CYBERSECURITY TIPS AND TOOLS

BASIC INCIDENT RESPONSE

Frosty Walker

Chief Information Security Officer

Texas Education Agency

Frosty.Walker@tea.texas.gov

(512) 463-5095

Data Security Advisory Committee

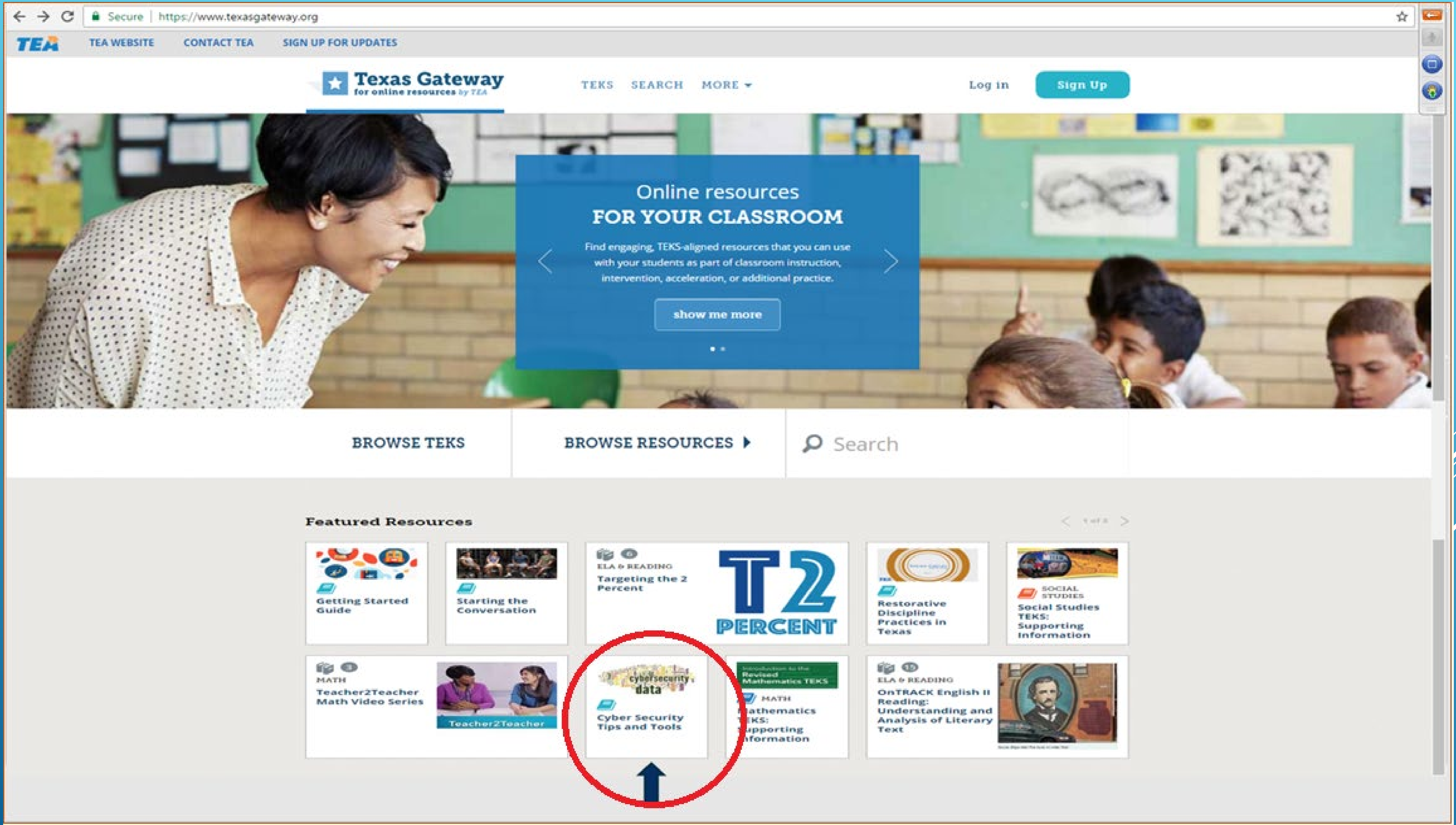
The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

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



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.

