



CYBERSECURITY TIPS AND TOOLS INCIDENT RESPONSE, BEING PREPARED

Frosty Walker

Chief Information Security Officer
Texas Education Agency

Frosty.Walker@tea.texas.gov

(512) 463-5095



Data Security Advisory Committee

The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESC's, TEA and the private sector.

Texas Gateway

<https://www.texasgateway.org/>

Cybersecurity Tips and Tools

Three white diagonal lines of varying lengths and thicknesses are positioned in the bottom right corner of the slide, pointing towards the top right.

Online resources FOR YOUR CLASSROOM

Find engaging, TEKS-aligned resources that you can use with your students as part of classroom instruction, intervention, acceleration, or additional practice.

show me more

BROWSE TEKS

BROWSE RESOURCES ▶

Search

Featured Resources

Getting Started Guide

Starting the Conversation

ELA & READING
Targeting the 2 Percent

Restorative Discipline Practices in Texas

SOCIAL STUDIES
Social Studies TEKS: Supporting Information

MATH
Teacher2Teacher Math Video Series

Teacher2Teacher

cybersecurity data
Cyber Security Tips and Tools

Introduction to the Revised Mathematics TEKS
MATH
Mathematics TEKS: Supporting Information

ELA & READING
OnTRACK English II Reading: Understanding and Analysis of Literary Text



Confidentiality Provisions Applicable to School Districts and Charters

Students:

FERPA (20 U.S.C. 1232g; 34 C.F.R. 99.3) defines “personally identifiable information” to include the student’s name, the name of the student’s parent or other family members, the address of the student or student’s family, a personal identifier (SSN, student number, biometric record), other indirect identifiers (DOB, place of birth, mother’s maiden name), or other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty.

FERPA is applicable to personally identifiable information contained in education records. “Education records” means those records, files, documents, and other materials that contain information directly related to a student and are maintained by an educational agency or institution.

FERPA and section 26.013 of the Texas Education Code address “directory information.” A school district is permitted to designate certain information about students as directory information that is publicly available. However, a parent or eligible student must be given the opportunity to opt out of directory information. Directory information may include the student’s name, address, telephone number, email address, photograph, date and place of birth, grade level, enrollment status, dates of attendance, participation in recognized activities and sports, and honors and awards received.

Section 39.030 provides the results of individual student performance on academic skills assessment instruments are confidential and may be released only in accordance with FERPA. However, overall student performance data must be aggregated by ethnicity, sex, grade, subject, campus, and district and made available to the public. This data may not contain the names of individual students or teachers.

Confidentiality Provisions Applicable to School Districts and Charters

Educators/District Employees:

Education Code Section 21.0481 provides the results (numerical score and pass/fail) of educator certification examinations are confidential.

Education Code Section 21.355 states a document evaluating the performance of a teacher or administrator is confidential.

Education Code Section 22.08391 provides criminal history record information must not be disclosed except under certain circumstances.

Government Code Section 552.117 provides the home address and phone number, emergency contact information, social security number, or information that reveals whether the individual has family members is excepted from public disclosure if the current or former employee of a government body makes the election to withhold such information under section 552.024 of the Government Code.

Confidentiality Provisions Applicable to School Districts and Charters

Educators/District Employees:

Government Code Section 552.126 provides the name of an applicant for the position of superintendent of a school district is excepted from public disclosure, except the board of trustees must give public notice of the name(s) of the finalists being considered at least 21 days before the date of the meeting at which final action or vote is to be taken on the employment of the person.

Government Code Section 552.1 provides an informer's name or information that would substantially reveal the identity of an informer is excepted from public disclosure. "Informer" is defined as a student or former student or an employee or former employee of a school district who has furnished a report of another person's or persons' possible violation of criminal, civil, or regulatory law to the school district or the proper regulatory enforcement authority.

Government Code Section 552.136 provides a credit card, debit card, or access device number (a card, code, account number, etc. used to obtain money, goods, or services) is confidential.

