PRAIRIE VIEW A&M UNIVERSITY

A Member of the Texas A&M University System

Security Incident Reporting Form

☐ **Check box if no incidents to report and complete contact information section only.**

Date Submitted: _____

Instructions: To enhance mutual support, Texas Administrative Code (TAC) 202.76 Security Incidents requires institutions of higher education to provide timely reporting of security incidents to the Texas Department of Information Resources (DIR) through the Information Security Officer (ISO). Each system administrator is responsible for assessing the significance of a security incident within their department and for submitting this report to the ISO based on the potential business impact on affected resources and the current or potential technical effect of the incident (e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks). Please use the following form to document all relevant security incident information.

Depending on the criticality of the incident, it may not always be feasible to gather all the information prior to reporting the incident to the ISO. In such cases, make an initial report and then continue to report information to the ISO as it is collected. All security incident reports provided to the ISO in response to TAC 202.76 requirements will be classified and handled as confidential per Texas Government Code Chapters 2059.055 Restricted Information and 552.139 Exception: Confidentiality of Government Information Related To Security or Infrastructure Issues For Computers.

If criminal action is suspected, (e.g., violations of Penal Codes Chapter 33 Computer Crimes, or Chapter 33A Telecommunications Crimes), the ISO is also responsible for contacting the appropriate law enforcement and investigative authorities.

1. Contact Information	
Full name:	
Job title:	
College/Department:	
Office:	
Work phone:	
Mobile phone:	
E-mail address:	
Fax number:	
Additional contact information:	

Information Security Officer
P.O. Box 519, Mail Stop 1460 | Prairie View, Texas 77446
Phone (936) 261-2126 | Fax (936) 261-9342

Revised May 2013

2. Type of Incident (Check all that apply)	
☐ Account compromise (e.g., lost password) ☐ Denial of service (including distributed) ☐ Malicious code (e.g., virus, worm, Trojan) ☐ Misuse of systems (e.g., acceptable use) ☐ Reconnaissance (e.g., scanning, probing)	☐ Social engineering (e.g., phishing, scams) ☐ Technical vulnerability (e.g., 0-day attacks) ☐ Theft/loss of equipment or media ☐ Unauthorized access (e.g., systems, devices) ☐ Unknown/Other (Please describe below)
Description of incident:	

3. Scope of Incident (Check one)	
☐ Critical (e.g., affects public safety or state-wide information resources) ☐ High (e.g., affects departments entire network or critical business or mission systems) ☐ Medium (e.g., affects departments network infrastructure, servers, or admin accounts) ☐ Low (e.g., affects departments workstations or user accounts only) ☐ Unknown/Other (Please describe below)	
Estimated quantity of systems affected:	
Estimated quantity of users affected:	
Third-parties involved or affected: (e.g., vendors, contractors, partners)	
Additional scope information:	

4. Impact of Incident (Check all that apply)	
☐ Loss of access to services ☐ Loss of productivity ☐ Loss of reputation ☐ Loss of revenue	☐ Propagation to other networks ☐ Unauthorized disclosure of data/information ☐ Unauthorized modification of data/information ☐ Unknown/Other (Please describe below)
Estimated total cost incurred: (e.g., cost to contain incident, restore systems, notify data owners)	
Additional impact information:	

Information Security Officer
P.O. Box 519, Mail Stop 1460 | Prairie View, Texas 77446
Phone (936) 261-2126 | Fax (936) 261-9342

Revised May 2013

5. Sensitivity of Affected Data/Information (Check all that apply)	
☐ Confidential/Sensitive data/info ☐ Non-sensitive data/info ☐ Publicly available data/info ☐ Financial data/info	☐ Personally identifiable information (PII) ☐ Intellectual property/copyrighted data/info ☐ Critical infrastructure/Key resources ☐ Unknown/Other (Please describe below)
Quantity of data/information affected: (e.g., file sizes, number of records)	
Additional affected data information:	

6. Systems Affected by Incident(Provide as much detail as possible)	
Attack sources (e.g., IP address, port):	
Attack destinations (e.g., IP address, port):	
IP addresses of affected systems:	
Domain names of affected systems:	
Primary functions of affected systems: (e.g., web server, domain controller)	
Operating systems of affected systems: (e.g., version, service pack, configuration)	
Patch level of affected systems: (e.g., latest patches loaded, hotfixes)	
Security software loaded on affected systems: (e.g., anti-virus, anti-spyware, firewall, versions, date of latest definitions)	
Physical location of affected systems: (e.g., state, city, building, room, desk)	
Additional system details:	

Information Security Officer
P.O. Box 519, Mail Stop 1460 | Prairie View, Texas 77446
Phone (936) 261-2126 | Fax (936) 261-9342

Revised May 2013

7. Users Affected by Incident (Provide as much detail as possible)	
Names and job titles of affected users:	
System access levels or rights of affected users: (e.g., regular user, domain administrator, root)	
Additional user details:	

8. Timeline of Incident (Provide as much detail as possible)	
a. Date and time when College/Department first detected, discovered, or was notified about the incident:	
b. Date and time when the actual incident occurred: (estimation if exact date and time unknown)	
c. Date and time when the incident was contained, or when all affected systems or functions were restored: (use whichever date and time is later)	
Elapsed time between the incident and discovery: (e.g., difference between a. and b. above)	
Elapsed time between the discovery and restoration: (e.g., difference between a. and c. above)	
Detailed incident timeline:	

9. Remediation of Incident (Provide as much detail as possible)	
Actions taken by College/Dept. to identify affected resources:	
Actions taken by College/Dept. to remediate incident:	
Actions planned by College/Dept. to prevent similar incidents:	
Additional remediation details:	

Information Security Officer
P.O. Box 519, Mail Stop 1460 | Prairie View, Texas 77446
Phone (936) 261-2126 | Fax (936) 261-9342

Revised May 2013

10. Miscellaneous (Provide any other relevant information)
Additional information:

Please submit* completed form to:

miasghar@pvamu.edu
Information Security Officer
Harrington Science, Suite 311
Prairie View, Texas 77446

To immediately report an incident, please contact:

Midhat Asghar
miasghar@pvamu.edu
Office (936) 261-2156
Fax (936) 261-9432

*PLEASE NOTE: All Security Incident Reporting Forms and accompanying documentation must be transmitted in a safe and secure manner.