling a projectile and causing injury by any means including, but not limited to, spring, compressed air, spring-piston, pneumatic or CO2. Examples include, but are not limited to, BB guns, Airsoft guns, pellet guns and any protective device designed to administer an electric shock.
- Possessing a homemade weapon, defined as a device or item that was manufactured, modified or adapted by an individual for the use or intended use of inflicting harm on another person.

Note that possession and use of paging devices or cellular telephones must be in accordance with District and campus policy.

Inappropriate Use of Computer/Internet/Email

- Violating policies, rules, or any agreements signed by the student or the student's parent regarding the use of technology resources [TSD Acceptable Use Policy].
- Attempting to access or circumvent passwords or other security-related information of the district, students or employees or uploading or creating computer viruses, either on or off school property, if the conduct causes a substantial disruption to the educational environment.
- Attempting to alter, destroy or disable district technology resources, including but not limited to computers and related equipment, district data, the data of others or other networks connected to the district's system, either on or off school property, if the conduct causes a substantial disruption to the educational environment.
- Using email or websites to engage in or encourage illegal behavior or threaten school safety, including off property if the conduct causes a substantial disruption to the educational process.
- Sending, posting, or possessing electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including cyberbullying (see glossary) and "sexting," either on or off school property if the conduct causes a substantial disruption to the educational environment.

B. Consequences for General Misconduct

Students who engage in general misconduct as defined in Part A will be disciplined. Students will be disciplined via appropriate discipline management techniques; removal from the regular classroom environment and/or placement in a Disciplinary Alternative Education Program (DAEP).

Notification

The DBC or Department Administration shall promptly notify a student's parent by phone or in person of any violation that may result an in-school suspension or out-of-school suspension. Placement in a DAEP will require an ARD meeting. The DBC or Department Administration shall also notify a student's parent if a law enforcement officer takes custody of a student under the disciplinary provisions of the education code. A good faith effort shall be made on the day the action was taken to give the student written notification of the disciplinary action to deliver to the student's parent/legal guardian. If the parent is unable to be reached by telephone or in person by 5:00 p.m. of the first business day after the day of the disciplinary action, the DBC shall send written notification by U.S. Mail. If the DBC is unable to provide notice to the parent, the principal or designee shall provide the notice.

Removal from the School Bus

Since the district's primary responsibility when transporting students in district vehicles is to do so as safely as possible, the operator of the vehicle must focus on driving and not have their attention distracted by student misbehavior. Therefore, when appropriate disciplinary management techniques fail to improve student behavior or when specific misconduct warrants immediate removal, the bus driver may refer a student to the principal's office to maintain effective discipline on the bus. The principal must employ additional discipline management techniques, as appropriate. If concerns arise regarding riding the bus safely, an ARD would be conducted.

Removal By Teacher [TEC 37.002(B) (D)]

A teacher also has the authority to remove a student. A teacher may remove from class a student who has been documented by the teacher to repeatedly interfere with the teacher's ability to communicate effectively with the students in the class or with the ability of the student's classmates to learn; or whose behavior the teacher determines is so unruly, disruptive or abusive that it seriously interferes with the teacher's ability to communicate effectively with the students in the class or with the ability of the student's classmates to learn [TEC 37.002 (b)]. A teacher or administrator may also remove a student from class for an offense for which a student may be suspended and/or placed in a Disciplinary Alternative Education Program [TEC 37.002 (d)]. If the following offenses are committed against the teacher, the student may not be returned to the class without the teacher's consent: assault with bodily injury, aggravated assault, sexual assault, or aggravated sexual assault. The principal or appropriate administrator must send a copy of the teacher's documentation or of the Code of Conduct violation to the student's parent or legal guardian within 24 hours of receiving it.

Conference

When a student is removed from the regular classroom, a conference will be scheduled within three school days with the student's parent/legal guardian, the teacher and the student. It is our goal to ensure we restoratively approach issues when they surface. Pending the conference, the principal or other appropriate administrator may place a student in:

- Another appropriate classroom.
- In School Suspension.
- A Disciplinary Alternative Education Program.
- Out-of-school suspension.

After the conference, the principal will notify the student and parent(s) of the consequences for the Code violation. When a student has been formally removed from class [TEC 37.002], the principal or other administrator may not return the student to the teacher's class without the appropriate teacher's consent unless the Administrative Team or ARD committee makes recommendations.

Suspension [TEC 37.005]

Students may be suspended for any behavior listed in the Code as a general misconduct violation, Disciplinary Alternative Education Program placement or expellable offense. In addition, suspensions may be used for students who have committed a removal or expulsion offense and for whom a conference or hearing is pending. State law allows a student to be suspended from school for up to three school days per offense. Students who have 10 or more days in cumulation would require an ARD.

The administrator will take into consideration any mitigating factors that may apply, including whether the student acted in self-defense, the intent or lack of intent at the time the student engaged in the conduct, the student's disciplinary history, whether the student has a disability that substantially impairs the student's capacity to appreciate the wrongfulness of the student's conduct, and a student's status in the conservatorship of the Department of Family and Protective Services or a student's status as a student who is homeless. The principal or other appropriate administrator will determine the suspension duration. Any restrictions on participation in school-sponsored or school-related extracurricular and noncurricular activities will be determined by the principal or other appropriate administrator. A student may appeal the decision of the DBC to the campus principal or designee. The student will remain on suspension pending any appeal. The campus principal's decision cannot be appealed.

