Computer Security

Incident Response Plan (CSIRP)

LOGO

Information Services
District

Purpose:

The purpose of a Computer Security Incident Response Plan (CSIRP) is to provide the District with a plan that outlines how XXXX County Schools will respond in the event of a computer security incident (or suspected incident). A computer security incident is an event involving district-owned computer resources that threatens confidentiality, integrity or availability of District information assets.

Scope:

This CSIRP applies to all information technology devices, systems and networks owned or used by XXXX. The Information Services department will take all actions necessary to assure the protection of XXXX information technology resources and data that reside under XXXX control.

Roles and Responsibilities:

Computer security may occur at any time and require full support from District staff as well as leadership from schools and departments to manage the outcome. Various roles and responsibilities must be fulfilled to ensure that appropriate leadership and technical resources are involved in successfully resolving an incident and minimizing damage to the District.

Within this section, the roles and responsibilities during a computer security incident are defined for the Director of IT and others involved (Computer Security Incident Response Team—CSIRT) in investigation and response to a computer security incident

The Director of IT is responsible for executing or delegating the following:

a) Setting priorities.
b) Notifying the Superintendent that a high priority incident has occurred.
c) Participating with any forensic investigation decisions.
d) Managing incident resources.
e) Notifying Community Relations as appropriate for internal and external communication
.f) Notifying Human Resources as appropriate.
g) Notifying Legal Counsel as appropriate.
h) Activating the CSIRT when the level of the incident warrants activation.

The CSIRT is responsible for the following:

a) Updating the Director of IT on a regular basis during a critical incident.
b) Creating and updating the incident report, collect and document the case (as needed).
c) Declaring the security incident and its severity if appropriate.
d) Determine the root cause of the incident.
e) Working closely with the Director of IT and Legal during forensic investigations.
f) Identifying external personnel/resources as needed.
g) Working to bring all systems back to operational quality.
h) Ensuring destruction/retention of all materials at incident's close.
i) Escalating the incident's severity if warranted.
j) Ensuring that proper follow-up debriefing and reporting occur.

k) Adjusting procedures so that responses to future incidents are improved.

The CSIRT may be composed of different individuals, including but not limited to:

a) IT Director.
b) Director for Network/Operations Services.
c) IT staff based on the type of platform (Windows, Mac, Linux, etc.) that was affected.
d) Webmaster for Internet or Web service related incidents.
f) Server Administrators and/or Network Administrators (when appropriate).

The CSIRT will be convened if the security incident:

a) Is likely to become public knowledge.
b) Places individuals at risk of identity theft, financial loss, or other negative consequences.
c) Significantly impacts the District's services, resources, or external relationships.
d) Represents a significant threat to other organizations, local communities, or the nation.
e) Disrupts core IT services, leading to a notable cessation of business or academic services.

Training:

The Computer Security Incident Response Team (CSIRT) should receive training each year (or as needed) to ensure new team members are familiar with this Directive and how to respond when an incident occurs.

A security incident may also involve any or all of the following:

- A violation of District computer security policies and standards.
- Unauthorized computer access or system malfunction that creates a security concern.
- Loss of information confidentiality.
- Loss of information availability.
- Compromise of information integrity.
- A denial of service attack or virus.
- Misuse of service, systems or information.
- Physical or logical damage to systems.
- Unauthorized release of student or staff Personally Identifiable Information.
- A violation of state or federal laws that related to Information Security (i.e. FERPA, CIPA, etc.).

Security incident preparation:

IT has multiple preventative, detective, recovery controls, and procedures in place depending on the 'security incident' classification and priority level of incident. This ensures that the security incident is responded appropriately. These controls and policies are detailed in documents such as the Computer Use Manual, Disaster Recovery Plan, AUP and other XXXX documents and procedures.

Security incident reporting:

All suspected or confirmed computer security incidents within the District will be subject to a reporting requirement. The Director of IT (or his/her designee) will assign an incident priority based on the Security Incident Priority Classification Table (if able). The initial priority level may be escalated or de-escalated by the IT. This initial incident priority helps to determine support staff and management engagement in a reported security incident. Employees must not attempt to repair or rebuild a possibly compromised computer system without authorization from IT.

Security incident classification:

All computer security incidents within the District will be subject to classification. Security incident classification assists staff to determine the severity and criticality of the security incident and ensure that the event receives the resource level attention relative to the incident priority. The classification also ensures that the security incident is reported to the appropriate manager, consistent with the priority of the security incident.

Security Incident Priority Classification Table

Incident Factors	Security Incident Report Priority Level		
	Low (1)	Med (2)	High (3)
Unauthorized computer access, misuse or user permission issue		X	
Computer/system theft, damage or loss		X	
Hacking or system breach to core systems			X
Malicious Denial of Service Attack or other attempt to interrupt normal operations		X	
Unauthorized release of Personally Identifiable Information (PII) (Student or Staff)			X
Violation of School Board rules, directives or policies that relate to computer security	X		
User system virus or malware detected	X		

Security incident reporting procedure:

- The following steps should be taken if a suspected security incident is discovered:
- Within (1) day or upon incident or suspected incident discovery, call IT Help Desk and provide a real-time report of the concern or incident. IT will help determine if the reported incident is valid and related to computer security.
- IT will contact appropriate District Executive leadership of level 2 or 3 incidents.
- The District will adhere to FS 501.171 (Security of Personal Information) for breaches affecting 500 or more individuals.
- Document the incident. Depending upon the incident, the following are areas for consideration in the documentation of the incident:
  - Indicate how the records or sensitive data (digital or hard copy) were lost, stolen or disclosed?
  - Explain how the incident occurred.
  - Identify what types of data elements were compromised? (i.e. SSN, student grades, etc.)
  - Identify how many students or employees were affected?
  - Identify what you believe is the cause of the incident?
  - Date and time of incident discovery.
  - General description of the incident.
  - Systems and/or data at possible risk.
  - Actions they have taken since incident discovery.

Basic Security Incident Reporting Elements

Information to Record	Description
References	Use the assigned Web Help Desk Ticket number or submit a new ticket
Suggested Priority	Level Low, Medium, High
Type of Incident	Note all types that apply: 1. Compromised System 2. Compromised User Credentials 3. Network Attacks (DOS, Scanning, Sniffing) 4. Malware (Viruses, Worms, Trojans) 5. Lost Equipment/Theft 6. Physical Break-in 7. Social Engineering (Phishing) 8. Law Enforcement Request 9. Policy Violation 10. Loss of Personal Identifiable Information (Student/Employee)
Incident Timeline	Date/time that the incident was discovered Date/time that the incident was reported Date/time that the incident occurred (if known)
Who or what reported the event	Contact Information for the Incident Reporter: full name, E Number, District department, email address, phone number, location If an automated system reported the event include the name of software package, Name of the host where the software is installed, physical location of the host, host or CPU ID of the host, network address of the host, and MAC address of the host if possible.
Identification of the host(s)	List contact information for all parties involved in the incident.
Incident Handling Action Log	Include: actions taken, when, by whom
Physical Security Controls	If there is limited physical access to the computer, document the physical security controls that limit access (ask the person reporting the event to describe what they have to do to access the computer).