




Internet Advisory Committee

November 26, 2018

Today's Agenda

- Committee Development Jennifer Miller
 - Security Frameworks James Costello and Jennifer Miller
 - Trusted Learning Environment Status Jennifer Miller
 - Website Access - Vimeo and Archive.org Greg Rhodes
 - Content Filter RFP Greg Rhodes and Paula Ross
 - LEARN Network Update Frankie Jackson and Paula Ross
 - KnowBe4 Training James Costello
 - 1819 Know Be 4 District Instructions
 - Training series distribution
 - Training series participation
 - Reminder process
 - Process implementation Eric Pina
 - Resource Approval or Utilization Process
 - Qualys SSL Server Test
 - Technology Services Responsible Use Policy
 - Data Privacy Agreement Eric Pina
 - Campus/Department Questions James Costello and Jennifer Miller
- 

Committee Development

- **Internet Advisory Committee**

- **Purpose:** To make recommendations, provide feedback, and disseminate information as it relates to the protection, privacy, and security of students, employees, and personal data.
- **Members:** Instructional Technology Representatives, Technology Services Representatives, Curriculum Coordinators/Coaches, Campus Appointee(s), Librarians, Student Representatives

- **Governance Authority Committee**

- **Purpose:** To develop and implement data privacy and security policies and practices as it relates to the protection, privacy, and security of students, employees, and personal data.
- **Members:** Chief Technology Officer, Security Specialist Officer, Human Resources Director, Student Services, Curriculum Director, Principal Cluster Representatives, Technology Directors, Legal, Police Department



Internet Advisory Committee

- **Purpose:** To make recommendations, provide feedback, and disseminate information as it relates to the protection, privacy, and security of students, employees, and personal data.
- **Members:** Instructional Technology Representatives, Technology Services Representatives, Curriculum Coordinators/Coaches, Campus Appointee(s), Librarians, Student Representatives

Larry Barrios
James Costello
Becky Cook
John Crumbley
Diane Garland
Jennifer Hill
Frankie Jackson
Deborah Jones
Jenifer Jones

Beth Keene
Mary Bridget Maddan
Heather McGuire
Jennifer Miller
Andrea Morris
John Morrison
Kay Pechacek
Eric Pina
Paula Ross

Greg Rhodes
Linda Sams
Todd Sepulveda
David Srubar
Steven Stone
Stefanie Ware



Governance Authority Committee

- **Purpose:** To **develop and implement** data privacy and security policies and practices as it relates to the protection, privacy, and security of students, employees, and personal data.
- **Members:** Chief Technology Officer, Security Specialist Officer, Human Resources Director, Student Services, Curriculum Director, Principal Cluster Representatives, Technology Directors, Legal, Police Department