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
- Cyber Security Tips and Tools
- MATH — Mathematics TEKS: Supporting Information
- ELA & READING — OnTRACK English II Reading: Understanding and Analysis of Literary Text

LIFE CYCLE OF A CYBERSECURITY INCIDENT

- Discovery
- Assemble Incident Response Team (potentially led by 3rd party vendor)
- Internal Notification
- Investigate and Remediate (potentially led 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 led by 3rd party vendor)
- Begin notification process, procure protection services for affected
- Notification to affected parties (potentially led by 3rd party vendor depending on contract terms)
- Make public announcement with single point of contact (potentially led by 3rd party vendor depending on contract terms)
- Respond to inquiries
- Resume business as usual

Rule # 1 for Incident Response

Have a plan!

Where can I get a plan?

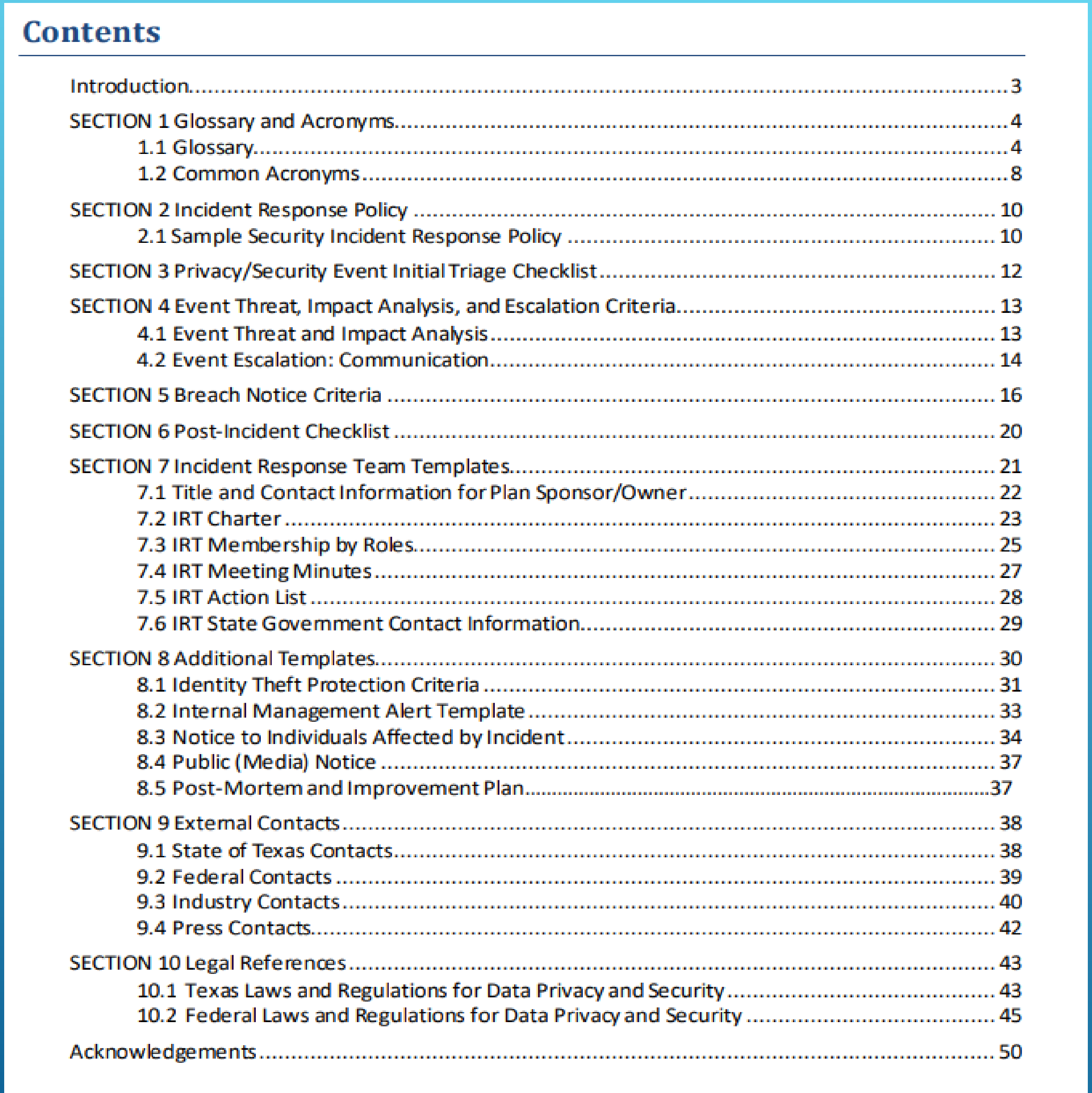
Texas DIR Incident Response Team Redbook