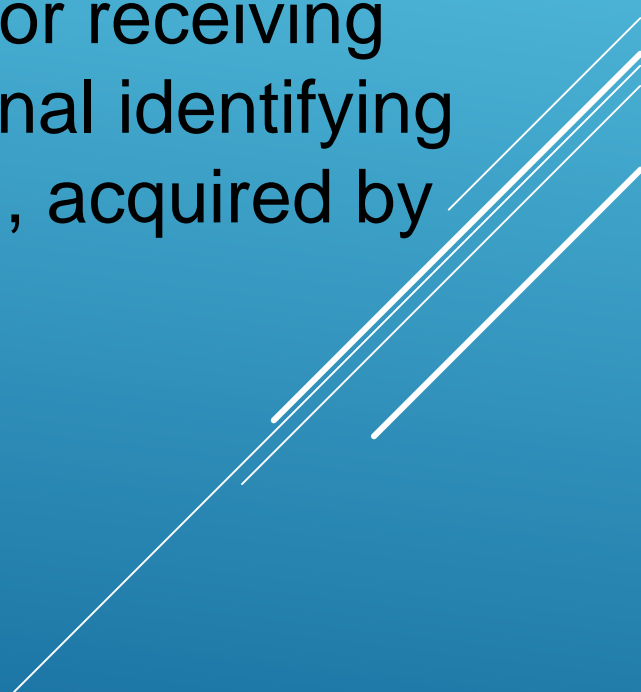
Government Code Section 552.137 states a personal email address is confidential (this does not include the work email address of a government employee).

Government Code Section 552.147(a-1) provides the social security number of an employee of a school district in the custody of the district is confidential.

Breach Notice Criteria

Texas Business and Commerce Code Ch. 521, §521.053


Report any breach of system security, after discovering or receiving notification of the breach, to any individual whose personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person, if it was not encrypted.

Three white diagonal lines of varying lengths and thicknesses are positioned in the bottom right corner of the slide, extending from the right edge towards the center.

LIFE CYCLE OF A BREACH

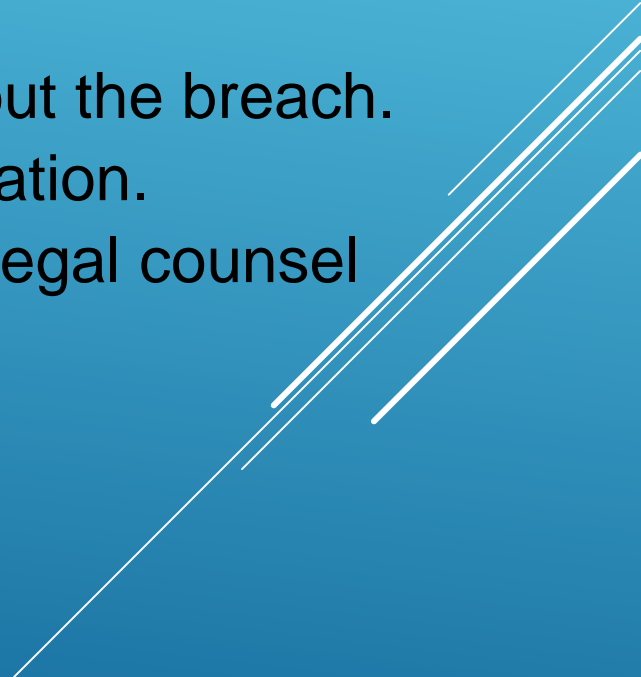
- Discovery
- Assemble Internal Response Team (potentially lead by 3rd party vendor)
- Internal Notification
- Investigate and Remediate (potentially lead by 3rd party vendor)
- Contact authorities on a need to know basis
- Employ vendors such as forensics, data breach resolution law and PR firms as needed (potentially lead by 3rd party vendor)
- Begin notification process, procure protection services for affected
- Notification to affected parties (potentially lead by 3rd party vendor depending on contract terms)
- Make public announcement with single point of contact (potentially lead by 3rd party vendor depending on contract terms)
- Respond to inquiries
- Resume business as usual

Panicking won't get you anywhere once you've discovered a data breach. Accept that it has happened and immediately begin following your documented process.