No elementary student enrolled in a grade level below grade three shall be placed in out-of-school suspension, unless while on school property or while attending a school-sponsored or school-related activity on or off school property, the student engaged in: conduct that contains the elements of an offense related to weapons (unlawful carrying weapons or prohibited weapons); conduct that contains the elements of a violent offense (assault [see glossary], sexual assault, aggravated assault or aggravated sexual assault); or selling, giving or delivering to another person or possessing, using or being under the influence of any amount of marijuana or a controlled substance, a dangerous drug or an alcoholic beverage [TEC Section 37.005].

No student who is homeless may be placed in out-of-school suspension unless while on school property or while attending a school-sponsored or school-related activity on or off school property, the student engaged in: conduct that contains the elements of an offense related to weapons (unlawful carrying weapons or prohibited weapons); conduct that contains the elements of a violent offense (assault [see glossary], sexual assault, aggravated assault or aggravated sexual assault); or selling, giving or delivering to another person or possessing, using or being under the influence of any amount of marijuana or a controlled substance, a dangerous drug or an alcoholic beverage [TEC Section 37.005].

Disciplinary Alternative Education Program (DAEP)

A. Behavior Subject to Removal to a DAEP

Mandatory Removals

A student must be placed in a Disciplinary Alternative Education Program if the student commits any of the following offenses on school property, including a parking lot, parking garage or other parking area owned by the school district; on a school bus; within 300 feet of the school's real property line; while attending a school-sponsored or school-related activity on or off school property [TEC Section 37.005], and determined in an ARD meeting:

- Engaging in conduct punishable as a felony.
- Committing an assault with injury.
- Selling, giving, delivering, possessing, using or being under the influence of any amount of marijuana or a controlled substance or a dangerous drug, in an amount not constituting a felony offense.
- Selling, giving or delivering an alcoholic beverage; committing a serious act or offense while under the influence of alcohol.
- Possessing, using, or being under the influence of an alcoholic beverage.
- Behaving in a manner that contains the elements of an offense: relating to the abuse of glue or aerosol paint or relating to volatile chemicals; of public lewdness; of the offense of indecent exposure.
- Engaging in conduct that contains the elements of the offense of harassment under Section 42.07(a)(1), (2), (3), or (7), Penal Code, against an employee of the school district.

In addition, a student must be placed in a DAEP if the student:

- Engages in conduct that contains the elements of the offense of retaliation against any school employee, regardless of where or when the conduct occurs. (
- Engages in "Bullying" as defined in Section 37.0832 that encourages a student to commit or attempt to commit suicide; or incites violence against a student through group bullying; or releases or threatens to release intimate visual material of a minor or student who is 18 years of age or older without the student's consent.
- Makes a terroristic threat; false alarm or report (see glossary) (e.g., bomb threats).

Texas School for the Deaf is not intended to serve: students whose needs are appropriately addressed in a home or hospital setting or a residential treatment facility; or students whose primary, ongoing needs are related to a severe or profound emotional, behavioral, or cognitive deficit. Tex. Educ. Code § 30.051(a) Students will be referred back to their Local Education Agency (LEA) to continue to receive services for conduct resulting in: a) an expulsion; b) being declared delinquent or in need of supervision and is on probation or other conditional release for that conduct; or c) conviction of a criminal offense and is on probation or other conditional release. Texas Education Code 25.001(d).

Students who do not meet the statutory criteria above quoted for receiving services at the School will not be eligible for continued enrollment when the definitions in this policy are applied to the relevant information. If the School determines that a prospective student is ruled ineligible to attend the School, the School can provide resources to the family or the local education agency (LEA) upon request [FD].

A student under 10 years of age who engages in expellable conduct described in Section 37.007 shall receive educational services in the district's DAEP. A student under the age of six may not be removed to a DAEP (as described in 37.008) unless they commit a federal firearms offense.

Discretionary Removals

A student may also be removed from class and placed in a DAEP under Section 37.008 based on conduct occurring off campus and while the student is not in attendance at a school-sponsored or school-related activity if:

- The continued presence of the student in the regular classroom threatens the safety of other students or teachers or will be detrimental to the educational process.

In addition, students may be removed from class and placed in a DAEP who are found to be:

- Involved in a public-school fraternity, sorority, secret society or a gang, including participating as a member or pledge or soliciting another person to become a pledge or member of such a group.
- Involved in criminal street gang activity (see glossary)

A student **may** also be removed to a DAEP for serious or persistent misbehavior. The district defines "persistent" to be two or more violations of the Code or repeated occurrence of the same violation. A student may be removed for persistent misbehavior if behavioral interventions have not been successful and removal to a DAEP is deemed necessary to improve the student's behavior. The district defines "serious" offenses as offenses that pose a physical danger to the student or others or to property. An ARD meeting will be conducted.

B. Removal to a DAEP

The board delegates to the principal the authority to remove a student to a DAEP in which the student will be separated from other students for the entire school program day and will be provided instruction in the core subjects with the goal of reaching/maintaining grade level. Counseling will also be provided to the student. The duration of a student's placement in a DAEP will be determined on a case-by-case basis. The maximum period of a DAEP placement is 45 days.

Teacher/Administrator Removal [TEC 37.006]

A teacher shall remove a student from class and send the student to the principal or other appropriate administrator if the student engages in an offense specified under TEC 37.006 (http://www.statutes.legis.state.tx.us/Docs/ED/htm/ED.37.htm#37.006). When a violation of TEC 37.006 is alleged, the principal or other appropriate administrator will schedule a conference with the student's parent, teacher (if appropriate) and the student within three school days of receiving the violation report. The campus administrator will make a good-faith effort to schedule the hearing in collaboration with the student's parent but may proceed with the hearing in absence of the parent if the parent does not attend the conference after a valid effort is made to secure the parent's attendance.