https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

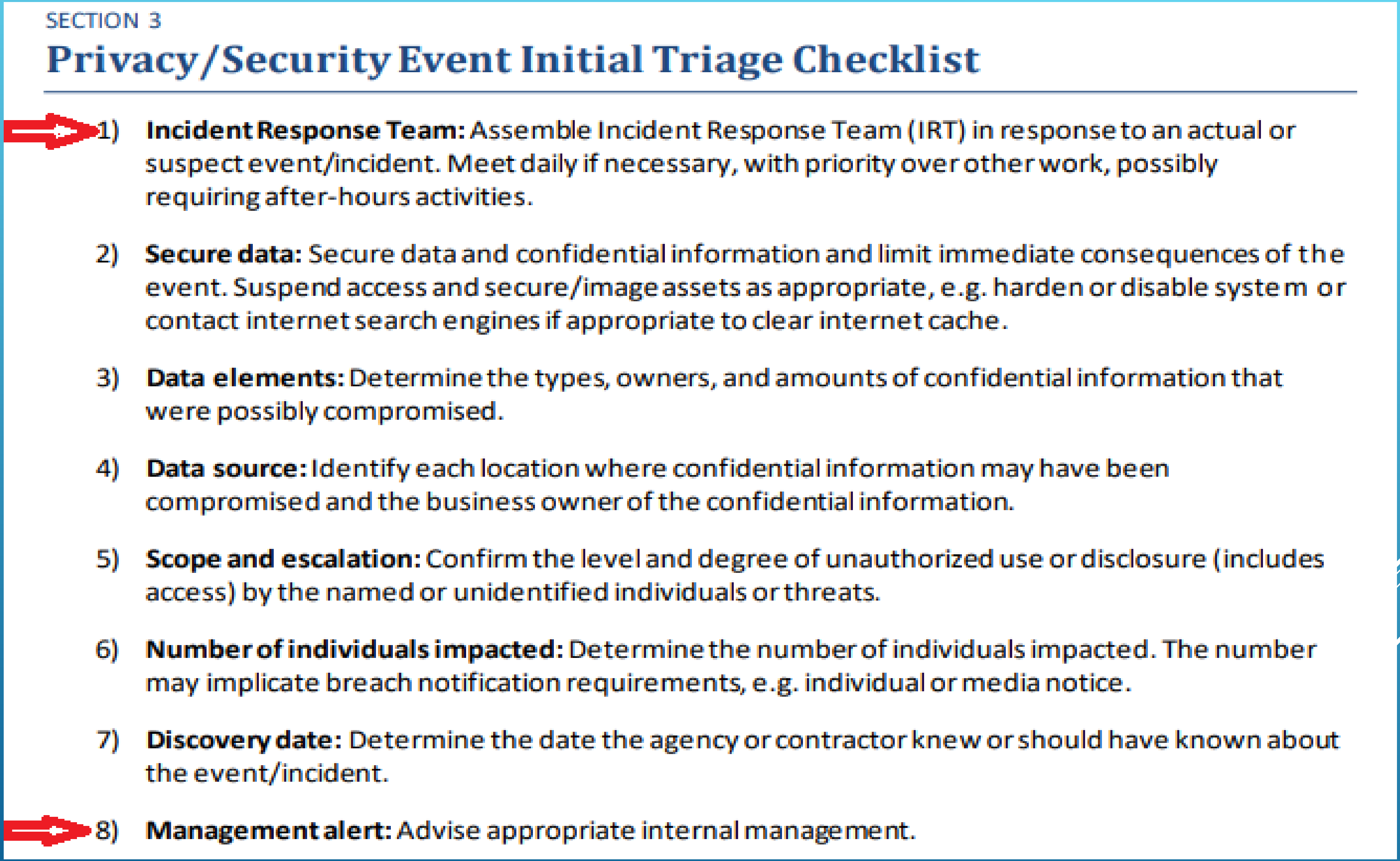
TEXAS DEPARTMENT OF INFORMATION RESOURCES

Incident Response Team Redbook

April 2019



Contents



SECTION 3

Privacy/Security Event Initial Triage Checklist

1) **Incident Response Team:** Assemble Incident Response Team (IRT) in response to an actual or suspect event/incident. Meet daily if necessary, with priority over other work, possibly requiring after-hours activities.

2) **Secure data:** Secure data and confidential information and limit immediate consequences of the event. Suspend access and secure/image assets as appropriate, e.g. harden or disable system or contact internet search engines if appropriate to clear internet cache.

