Texas A&M University System

Information Security Incident Notification/Communication Matrix

Type of Information	Confidential			Internal Use			Notes
The Texas A&M University System maintains a data classification standard that is reflected here to assist readers of their responsibilities in notifying the correct personnel in the case of a breach of information as defined by the type of information breached.	Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement (1 TAC §202.1).			Information that is not generally created for or made available for public consumption but that may or may not be subject to public disclosure through the Texas Public Information Act or similar laws.			Notes that modify or clarify notification and communication with parties involved or affected. Affected member leadership is responsible for communicating initially to System-level SCIO and SCISO personnel who will then notify other responsible parties on the notification matrix.
Notified parties/Time line	24 hrs	48 hrs	72 hrs	24 hrs	48 hrs	72 hrs	
Chancellors' Office	X					X	Notification of the Chancellor's representative
SCIO	X				X		
SCISO	X			X			
Security Operations Center (Part 26)	X			X			
Chief Research Security Officer	X			X			Notify if applicable to research data
Agency/University President/Provost	X			X			
Agency/University CIO	X			X			
Agency/University ISO/CISO	X			X			
Agency/University Department head	X			X			
Office of General Counsel	X				X		
Vendors, Partners Affected		X				X	
Affected people (students, employees)			X			X	
SO Marcom	X				X		
Internal Audit	X				X		
Compliance	X				X		
Texas Department of Information Resources		X				X	SCISO to be copied on all communications to DIR for incidents
Law Enforcement		X			X		Only as needed. OGC would determine need to inform and involve
Office of Civil Rights	X						HIPAA-only data breach of 500 records or more. SCISO to determine.

Information Gathering and Evidence for Incident Response:

When notifying, have the following info:

		Potential Impact Related to Information Breach	
Who	Who was impacted?	**Low**	The unauthorized disclosure of information would be expected to have no or only slight adverse affect on the organzation's operations, assets or on individuals. This could include network probes or system scans, isolated virus infections and acceptable use violations.
What	What was breached, exposed, stolen or destroyed?		
When	When did it happen? What's the timeline? Can you determine when it was breached?		
Where/Source	Where did it happen? Are there another parties affected, such as a vendors?		
Why	Is there a reason why or is it known why the incident occurred?	**Moderate**	The unauthorized disclosure of information would be expected to have limited adverse effect on organizational operations, assets and indviduals. This would affect a small (less than 500) individuals. This would also include small-scale Denial-of-Service (DoS) attacks, website compromises and unauthorized access against FTP, ssh and other protocols.
How	How did it happen? Is it known or should internal and external investigation be initiated?		
Status	What's the status of the incident? Have we halted the incident or at least prevented additional information from being exposed, stolen or destroyed?		
Containment/Remediation	What's the plan for remediation? How quickly can we move on containment and remediation and eliminating the threat if it is ongoing?	**High**	The unauthorized disclosure of information would be expected to have severe or catastrophic adverse effect on organizational operations, assets or on individuals. This would be classed as information that would impact multiple organizations, including external partners, vendors and affiliates. This could also include large-spread compromises of sensitive data and malware code attacks.
Recovery	Once root cause has been identified and completed after remediation, how quickly can we recover to normal operation? What's the timeline to recover?		
Lessons Learned	Have we preserved evidence for analysis to perform a lessons learned? Do we need to involve outside parties, such as forensics investigators, to perform analysis to complete the lessons learned? Do we need to adjust our security posture and policies to prevent this incident from reoccurrance?		