Larry Barrios

Heather Bergman

James Costello

Becky Cook

Cheryl Fisher

Sarah Harty

Frankie Jackson

Gary Kinninger

Denise Kubecka

Barbara Levandoski

Maria Mamaux

Onica Mayers

Candy McCown

Eric Mendez

Jennifer Miller

Lana Mock

Eric Pina

Paula Ross

Greg Rhodes

Jae Simpson-Butler

Marney Sims

Jill Smith

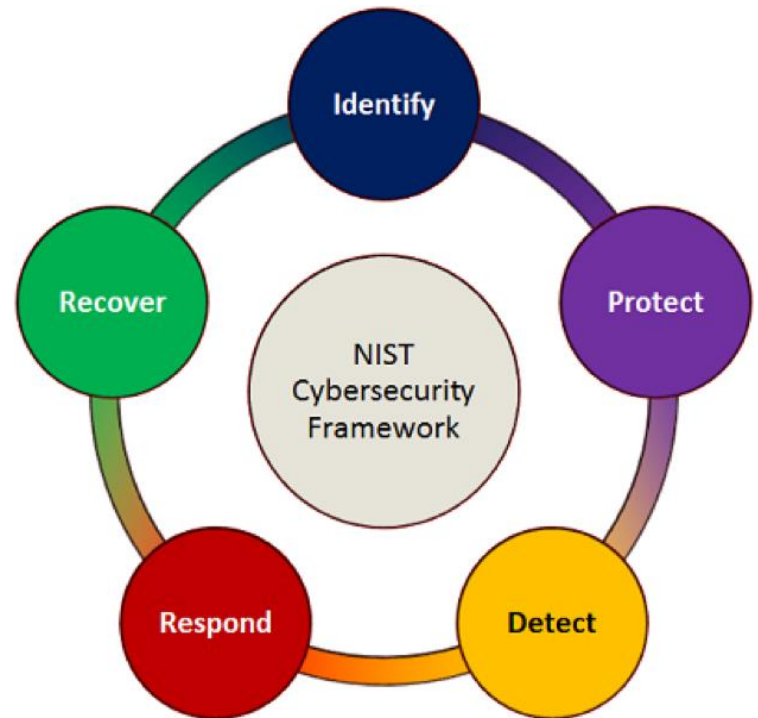
Kenya Turner



Frameworks

NIST Cybersecurity Framework

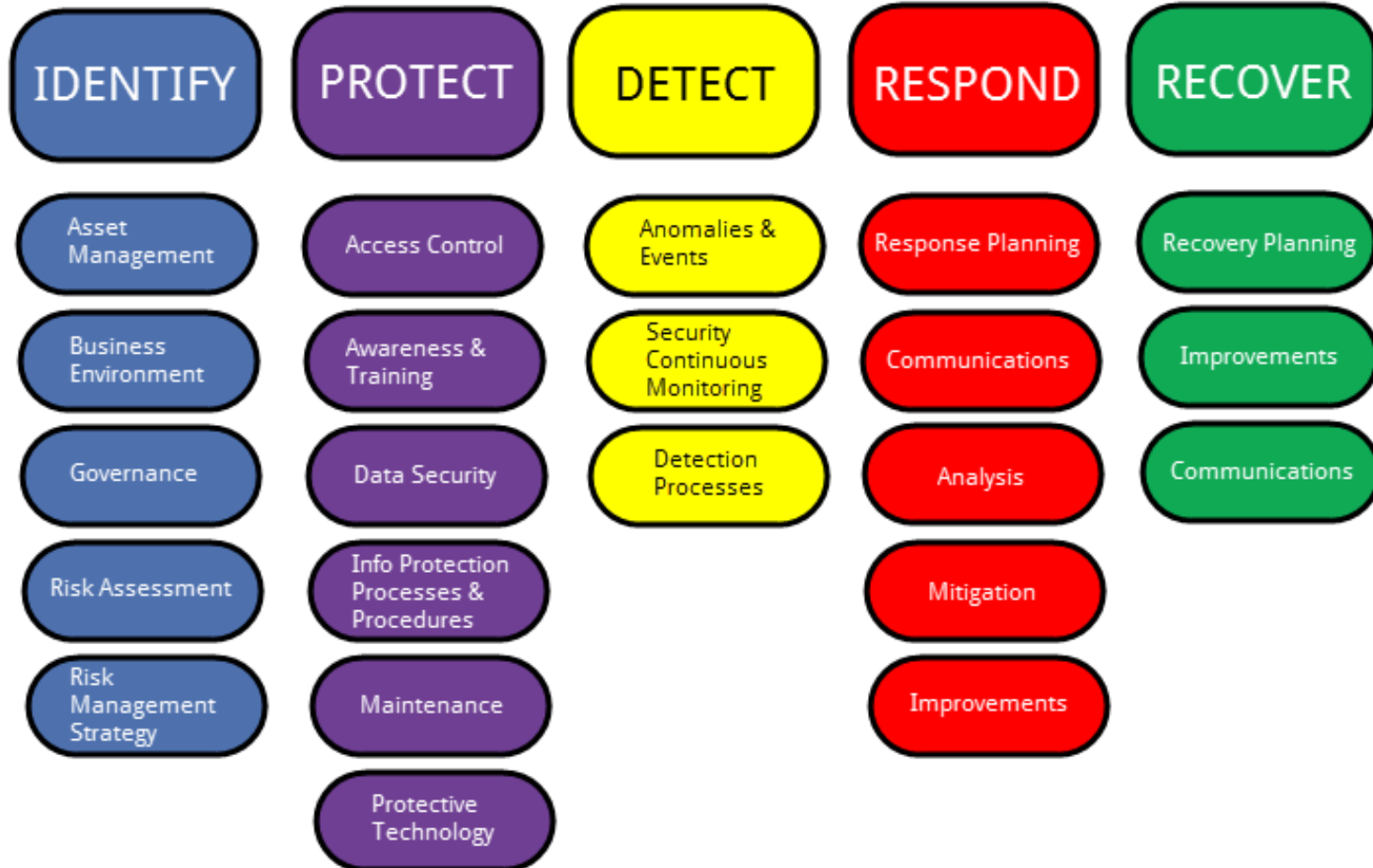
- Best practices created to prevent, detect, and respond to cyber-attacks.
- Goals of using a framework:
 - To improve the protection, privacy, and security of students, employees, and district data.
 - Align with regulations such as FERPA, CIPA, COPPA, and PPRA.