3) **Data elements:** Determine the types, owners, and amounts of confidential information that were possibly compromised.

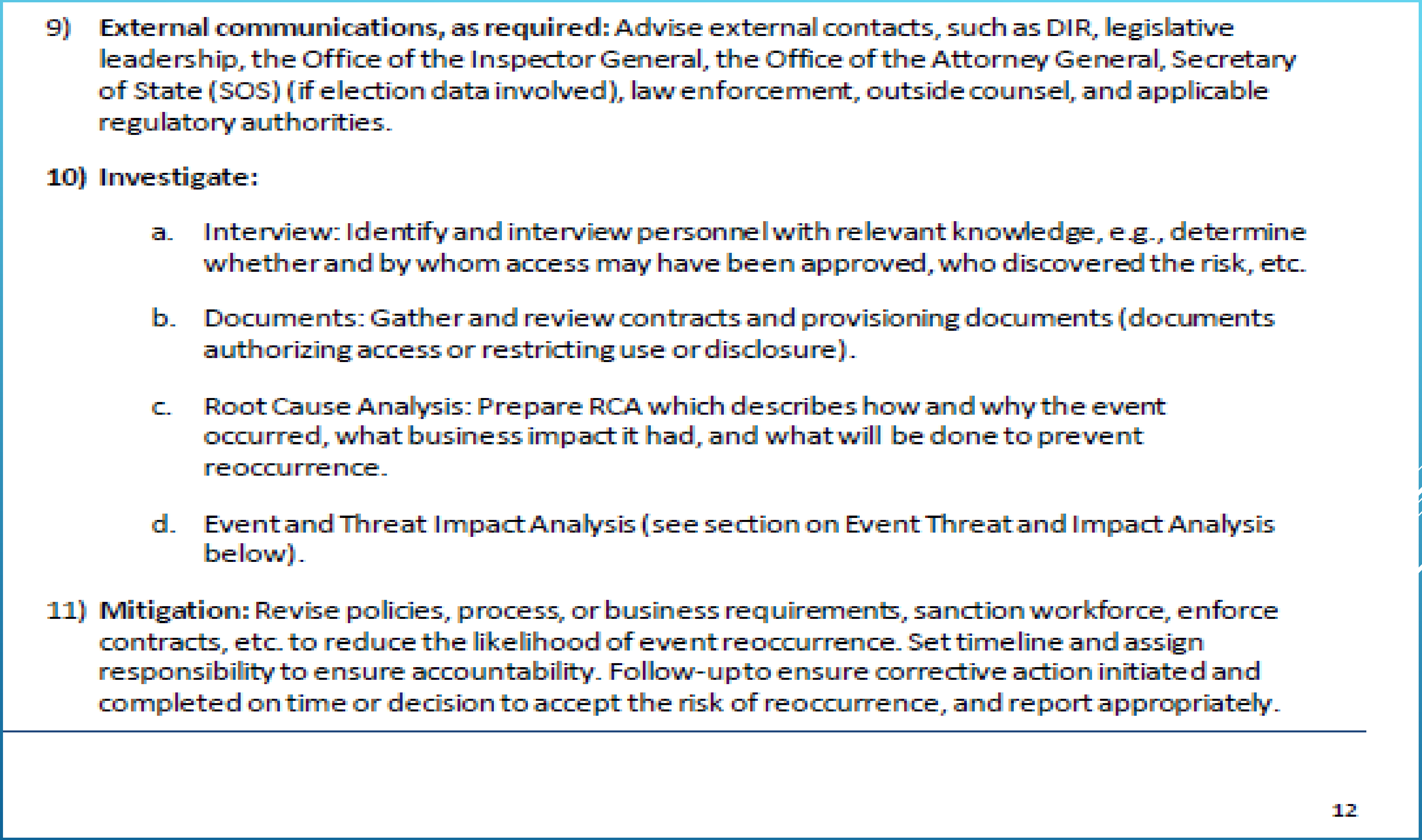
4) **Data source:** Identify each location where confidential information may have been compromised and the business owner of the confidential information.

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. The number may implicate breach notification requirements, e.g. individual or media notice.

7) **Discovery date:** Determine the date the agency or contractor knew or should have known about the event/incident.

8) **Management alert:** Advise appropriate internal management.



9) **External communications, as required:** Advise external contacts, such as DIR, legislative leadership, the Office of the Inspector General, the Office of the Attorney General, Secretary of State (SOS) (if election data involved), law enforcement, outside counsel, and applicable regulatory authorities.