Until a conference can be held as a result of a teacher removal or administrator removal, the principal or other appropriate administrator may place a student in:

- Another appropriate classroom.
- In School Suspension.
- A DAEP.
- Out-of-school suspension.

Due process will be afforded at the conference or ARD The principal or other appropriate administrator will explain the allegations against the student and give the student an opportunity to explain the student's version of the incident. Before ordering placement of the student in a DAEP, the Campus administrator will consider the following mitigating factors: whether the student acted in self-defense, the intent or lack of intent at the time the student engaged in the misconduct, the student's disciplinary history, and whether the student has a disability that substantially impairs the student's capacity to appreciate the wrongfulness of the student's conduct. After the conference, if the student is placed in the DAEP, a written placement order shall be provided to the student and the parent, together with notice of the right to appeal the removal. The order will include notice of the school district's obligation to provide the student with the opportunity to complete coursework required for graduation at no expense to the student.

If the student's placement in a DAEP is inconsistent with the district's placement guidelines as set forth in this Code, the order must give notice of the inconsistency.

Participation in Activities

The district does not permit a student who is placed in a DAEP to participate in any school-sponsored or school-related extracurricular or co-curricular activity, including seeking or holding honorary positions and/or membership in school-sponsored clubs or organizations.
Please see district policy FMH concerning removals for graduating seniors and participation in commencement activities.

Emergency Placement in DAEP [Section 37.019]

In situations that the principal or an appropriate administrator consider to be emergencies, the principal may order the immediate placement of a student when a student is so unruly, disruptive or abusive that the student's presence seriously interferes with the teacher's ability to communicate effectively with the students in a class, the ability of the student's classmates to learn, or the operation of school or a school-sponsored or a school-related activity. As required by law, the student will be given the appropriate conference required for DAEP placement within ten days.

Admission of Removed Students

The district will decide on a case-by-case basis the placement of a student who enrolls in the district having been assigned to the DAEP in another district, including a district in another state or an open-enrollment charter school. The district may place the student in the district's DAEP or a regular classroom setting.

III. Placement and/or Expulsion for Certain Serious Offenses

This section includes two categories of serious offenses for which the Texas Education Code provides unique procedures and requires specific consequences.

A. Registered Sex Offenders

Upon receipt of notification in accordance with state law that a student is currently required to register as a sex offender, the administration must remove the student and the student will be referred back to their home district where they can continue to receive all of their IEP services.

If the student is under any form of court supervision, including probation, community supervision or parole, the placement will be in DAEP.

The placement may not be in the regular classroom if the board or the associate superintendent or associate superintendent's designee determines that the student's presence:

- Threatens the safety of other students or teachers.
- Will be detrimental to the educational process.
- Is not in the best interest of the district's students.

Review Committee

At the end of the first semester of a student's placement in a DAEP and before the beginning of each school year for which the student remains in an alternative placement, the district shall convene a committee, in accordance with state law, to review the student's placement. The committee, whose membership will include the Director of Instruction, Special Education Director or designee, will recommend whether the student should return to the regular classroom or remain in placement.

The Admission, Review and Dismissal (ARD) committee must review placement of a student with a disability who receives special education services.

B. Certain Felonies

Regardless of whether placement or expulsion is required or permitted due to one of the reasons in the DAEP or Expulsions sections, in accordance with Texas Education Code 37.0081, a student may be expelled and placed in either a DAEP if the board or its designee, the Director of Instruction or Special Education Directior, makes certain findings and the following circumstances exist in relation to aggravated robbery or a felony offense under Title V of the Texas Penal Code. The student must have:

- Received deferred prosecution (see glossary) for conduct defined as aggravated robbery or a Title V Felony Offense;
- Been found by a court or jury to have engaged in delinquent conduct (see glossary) for conduct defined as aggravated robbery or a Title V felony offense;
- Been charged with engaging in conduct defined as aggravated robbery or a Title V offense;
- Been referred to a juvenile court for allegedly engaging in delinquent conduct for conduct defined as aggravated robbery or a Title V offense;
- Received probation or deferred adjudication (see glossary) or been arrested for, charged with or convicted of aggravated robbery or a Title V felony offense.

IV. Expulsion

A. Offenses Subject to Expulsion [Tec 37.007 and 37.125]

Mandatory Expulsions

A student **must** be expelled for any following offense if committed on school property, including a parking lot, parking garage, or other parking area owned by the school district, on a school bus or while attending a school-sponsored or school-related activity on or off school property:

- Bringing to school a firearm, as defined by federal law as:
    - Any weapon (including a starter gun), which will or is designed to or which may readily be converted to expel a projectile by the action of an explosive.
    - The frame or receiver of any such weapon.
    - Any firearm muffler or silencer.
    - Any destructive device, such as any explosive, incendiary or poison gas bomb or grenade.
- Use, exhibition or possession of the following, under the Texas Penal Code:
    - A firearm (defined as any device designed, made or adapted to expel a projectile through a barrel by using the energy generated by an explosion or burning substance or any device readily convertible to that use).
    - A location-restricted knife, defined as a knife with a blade over five-and-a-half inches.
    - A prohibited weapon, such as an explosive weapon (see glossary); a machine gun; a short-barrel firearm; a firearm silencer; armor-piercing ammunition; a zip gun; or a tire deflation device.
- Behavior containing the elements of the following under Texas Penal Code:
    - Aggravated assault, sexual assault or aggravated sexual assault.
    - Aggravated kidnapping.
    - Aggravated robbery.
    - Arson (see glossary).
    - Behavior punishable as a felony that involves being under the influence of, possession or use of, or the selling, giving or delivering to another person: any amount of marihuana or a controlled substance, a dangerous drug, or alcohol; or committing a serious act while under the influence of alcohol.
    - Continuous sexual abuse of a young child or children.
    - Indecency with a child.
    - Murder, capital murder or criminal attempt to commit murder or capital murder; manslaughter; or criminally negligent homicide. Retaliation against a school employee combined with one of the above-listed offenses on or off school property or at a school-related activity.