Frameworks

5 Functions, 22 Categories, and 98 subcategories

We need and appreciate your help in keeping our district safe!



Frameworks

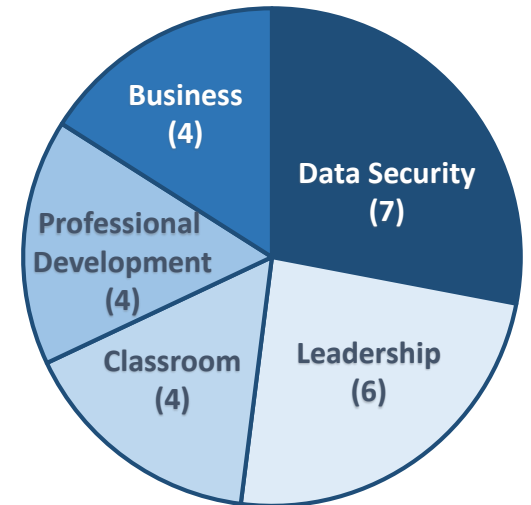
Trusted Learning Environment

- Nation's only data privacy seal for school systems
- Focused on building a culture of trust and transparency.
- Developed by CoSN (the Consortium for School Networking), in collaboration with a diverse group of 28 school system leaders nationwide and with support from AASA, the School Superintendents Association, the Association of School Business Officials International (ASBO) and ASCD
- Program requirements have been validated by more than 50 school systems.



Trusted Learning Environment Framework

- Leadership Practices
 - Manage and collaborate with stakeholders regarding the use and governance of student data to inform instruction
- Business Practices
 - Establish acquisition vetting processes and contracts that, at a minimum, address applicable compliance laws while supporting innovation.
- Data Security Practices
 - Perform regular audits of data privacy and security practices and publicly detail these measures
- Professional Development Practices
 - Require school staff to conduct privacy and security training and offer the instruction to all stakeholders
- Classroom Practices
 - Implement educational procedures and processes to ensure transparency while advancing curricular goals