10) **Investigate:**

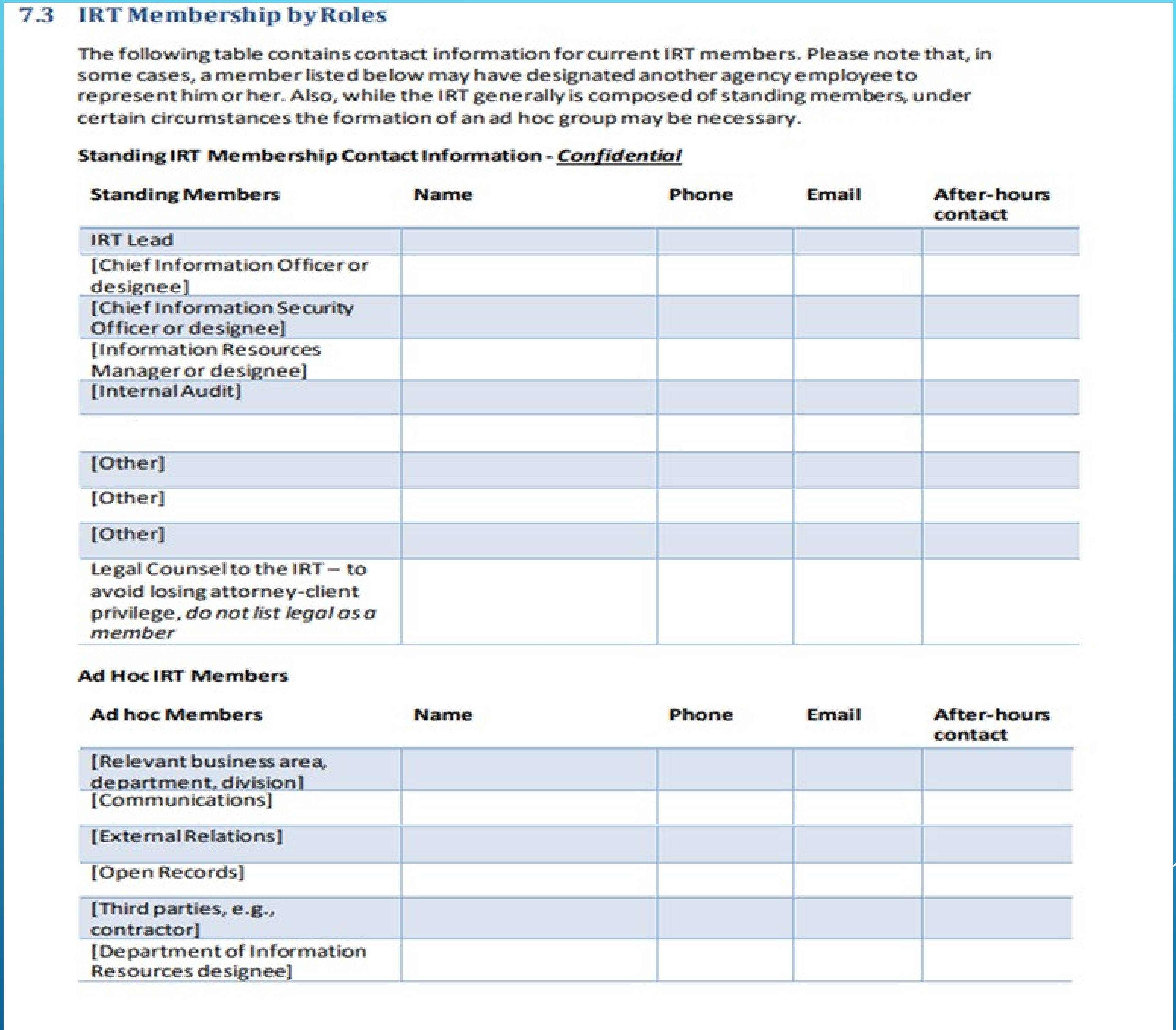
    a. Interview: Identify and interview personnel with relevant knowledge, e.g., determine whether and by whom access may have been approved, who discovered the risk, etc.

    b. Documents: Gather and review contracts and provisioning documents (documents authorizing access or restricting use or disclosure).

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

    d. Event and Threat Impact Analysis (see section on Event Threat and Impact Analysis below).

11) **Mitigation:** Revise policies, process, or business requirements, sanction workforce, enforce contracts, etc. to reduce the likelihood of event reoccurrence. Set timeline and assign responsibility to ensure accountability. Follow-upto ensure corrective action initiated and completed on time or decision to accept the risk of reoccurrence, and report appropriately.