Discretionary Expulsions

Offenses Engaged in at Any Location

A student may be expelled for:

- Engaging in conduct that contains the elements of an offense under Section 22.01 of the Penal Code (assault with injury is when a person intentionally, knowingly or recklessly causes bodily injury to another, including the person's spouse) in retaliation against a school district employee or volunteer.
- Engaging in bullying as defined in Section 37.0832 that encourages a student to commit or attempt to commit suicide; or inciting violence against a student through group bullying; or releasing or threatening to release intimate visual material of a minor or student who is 18 years of age or older without the student's consent.
- Engaging in criminal mischief if punishable as a felony.
- Making a terroristic threat, false alarm or report (see glossary) (e.g., bomb threats) involving a public school.
- Engaging in conduct that contains the elements of offense of breach of computer security under section 33.02 of the Penal Code, if the conduct involves accessing a computer, computer network or computer system owned by or operated on behalf of a school district, and knowingly altering, damaging, deleting school district property or information, or committing a breach of any other computer, computer network or computer system [Chapter 37.007 (b)(5)].
- Engaging in conduct that contains the elements of one of the following offenses against another student, without regard to where the conduct occurs:
    - Aggravated assault, sexual assault or aggravated sexual assault.
    - Murder or capital murder.
    - Criminal attempt to commit murder or capital murder.

Offenses Engaged in at School, Within 300 Feet of School or at a School Event

A student may be expelled for:

- Engaging in any of the following offenses if committed on school property or within 300 feet of the school's real property line, or while attending a school-sponsored or school-related activity on or off school property:
    - Conduct that contains the elements of an offense under Section 22.01 of the Penal Code (assault with injury is when a person intentionally, knowingly or recklessly causes bodily injury to another, including the person's spouse) against a school district employee or volunteer.
    - Conduct that contains the elements of the offense of deadly conduct (see glossary) under Section 22.05 of the Penal Code.
- Engaging in any following offense if committed within 300 feet of the school's real property boundary line:
    - Aggravated assault, sexual assault or aggravated sexual assault.

- Arson (see glossary).
- Continuous sexual abuse of a young child or children.
- Felony drug or alcohol related offense.
- Indecency with a child, aggravated kidnapping, manslaughter, criminally negligent homicide or aggravated robbery.
- Murder, capital murder, or criminal attempt to commit murder or capital murder.
- Use, exhibition, or possession of a firearm (see glossary), a location-restricted knife, or prohibited weapon.

In addition, a student may be expelled for any offense that is a state-mandated expellable offense if the offense is committed on the property of another Texas school district in Texas or while the student is attending a school-sponsored or school-related activity at another Texas school district.

A student may be expelled for serious misbehavior if a student is already in a DAEP and continues to violate the district's Code despite documented interventions at the DAEP.

B. Expulsion Procedures [TEC 37.007]

The board delegates the authority to expel students to the superintendent or the superintendent's designee. A student under the age of six may not be removed to a DAEP (as described in 37.008) unless they commit a federal firearms offense. The duration of a student's expulsion will be determined in a case-by-case basis. The maximum period for an expulsion is a calendar year unless it is determined that the student is a threat to the safety of other student or to the district employees or an extended placement is in the student's best interest. Students who commit offenses requiring expulsion at the end of one school year may be expelled to the next school year to complete the assigned term of expulsion.

Notice

The DBC with the department principals will make a written recommendation to the superintendent who will make the ultimate decision.. The associate superintendent will make the decision to expel a student.

Placement Pending Notice

Until a hearing can be held, the principal or other appropriate administrator may place the student in:

- Another appropriate classroom.
- A DAEP.
- Emergency expulsion for a period not to exceed ten school days.
- Out-of-school suspension.
- Student Support Centers (in-school suspension).

Firearm Violations

State and federal law require a student to be expelled from the regular classroom for a period of at least one calendar year for bringing a firearm, as defined by federal law, to school. However, the superintendent or designee may modify the length of the expulsion on a case-by-case basis. Expelled students may receive educational services in the district's DAEP. Students under the age of ten shall receive educational services in the district's DAEP.

Admission of Expelled Students

The district will decide on a case-by-case basis the placement of a student who is subject to an expulsion order from another district or open-enrollment charter school and who requests admission into the district.

Participation in Activities

Expelled students are prohibited from being on school grounds or attending school-sponsored or school-related activities during the period of expulsion.

Emergency Expulsion [37.019]

In an emergency, the principal or other appropriate administrator may order the immediate expulsion of a student when the continued presence of the student on campus poses a danger of imminent harm to persons or property. When an emergency expulsion occurs, the student and parent/legal guardian will be given oral notice of the reason for the action. The reason must be a reason for which expulsion may be made on a non-emergency basis, and written notification will follow oral notification.
A student who is expelled on an emergency basis will be released to the student's parent, parent's representative, medical providers or law enforcement authorities. Within a reasonable amount of time after the emergency expulsion, but no later than the tenth day after the date of the emergency expulsion, the student will be given appropriate due process required for a student facing expulsion. For a student with disabilities the term of the student's emergency expulsion is subject to the requirements of federal law.