Practices in each category



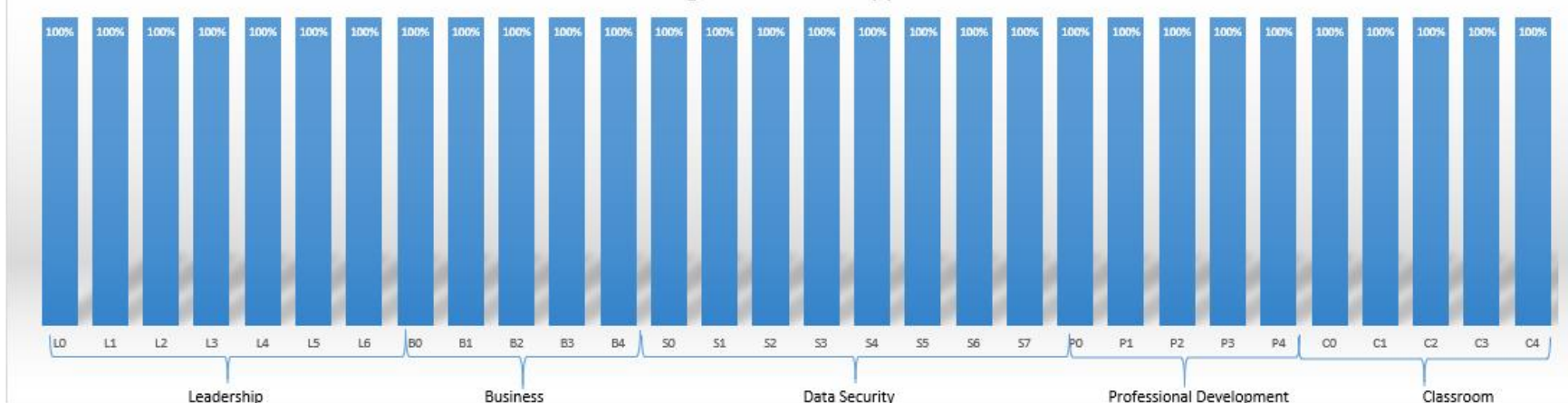
<https://trustedlearning.org/framework/>



Trusted Learning Environment Status

- Applied in May, 2018
 - Received recommendations
- Re-Applied October, 2018
 - Currently under review - awaiting response

Trusted Learning Environment Application Process



Website Access

- Vimeo
 - Blocked for students at the URL and application control layers.
 - Issue occurs when education applications use Vimeo to house videos.
 - Unblocking specific videos has not been successful and work-arounds have risks.
- Archive.org
 - The Good – free digital library of books, movies, music, and archived web pages.
 - The Bad – includes pornography and adult material.



Content Filter RFP

Desired Criteria:

- CIPA Compliant
- K12 Emphasis
- Integrated with AD
- Profiles based on AD Groups, subnets, machine type
- SSL Decryption
- Mobile and At Home Protection
- Entire School Year History available
- History should be exportable
- Custom Reporting
- Allows YouTube designated educational
- Website Overrides
- Reportable User Searches
- Real-time monitoring of user
- Up-to-date categorizations
- Educational Games Category
- Option to block Unrated sites
- URL and Application Control Blocking
- Customizable user notification/block pages
- Supports non-windows devices
- Supports multiple datacenters/ISPs with single history repository
- Supports large bandwidths and up to 300k devices
- Zero-minimum latency
- Network Peering Support (LEARN)
- Redundant
- Blocks Ultrasurf/Psiphon/proxies
- Adaptive alert capability – i.e. user has 30 porn blocks in last 15 minutes
- Industry/K12 recognized



LEARN Network Update

Frankie Jackson worked with the Network Infrastructure and Communications (NIC) team and strategic partners including Education Partners Solution and Layer3 Communications all during the week of **October 29, 2018 – November 2, 2018** to implement plans for upgrading the district's enterprise level network and taking security precautions. With Paula Ross as the lead, the following actions were implemented as precautionary measures.

- ✓ Increased the district's Cogent Internet bandwidth at Data Center 4 from 6 Gb to 12 Gb burstable to 20 Gb.
- ✓ As a pilot, at no additional cost to the existing ICTX contract, increased ICTX total bandwidth at Data Center 3 from 6 Gb to 10 Gb and ICTX added a 10 Gb connection to LEARN services.
- ✓ As a pilot, at no cost, added the LEARN's Distributed Denial of Service (DDOS) scrubbing for free through December as an immediate response.
- ✓ As a pilot, at no cost, implemented 10 Gb bandwidth of LEARN Peering and Caching to build infrastructure for "Safe and Secure Internet". The 10 Gb connection to priority content such as Amazon Web, Google and Microsoft offers secure and higher quality access to content.
- ✓ Optimized processes for identification and response to potential security issues and/or other Internet service disruption with Internal team, ICTX, Cogent, LEARN and Layer 3.