7.3 IRT Membership by Roles

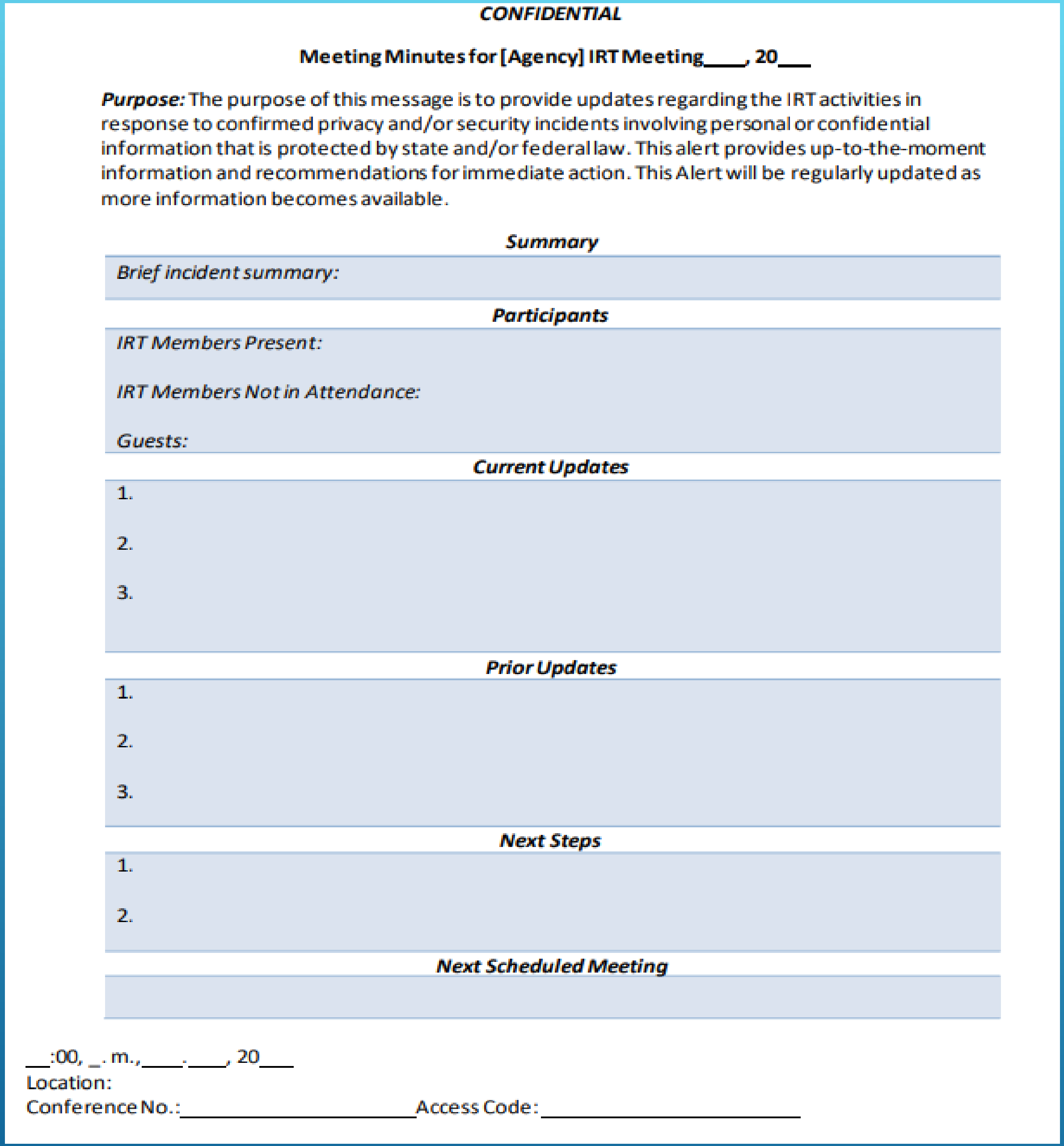
The following table contains contact information for current IRT members. Please note that, in some cases, a member listed below may have designated another agency employee to represent him or her. Also, while the IRT generally is composed of standing members, under certain circumstances the formation of an ad hoc group may be necessary.