Individuals with Disabilities Education Act (IDEA)

A student with disabilities may be removed to an appropriate and different setting or suspended for not more than 10 consecutive school days (to the extent such alternatives would be applied to students without disabilities). School personnel must consider any unique circumstances on a case-by-case basis when determining whether a change in placement is appropriate for the child with a disability who violates a code of student conduct.

Within 10 school days of any decision regarding a disciplinary change of placement due to a Code violation, the ARD committee must determine whether the behavior of the student is a manifestation of the student's disability. When making a manifestation determination, the ARD committee must review all relevant information in the student's file, including the student's Individualized Education Program (IEP), any teacher observations and any relevant information provided by the parents to determine if the conduct in question was caused by or had a direct and substantial relationship to the student's disability or if the conduct in question was the direct result of an IEP implementation failure. If either is applicable the conduct shall be determined to be a manifestation of the student's disability. If the behavior is determined to be a manifestation of the student's disability, the ARD committee must either:

1. Conduct a functional behavioral assessment and implement a behavioral intervention plan if such assessment for conduct was not completed prior to behavior;

2. Or if a behavioral intervention plan has been developed, the ARD shall review the plan, modify it, as necessary, to address the behavior and return the student to the placement from which they were removed, if both the parent/legal guardian and school agree to a change of placement as part of the modification of the behavioral intervention plan, or special circumstances exist.

Special Circumstance: School personnel may remove a student to an appropriate interim alternative placement for not more than 45 school days without regard to whether the behavior is determined to be a manifestation of the child's disability if the student:

- Carries a weapon to school or to a school function.
- Knowingly possesses or uses illegal drugs or sell or solicits the sale of a controlled substance while at school or a school function.
- Has inflicted serious bodily injury upon another person while at school, on school premises or at a school function.

The ARD committee shall determine the interim alternative education setting. If the behavior is determined not to be a manifestation of the student's disability, disciplinary procedures applicable to students without disabilities may be applied to the student in the same manner and for the same duration in which the procedures would be applied to students without disabilities except that services during periods of the removal must be provided.

When a student is removed from the current educational placement either because of special circumstance or because the behavior is not a manifestation of the student's disability, the ARD committee must determine educational services for a Free Appropriate Public Education (FAPE) which may be provided in an alternate setting, so as to enable the child to continue to:

- Participate in the general education curriculum, although in another setting;
- Progress toward meeting the goals set out in the student's IEP;
- Receive, as appropriate, a functional behavioral assessment, behavioral intervention services and modifications designed to address the behavior violation so that it does not recur.

The ARD committee shall determine the interim alternative education setting.

After the tenth cumulative day of removal in a school year, the student must be provided educational services needed to receive a FAPE. Services must enable the student to: continue to participate in the general curriculum, although in another setting, and progress toward meeting the goals set out in the IEP.

On the date in which the decision is made to change a student's placement because of a code of conduct violation, the school must notify the parents/legal guardians of that decision and of all procedural safeguards.

Nothing in the Code shall be construed to prohibit the school district from reporting a crime committed by a student with a disability to appropriate authorities. When reporting a crime to authorities, school district must ensure that copies of the special education and disciplinary records of the student are transmitted for consideration by those authorities.

The child with a disability may not be disciplined for bullying, harassment or making a hit list until an ARD committee meeting has been held to review the conduct. An interim action plan would take place as to ensuring the safety of all students until an ARD has been held. The school is also required to investigate reports of bullying as well.

The parent/legal guardian of a student with a disability who disagrees with any decision regarding disciplinary placement or the manifestation determination may request a hearing. During the appeal the child shall remain in the interim alternative educational setting pending the decision or until the expiration of the time period, whichever occurs first, unless the parent/legal guardian and the district otherwise agree. The state or district shall arrange for an expedited hearing, which shall occur within 20 school days of the date the hearing is requested; a determination shall be made within 10 school days.

VII. Glossary

Abuse is improper or excessive use.

Aggravated robbery is defined in part by Texas Penal Code 29.03(a) as when a person commits robbery and:

1. Causes serious bodily injury to another;
2. Uses or exhibits a deadly weapon; or
3. Causes bodily injury to another person or threatens or places another person in fear of imminent bodily injury or death, if the other person is:

    a. 65 years of age or older, or
    b. A disabled person.

Armor-piercing ammunition is handgun ammunition used in pistols and revolvers and designed primarily for the purpose of penetrating metal or body armor.

Arson is a crime that involves:

1. Starting a fire or causing an explosion with intent to destroy or damage:

    a. Any vegetation, fence or structure on open-space land; or
    b. Any building, habitation or vehicle:

        i. Knowing that it is within the limits of an incorporated city or town;
        ii. Knowing that it is insured against damage or destruction;
        iii. Knowing that it is subject to a mortgage or other security interest, knowing it is located on property belonging to another;
        iv. Knowing that it is located within property belonging to another; or
        v. When the person starting the fire is reckless about whether the burning or explosion will endanger the life of some individual or the safety of the property of another.

2. Recklessly starting a fire or causing an explosion while manufacturing or attempting to manufacture a controlled substance and the fire or explosion damages any building, habitation or vehicle; or

3. Intentionally starting a fire or causing an explosion and in so doing:

    a. Recklessly damaging or destroying a building belonging to another, or
    b. Recklessly causing another person to suffer bodily injury or death.