Next Steps:

- ❑ During November, use LEARN services for scrubbing, peering and caching for secured access.
- ❑ Upgrade the network's routing infrastructure.
- ❑ Evaluate a LEARN proposal for the pilot services through an interlocal agreement with ESC Region 4 to maintain services through June 30, 2019.
- ❑ Work with current providers of ICTX and PS Lightwave for access to LEARN services through June 2019 and leverage E-Rate funding currently and long-term when possible.
- ❑ Investigate increased Internet monitoring tools and services including the proposal from Layer 3.
- ❑ Continue to identify long term solutions for further strengthening security networking practices.



Cybersecurity Training Announcement



KnowBe4 Cybersecurity Training Beginning September 7, 2018

Beginning Friday, September 7, 2018, you will receive an email notifying you of new cybersecurity training from KnowBe4. KnowBe4 is a third-party cybersecurity software used for security awareness training and simulated phishing attacks that helps us keep our electronic information safe. Once you click the link, you will be directed to a webpage with instructions to check your email inbox. A new email will appear in your email inbox with a unique secure link that does not require a password. The link provided will connect you to the training module.

Cybersecurity training will be distributed periodically throughout the year. It is our goal to continue to bring updates, new information, and training to ensure our electronic information is safe and secure.



Cybersecurity Training Process

- Training began September 7, 2018
- Trainings or Reminders distributed every Monday
- Training Distribution – All Employees
 - September 7 – Social Engineering 101
 - September 24 – Phishing
 - October 8 – Cloud Security
 - October 22 – Free Wi-Fi
 - November 5 – Secure Passwords
- Training Distribution – Technicians
 - September 19 – Privileged Access
 - October 17 – Malware
 - November 14 – Spot the Bad Attachment



Cybersecurity Training Participation

- Training Participation

- September 7 – Social Engineering 101 – 46% – 5,971
- September 24 – Phishing – 45% – 5,916
- October 8 – Cloud Security – 39% – 5,117
- October 22 – Free Wifi – 36% – 4,725
- November 5 – Secure Passwords – 31% – 3,981

- Training Participation – Technicians

- September 19 – Privileged Access – 95%
- October 17 – Malware – 93%
- November 14 – Spot the Bad Attachment – 75%

25,710
completed
trainings



Changes in Student Handbook

- **SYSTEM ACCESS** Access to the district's electronic communications system will be governed as follows:
 - ~~3. Students will be granted access to the district's system and will be assigned individual accounts. Students are not to share their login/password with others.~~
 3. Students who are granted access to the district's system will be assigned individual accounts. Students are not to use a computer that is logged in under another user's name.



Changes in Employee Handbook

The addition of the "Information Security and Data Privacy" section on pages 74-76.

Topics covered:

- Examples of sensitive information at CFISD
- Guidelines for properly securing this information
- Password Management
- Listing and describing the various Federal laws/acts (FERPA, COPPA, CIPA) addressing data security and protection.
- Guarding against social engineering attacks (i.e. phishing)
- Avoiding unsecure networks outside of the office
- Properly and securely destroying sensitive information (hard copy and electronic) when no longer needed
- Immediately report suspicious information security activity to the Customer Care Center or isupport@cfisd.net



Changes in Compliance Course

INFORMATION SECURITY AND DATA PRIVACY TRAINING


- Added to Module 8: Responsible Use Guidelines
 - Topics Covered:
 1. Keep Sensitive Information Physically Secure
 2. Manage Your Passwords
 3. Understand Data Privacy Security to Protect Student and Employee Data
 4. Guard against Social Engineering Attacks (Phishing)
 5. Avoid Unsecure Networks Outside the Office
 6. Securely Destroy Sensitive Information (Hard-copy and Electronic) when no longer needed.
 7. Immediately Report Suspected Information Security events to the Customer Care Center 281-897-4357 or isupport@cfisd.net



Process Implementation

- Resource Approval or Utilization Process
 - Qualys SSL Server Test

Qualys SSL Server Test
<https://www.ssllabs.com/ssltest/index.html>




The SSL server test is an online service that enables you to inspect the configuration of any public SSL web server.