FIRST 24 HOUR CHECK LIST

- Record the date and time when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.
- Alert and activate everyone on the response team, including external resources, to begin executing your preparedness plan.
- Secure the premises around the area where the data breach occurred to help preserve evidence.
- Stop additional data loss. Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives.
- Document everything known thus far about the breach: Who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected, what devices are missing, etc.

- Interview those involved in discovering the breach and anyone else who may know about it. Document your investigation.
 - Review protocols regarding disseminating information about the breach for everyone involved in this early stage.
 - Assess priorities and risks based on what you know about the breach.
 - Bring in your forensics firm to begin an in-depth investigation.
 - Notify law enforcement, if needed, after consulting with legal counsel and upper management.
- 

THIRD PARTY VENDOR POTENTIAL BREACH PROCESS

Review contract for potential steps as outlined in contract regarding notification.

Information needed from third party:

- Root Cause Analysis including:
 - What Happened and When
 - How Discovered
 - List of exposure
 - Remediation process used to remediate
 - Remediation completion date
 - Verification process
 - Verification completion date

NOTIFICATION PROCESS

- Internal need to know
- Authorities
- Exposure Notification to affected parties
- Make public announcement with single point of contact
- Respond to inquiries
- Resume business as usual



TEXAS DEPARTMENT OF INFORMATION RESOURCES

Incident Response Team Redbook

Confidential

July 2014

Incident Response Team Redbook

Glossary and Acronyms

Incident Response Policy

Privacy/Security Event Initial Triage Checklist

Event Threat, Impact Analysis, and Escalation Criteria

Breach Notice Criteria

Post-Incident Checklist

Three white diagonal lines of varying lengths and thicknesses are positioned in the bottom right corner of the page, extending from the right edge towards the center.

Incident Response Team Templates

Title and Contact Information for Plan Sponsor/Owner

IRT Charter

IRT Membership by Roles

IRT Meeting Minutes

IRT Action List

IRT State Government Contact Information

Additional Templates

Identity Theft Protection Criteria

Internal Management Alert Template

Notice to Individuals Affected by Incident

Public (Media) Notice



External Contacts

State of Texas Contacts

Federal Contacts

Industry Contacts

Press Contacts



Legal References

Texas Laws and Regulations for Data Privacy and Security
Federal Laws and Regulations for Data Privacy and Security



Privacy/Security Event Initial Triage Checklist

- 1) Incident Response Team:** Assemble Incident Response Team (IRT) in response to an actual or suspect event/incident.
- 2) Secure data:** Secure data and confidential information and limit immediate consequences of the event. Suspend access and secure/image assets as appropriate.
- 3) Data elements:** Determine the types, owners, and amounts of confidential information that were possibly compromised.
- 4) Data source:** Identify each location where confidential information may have been compromised and the business owner of the confidential information.
- 5) Scope and escalation:** Confirm the level and degree of unauthorized use or disclosure (includes access) by the named or unidentified individuals or threats.
- 6) Number of individuals impacted:** Determine the number of individuals impacted.
- 7) Discovery date:** Determine the date the agency or contractor knew or should have known about the event/incident.

Privacy/Security Event Initial Triage Checklist

8) Management alert: Advise appropriate internal management.

9) External communications, as required: Advise external contacts, such as legislative leadership, the Office of the Inspector General, the Office of the Attorney General, law enforcement, outside counsel, and regulatory authorities.

10) Investigate:

a) Interview: Identify and interview personnel with relevant knowledge, e.g., determine whether and by whom access may have been approved, who discovered the risk, etc.

b) Documents: Gather and review contracts and provisioning documents.

c) Root Cause Analysis: Prepare RCA which describes why the event occurred, what business impact it had, and what will be done to prevent reoccurrence.

d) Event and Threat Impact Analysis

11) Mitigation: Revise policies, process, or business requirements, sanction workforce, enforce contracts, etc. to reduce the likelihood of event reoccurrence.

Questions?

frosty.walker@tea.texas.gov

512 463-5095

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.