Assault is defined in part by Texas Penal Code §22.01(a)(1) as intentionally, knowingly or recklessly causing bodily injury to another; §22.01(a)(2) as intentionally or knowingly threatening another with imminent bodily injury; and §22.01(a)(3) as intentionally or knowingly causing physical contact with another that can reasonably be regarded as offensive or provocative.

Bullying means a single significant act or a pattern of acts by one or more students directed at another student that exploits an imbalance of power and involves engaging in written or verbal expression, expression through electronic means or physical conduct that a school district's board or the board's designee, the principal or other appropriate administrator determines:

1. Has the effect or will have the effect of physically harming a student, damaging a student's property or placing a student in reasonable fear of harm to the student's person or of damage to the student's property;
2. Is sufficiently severe, persistent or pervasive enough that the action or threat creates an intimidating, threatening or abusive educational environment for a student; or
3. Infringes on the rights of the victim at school; and
4. Includes cyberbullying.

This conduct is considered bullying if it:

1. Interferes with a student's educational opportunities; or
2. Substantially disrupts the operation of a classroom, school, school-sponsored or school-related activity.

The school has discipline authority if bullying:

1. Occurs on or is delivered to school property or to the site of a school-sponsored or school-related activity on or off school property,
2. Occurs on a publicly- or privately-owned school bus or vehicle being used for transportation of student to or from school or a school-sponsored or school-related activity; and
3. Cyberbullying that occurs off school property or outside of a school-sponsored or school-related activity.

Chemical dispensing device is a device designed, made or adapted for the purpose of causing an adverse psychological or physiological effect on a human being. This category does not include a small chemical dispenser sold commercially for personal protection.

Club is an instrument specially designed, made or adapted for the purpose of inflicting serious bodily injury or death. A blackjack, mace, nunchucks and tomahawk are in the same category.

Criminal street gang is three or more persons having a common identifying sign or symbol or an identifiable leadership who continuously or regularly associates in the commission of criminal activities.

Child Study Team (CST): All campuses have a CST led by an administrator or his/her designee. The purpose of the CST shall be to review student performance issues to provide and monitor interventions for students experiencing attendance, academic and/or behavioral challenges not effectively addressed with Tier I and Tier II supports.

Cyberbullying is bullying that is done through the use of any electronic communication device, including through the use of a cellular or other type of telephone, computer, a camera, electronic mail, instant messaging, text messaging, a social media application, an Internet website or any other Internet-based communication tool.

Dating violence occurs when a person in a current or past dating relationship uses physical, sexual, verbal or emotional abuse to harm, threaten, intimidate or control another person in the relationship. Dating violence also occurs when a person commits these acts against a person in a marriage or dating relationship with the individual who is or was once in a marriage or dating relationship with the person committing the offense, as defined by Section 71.0021 of the Family Code.

Deadly conduct occurs when a person recklessly engages in conduct that places another in imminent danger of serious bodily injury, such as knowingly discharging a firearm in the direction of an individual, habitation, building or vehicle.

Deferred adjudication is an alternative to seeking a conviction in court that may be offered to a juvenile for delinquent conduct or conduct indicating a need for supervision.

Deferred prosecution may be offered to a juvenile as an alternative to seeking a conviction in court for delinquent conduct or conduct indicating a need for supervision.

Delinquent conduct is conduct that violates either state or federal law and is punishable by imprisonment or confinement in jail. It includes conduct that violates certain juvenile court orders, including probation orders, but does not include violations of traffic laws.

Disciplinary Alternative Education Program (DAEP). It is a disciplinary setting for secondary students that have had a due process conference or hearing and removed or expelled from the traditional school setting.

Discretionary means that something is left to or regulated by a local decision maker.

E-cigarette means an electronic cigarette or any other device that simulates smoking by using a mechanical heating element, battery or electronic circuit to deliver nicotine or other substances to the individual inhaling from the device. The term includes any device that is manufactured, distributed or sold as an e-cigarette, e-cigar or e-pipe or under another product name or description and a component, part or accessory for the device, regardless of whether the component, part or accessory is sold separately from the device.

Explosive weapon is any explosive or incendiary bomb, grenade, rocket or mine and its delivery mechanism that is designed, made or adapted for the purpose of inflicting serious bodily injury, death or substantial property damage, or for the principal purpose of causing such a load report as to cause undue public alarm or terror.

False alarm or report occurs when a person knowingly initiates, communicates or circulates: a report of a present, past or future bombing; fire; offense; or another emergency that he or she knows is false or baseless and that would ordinarily:

1. Cause action by an official or volunteer agency organized to deal with emergencies;
2. Place a person in fear of imminent serious bodily injury; or
3. Prevent or interrupt the occupation of a building, room or place of assembly.

Firearm is defined by federal law (18 U.S.C. § 921(a)) as:

1. Any weapon (including a starter gun) that will, is designed to or may readily be converted to expel a projectile by the action of an explosive;
2. The frame or receiver of any such weapon;
3. Any firearm muffler or firearm weapon; or
4. Any destructive device, such as any explosive, incendiary or poison gas bomb or grenade.

Such term does not include an antique firearm.

Firearm silencer means any device designed, made or adapted to muffle the report of a firearm.

Graffiti are marks with paint, an indelible pen or marker or an etching or engraving device on tangible property without the effective consent of the owner. The markings may include inscriptions, slogans, drawings or paintings.

Handgun is defined by Texas Penal Code 46.01(5) as any firearm that is designed, made or adapted to be fired with one hand.