This free service is a helpful tool to verify basic SSL security protocols are in place on web servers that may be handling student data.

Users enter the desired web address to begin the analysis of that site's SSL configuration. The SSL Server rating will be displayed at the completion of the analysis.

Summary

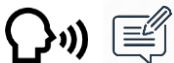
Overall Rating



Certificate	100
Protocol Support	95
Key Exchange	90
Cipher Strength	85

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Experimental: This server supports TLS 1.3 (draft 23).



Process Implementation

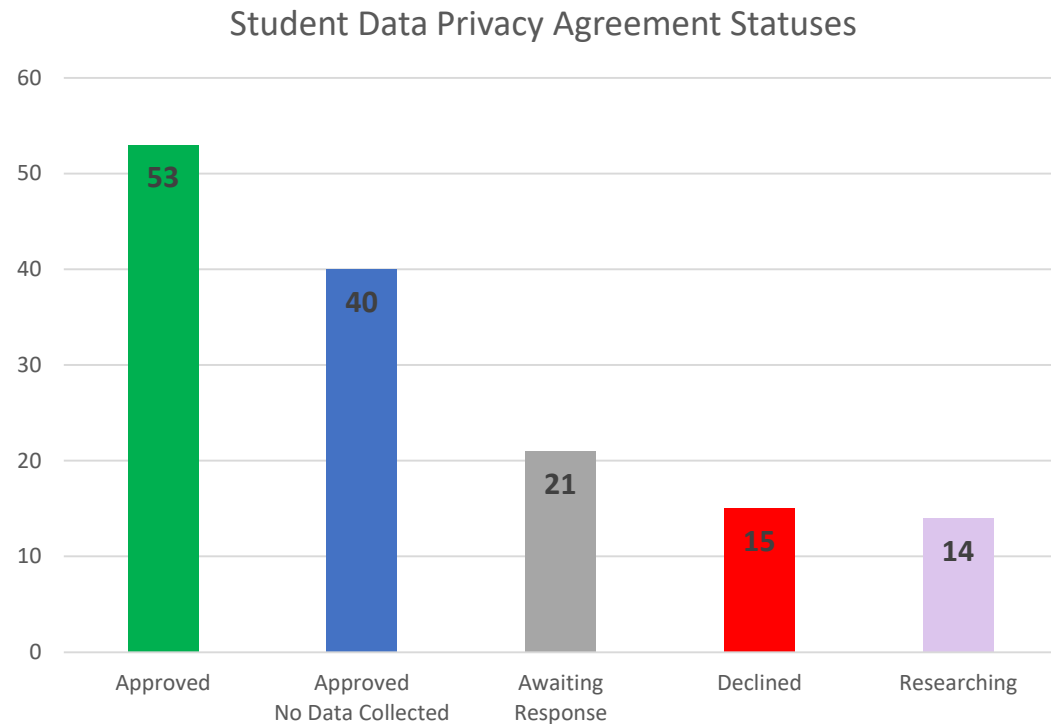
- Success of Qualys SSL Server Test

- rankonesports.com Grade **F** -> **A**
- sogosurvey.com Grade **B** -> **A**
- edgemakers.com Grade **C** -> **A**
- esgisoftware.com Grade **B** -> **A**



Data Privacy Agreement

- CFISD version distributed Spring – Fall, 2018
- Distributed to **143** Vendors
- Working to adopt the State Privacy Agreement – Winter, 2018



Data Privacy Agreement

- Benefits of the State Agreement
 - The Texas Data Privacy Agreement includes all data types and participants – employee data, as well as academic and facility data, and all types of documents.
 - The Texas Data Privacy Agreement allows additional districts to receive the same protection through one agreement. Cypress-Fairbanks ISD would be able to utilize another district's agreement with the signature in **Exhibit E**.
 - Standardization across the state.



Campus/Department Questions