Standing IRT Membership Contact Information - *Confidential*

Standing Members	Name	Phone	Email	After-hours contact
IRT Lead				
[Chief Information Officer or designee]				
[Chief Information Security Officer or designee]				
[Information Resources Manager or designee]				
[Internal Audit]				
[Other]				
[Other]				
[Other]				
Legal Counsel to the IRT – to avoid losing attorney-client privilege, *do not list legal as a member*				

Ad Hoc IRT Members

Ad hoc Members	Name	Phone	Email	After-hours contact
[Relevant business area, department, division]				
[Communications]				
[External Relations]				
[Open Records]				
[Third parties, e.g., contractor]				
[Department of Information Resources designee]				



CONFIDENTIAL

Meeting Minutes for [Agency] IRT Meeting____, 20___

Purpose: The purpose of this message is to provide updates regarding the IRT activities in response to confirmed privacy and/or security incidents involving personal or confidential information that is protected by state and/or federal law. This alert provides up-to-the-moment information and recommendations for immediate action. This Alert will be regularly updated as more information becomes available.

Summary

Brief incident summary:

Participants

IRT Members Present:

IRT Members Not in Attendance:

Guests:

Current Updates

1.

2.

3.

Prior Updates

1.

2.

3.

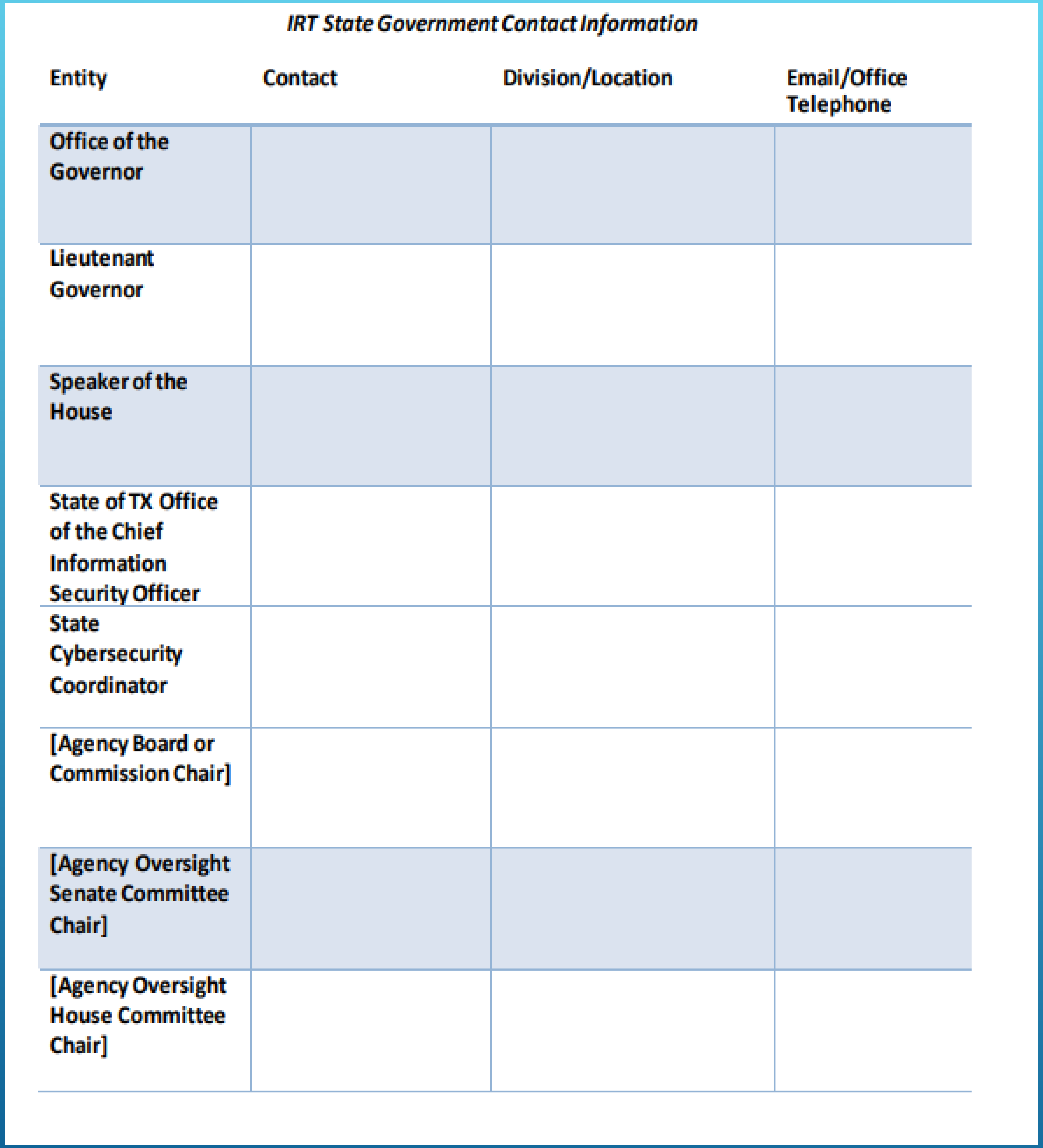
Next Steps

1.