Harassment is conduct that:

1. Meets the definition established in district policies DIA(LOCAL) and FFH(LOCAL); or
2. Threatens to cause harm or bodily injury to another person, including a district student, employee, board member or volunteer; is sexually intimidating; causes physical damage to the property of another student; subjects another student to physical confinement or restraint; or maliciously or substantially harms another student's physical or emotional health or safety.

Hazing is an intentional or reckless act, on or off campus, by one person alone or acting with others that endangers the mental or physical health or safety of a student for the purpose of pledging, initiation into, affiliation with, holding office in or maintaining membership in an organization.

Hit list is a list of people targeted to be harmed, using a firearm, a knife or any object to be used with intent to cause bodily harm.

Holistic approach to conflict would be to help students understand the nature of conflict, what defense mechanisms it triggers in them and how to take responsibility for those feelings. It can then equip students with the skills needed to approach the conflict so that all parties can move forward in a healthy way.

Incremental interventions are disciplinary interventions that use a range of graded disciplinary actions and responses in order to control and manage behavioral issues.

Intimate visual material is visual material that depicts a person with the person's intimate parts exposed or engaged in sexual conduct [Civil Practice and Remedies Code Section 98B.001(2)].

Location-restricted knife is defined by Texas Penal Code 46.01(6) as a knife with a blade of over five and one-half inches.

Knuckles are any instrument consisting of finger rings or guards made of a hard substance and designed or adapted for inflicting serious bodily injury or death by striking a person with a fist enclosed in the knuckles.

Machine gun is any firearm that is capable of shooting more than two shots automatically without manual reloading by a single function of the trigger.

Out-of-school suspension is defined as a temporary exclusion from school and school activities. Suspension from school may be used alone for violations of school rules or the Code. In addition, suspensions may be used for students who have committed a removal or expulsion offense and for whom a conference or hearing is pending.

Paraphernalia are devices that can be used for inhaling, ingesting, injecting or otherwise introducing a controlled substance into the human body.

Peer mediation is problem-solving youth-to-youth. In peer mediation, two or more students involved in a dispute meet in a private, safe and confidential setting to work out problems with the assistance of a trained student mediator.

Possession means actual care, custody, control or management of an object or substance. A student shall be considered in possession of any substance or object prohibited or regulated by this code if the substance or object is:

1. On the student's person or in the student's personal property, including but not limited to the student's clothing, purse, telecommunications or electronic devices, book bag or briefcase;
2. In any private vehicle used by the student for transportation to or from school or school-related activities, including but not limited to an automobile, truck, motorcycle or bicycle; or
3. In any school property used by the student, including but not limited to a locker or a desk.

Proactive intervention:
1. Being proactive is defined as serving to prepare for, intervene in or control an expected occurrence or situation, especially a negative or difficult one; anticipatory: proactive measures against crime.
2. Proactive interventions would anticipate a known behavior as opposed to reactive interventions, which are interventions that are used only once the behavior occurs. They are consequences (or reactions) to the behavior. The goal is to cut short the behavior to minimize damage.

Progressive discipline uses incremental interventions, whenever possible, to address inappropriate behavior with the ultimate goal of teaching pro-social behavior.

Prohibited weapon under Texas Penal Code 46.05(a) means:

1. An explosive weapon (see glossary);
2. A machine gun;
3. A short-barrel firearm or firearm silencer, unless registered with the U.S. Bureau of Alcohol Tobacco, Firearms and Explosives or classified as a curio or relic by the U.S. Department of Justice;
4. Armor-piercing ammunition;
5. A chemical dispensing device (see glossary);
6. A zip gun; or
7. A tire deflation device.

Pro-social behaviors/activities are any actions intended to help others. One motivation for prosocial behavior is altruism, or the desire to help others with no expectation of reward.

Public school fraternity, sorority, secret society or gang means an organization composed wholly or in part of students seeking to perpetuate the organization by taking on additional members from a school's student population based on a decision by membership rather than by the free choice of a qualified student. Educational organizations listed in Section 37.121(d) of the Education Code are exempted from this definition.

Reasonable belief is a determination made by the superintendent or designee using all available information, including information furnished under Article 15.27 of the Code of Criminal Procedure.

Restorative circle process is a community process for supporting those in conflict. It brings together the three parties to a conflict — those who have acted, those directly impacted and the wider community — within an intentional systematic context to dialogue as equals.

School-wide tiered framework: Positive Behavioral Interventions and Supports (PBIS) is a multi-tiered framework that is utilized to achieve important behavior changes. It requires adopting and organizing evidence-based behavioral interventions into an integrated continuum that enhances academic and social behavior outcomes for all students.

Self-defense is the use of force against another to the degree a person reasonably believes the force is immediately necessary to protect themselves.

Short-barrel firearm is a rifle with a barrel length of less than 16 inches or a shotgun with a barrel length of less than 18 inches, or any weapon made from a rifle or a shotgun that, as altered, has an overall length of less than 26 inches.

Social and Emotional Learning (SEL) is the process through which children and adults acquire and effectively apply knowledge, attitudes and skills necessary to understand and manage emotions, set and achieve positive goals, feel and show empathy for others, establish and maintain positive relationships and make responsible decisions.

Socially and emotionally-safe: An experience in which one feels safe to express emotions, security and confidence to take risks and feel challenged and excited to try something new. Emotionally safe learning environments can be achieved by making SEL an essential part of education.

Student Support Centers (In-School Suspension) is defined as a placement of a student in a location separate from the classroom under the supervision of a teacher or other staff person where the student continues to receive instruction in each course to the extent possible. This does not include time-out arrangements between teachers or specific behavior management programs operated by campuses.

Suspension: See listing for "Student Support Centers (In-School Suspension)" and "Out-of-School Suspension."