2.

Next Scheduled Meeting

__:00, _. m.,____.____, 20___
Location:
Conference No.:____________________Access Code:______________________



IRT State Government Contact Information

Entity	Contact	Division/Location	Email/Office Telephone
Office of the Governor			
Lieutenant Governor			
Speaker of the House			
State of TX Office of the Chief Information Security Officer			
State Cybersecurity Coordinator			
[Agency Board or Commission Chair]			
[Agency Oversight Senate Committee Chair]			
[Agency Oversight House Committee Chair]			

Communication Escalation

Entity Contact	Name	Office Email	Pesonal Email	Phone
TEA				
ESC				
School Board Members				
Legal				
Superintendent				
Cybersecurity Insurance provider				
Principal				
Chief Technology Officer				
Cybersecurity Coordinator				

Rule # 2 for Incident Response

Know your plan!

Cybersecurity Tips and Tools –Incident Response, Being Prepared—Session 4

https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

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.

FIRST 24 HOUR CHECK LIST
(continued)

- 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.

Communications to Consider

- Alert Notifications
- Issue Investigation - Internal
- Findings Communications – Internal
- Remediation Communications -Internal
- Third Party Communications
- Leadership Communications – Internal
- Media Communications
- Breach Notification

Cybersecurity Tips and Tools – Crisis Communication during a Cybersecurity Incident – Session 10

https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

Rule # 3 for Incident Response

Practice your plan!

Cybersecurity Tips and Tools –Practice, Practice, Practice – Session 11

https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

Step by Step Playbook for a two-day exercise with Gap Analysis questions

Two simple exercises included on Texas Gateway portal

HB3834 Update

Security Awareness Training Certification (HB 3834)

https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154#list

This site will be updated weekly.

Vendor Training Programs

Training Program Name	Training Program Provider
Alterity Cybersecurity Awareness Program	Alterity Solution, Inc.
Security Awareness	Capgemini
Security Awareness Training	Encore Support Systems, LP
Security Awareness Essentials Challenge	Global Learning Systems
Security First Solutions - Elite	Inspired eLearning LLC
KnowBe4 Security Awareness Training	KnowBe4
Cyber Awareness	LeaderQuest Holdings, Inc
Linkedin Learning Cyber Security Courses	LinkedIn Corporation
Texas Association of Counties Cybersecurity Awareness Training	MediaPRO
ThreatAdvice Cyber-Security Education	NXTsoft Cyber Security Solutions
Optiv - Security Awareness Circuit Training	Optiv Security
Optiv - CyberBOT	Optiv Security
Optiv - Rapid Awareness	Optiv Security
CJIS Security Awareness Training	Peak Performance Solutions
TX-3834 SANS Security Awareness Program	SANS Institute
SCAN13 Training Program	SCAN13
Information Security: How To Recognize, Respond, and Prevent Threats to Your Data	Strategic Government Resources
Syntient Security Awareness Program	Syntient Systems, LLC.
PII Protect	Technology Assets, LLC. DBA, Global Asset

In-House Approved Training Programs

Training Program Name	Training Program Provider
Cybersecurity Awareness Training for Educators	ESC 16) Education Agency, Texas
CISD Cyber Security Awareness Training	Canyon ISD
Security and Accessibility Awareness Training	Coordinating Board, Higher Education
3001: Information Security Awareness	Texas A&M University System Administration
Information Security Basics	Texas Engineering Extension Service (A&M)
Cybersecurity Awareness Training	Texas Tech University
Cybersecurity Awareness Training	Texas Tech University System
Cybersecurity Awareness at TWC	Texas Workforce Commission
Cybersecurity at TxDOT	Transportation, Department of
Secure Our Systems	University of Houston, University of Houston - Clear Lake, University of Houston - Downtown, University of Houston - Victoria, University of Houston System Administration
SCT100 FY 2019-2020 Information Security Compliance	University of Texas at San Antonio
FY2020 Information Security Training	University of Texas Southwestern Medical Center

Questions?