Terroristic threat is a threat of violence to any person or property with intent to:

1. Cause a reaction of any type by an official or volunteer agency organized to deal with emergencies;
2. Place any person in fear of imminent serious bodily injury;
3. Prevent or interrupt the occupation or use of a building, room, place of assembly or place to which the public has access; place of employment or occupation; aircraft, automobile or other form of conveyance; or other public place;
4. Cause impairment or interruption of public communications; public transportation; public water, gas or power supply; or other service;
5. Place the public or a substantial group of the public in fear of serious bodily injury; or
6. Influence the conduct or activities of a branch or agency of the federal government, the state or a political subdivision of the state (including the district).

Title V offenses are those crimes listed in Title V of the Texas Penal Code that involve injury to a person and may include:

- Murder;
- Kidnapping;
- Trafficking of persons;
- Smuggling or continuous smuggling of persons;
- Assault (see glossary);
- Aggravated assault;
- Sexual Assault
- Aggravated sexual assault;
- Unlawful restraint;
- Voyeurism;
- Indecency with a child;
- Invasive visual recording;
- Disclosure or promotion of intimate visual material;
- Injury to a child, an elderly person, or a disabled person of any age;
- Abandoning or endangering a child;
- Deadly conduct;
- Terroristic threat;
- Aiding a person to commit suicide;
- Tampering with a consumer product.

[See FOC]

Under the influence means a student's faculties are noticeably impaired by alcohol and/or drugs though the student need not be legally intoxicated. Impairment of a person's physical and/or mental faculties may be evidenced by a pattern of abnormal or erratic behavior, and/or the presence of physical symptoms of drug or alcohol use or by admission.

Use means a student has smoked, ingested, injected, imbibed, inhaled, drunk or otherwise taken internally, on or off campus, a prohibited substance recently enough that it may be detectable by, but not limited to, the following: the student's appearance, actions, breath or speech.

Zip gun is a device or combination of devices, not originally a firearm, but adapted to expel a projectile through a smooth-bore or rifled-bore barrel by using the energy generated by an explosion or burning substance.

Item **Proclamation of High School ELAR**

Information The State Board of Education (SBOE) issues a proclamation to call for new instructional materials. The proclamation lists the subject areas scheduled for review. It contains a schedule of adoption procedures, requirements, the Texas Essential Knowledge and Skills (TEKS), and instructions for providing electronic files for braille and large type materials.

Proclamation 2019 calls for instructional materials for English language arts and reading, grades K-8; handwriting (English and Spanish), grades K-5; and Personal Financial Literacy.

Contact Stella Egbert

Action Information Only

PROCLAMATION 2019

An Update on the ELAR K-8 Adoption

K-8 ELAR ADOPTION

- Writing materials were identified and selected in the Spring of 2019 within the the Reading/Writing/ASL Multi-Tiered Systems of Support Structuring Team.
- Implementation and Training

Department	Teacher Materials
ELEM	$4,791.6
MS	$2,404.6
	$7,196.20

K-8 ELAR ADOPTION

- Reading resources identified for each department and recommended through the Reading/Writing/ASL Multi-Tiered Systems of Support Structuring Team
- Core Literature Materials, K-5
- National Geographics, 6-8

Department	Resources
ELEM	$2,000.48
MS	$10,264.75
	$12,265.23

TOTAL IMAT FOR PROCLAMATION 19

Department	Resources
Empowering Writers K-8	$7,196.20
Reading Curriculum Materials	$12,265.23
	$19,461.43

Empowering® Writers

Write. Read. Succeed.

PROCLAMATION 2020

➤ HS ELAR

The State Board of Education (SBOE) issued *Proclamation 2020* at its April 2018 meeting. Instructional materials were adopted in November 2019 for high school English language arts and reading. The adopted materials are scheduled to go into classrooms in the 2020–21 school year.

➤ Committee

➤ Timeline

Item	**Election of Board Officers**
Information	The Board members will nominate and elect officers from among themselves for the upcoming calendar year.
Contact	Eric Hogue
Action	Board President will confirm election of officers for the next calendar year.

Item **Board Policies**

Information

DBA Employment Requirements and Restrictions: Credentials and Records
DEC Compensation and Benefits: Leaves and Absences
DFAC Probationary Contracts: Return to Probationary Status
DHE Employee Standards of Conduct: Searches and Alcohol Drug Testing
GNB Relations with Educational Entities: Regional Education Service Centers
GNC Community Relations: Colleges and Universities
GND Relations with Educational Entities: State Education Agency
FO Student Discipline
FOF Students Discipline: Students with Disabilities
FOE Student Discipline: Emergency and Alternative Placement
FOB Student Discipline: Out of School Suspension
FOD Student Discipline: Expulsion
EEJA (DELETE) Individualized Learning: Credit by Examination with Prior Instruction
EEJB (DELETE) Individualized Learning: Credit by Examination without Prior Instruction
EHBD Special Programs: Federal Title I
EHDB (NEW) Alternative Methods for Earning Credit: Credit by Examination with Prior Instruction
EHDC (NEW) Alternative Methods for Earning Credit: Credit by Examination without Prior Instruction
EFAA (DELETE) Instructional Materials: Selection and Adoption
EFA Instructional Resource: Instructional Materials
EHAB Basic Instructional Program: Required Instruction: Elementary
EHBF Special Programs: Career and Technical Education
EMI Miscellaneous Instructional Policies: Study of Religion
GKA (EXHIBIT) Community Relations: Conduct on School Premises

Contact Sha Cowan

Action Request for Approval