Cyber Incident Response & Recovery Framework

This framework defines the structured lifecycle for responding to and recovering from cyber incidents within an educational environment. It guides technology leaders and key stakeholders through the essential steps to contain threats, restore critical systems, and return operations to normal. The plan is designed to be both comprehensive in addressing security challenges and practical for swift, coordinated action.

LTC Learning Technology Center

Contents

1. CIRR Plan Foundation and Authority

Policy Statement	A formal statement of the school district's commitment to cybersecurity, incident management, and protecting its digital infrastructure and sensitive information assets.
Purpose & Goals	Define the primary objectives of the plan: to swiftly detect, respond to, and recover from cybersecurity incidents to ensure the continuity of educational services and protect against disruptions.
Scope & Authority	Specify the organizational scope, the types of incidents covered (e.g., data breaches, malware, phishing), and the authority granted to the Incident Response Team (IRT) to take necessary actions.
Definitions & Terminology	A glossary of key terms to ensure a common understanding among all educational staff, administrators, and IT personnel.

2. Incident Response Team (IRT)

Team Structure (Cross-Functional)	Define the core members of the IRT and their specific roles. The team must be cross-functional, including IT professionals, administrators, legal counsel, and communication experts, etc., to bring diverse skills and perspectives to the response.
Roles & Responsibilities	Clearly outline the duties of each team member during an incident. This includes the designated IRT Lead (for overall command), IT Lead (ex. forensic analysis and restoration), Communications Lead (ex. internal/ external messaging), and representatives from IT department, legal, human resources, public relations, and executive leadership.
External Contacts	List contact information for external stakeholders and partners, such as cyber insurance, law enforcement, legal counsel, and third-party forensic experts who may provide additional support.

Communication Channels	Specify the primary and secondary communication methods for the IRT to use during an incident, including secure channels for sharing sensitive information.

3. Communication Plan

Communication Strategy	Define clear protocols for notifying all stakeholders, including staff, students, parents, and regulatory authorities, about the incident. Ensure the communication plan details what information is released at specific points during and after an incident.
Internal Communication	Outline the process for communicating with employees, leadership, and the school board. Ensure communication is handled by designated spokespersons.
External Communication	Specify the process for engaging with external parties, including parents, media, and regulatory bodies. Ensure communication is consistent, accurate, and timely, and adheres to legal requirements, such as data breach notification laws.
Templates & Holding Statements	Include pre-approved templates for various communication scenarios to ensure consistent and timely messaging. Have the district's legal representation review all communication templates.

4. Incident Response Lifecycle

An effective plan should follow a structured lifecycle to ensure all necessary steps are taken in a coordinated manner.

PHASE 1: PREPARATION	
IR Capability Development (Training & Exercises)	Provide ongoing training and awareness programs for the Incident Response Team (IRT), staff, and students. Conduct tabletop exercises and simulated scenarios (e.g., phishing campaigns, security awareness drills) to test the plan and identify areas for improvement.
Tooling & Infrastructure	Ensure firewalls, intrusion detection systems, anti-malware software, and other security tools are properly configured, monitored, and regularly updated.
Assessment & Documentation	Regularly evaluate cybersecurity posture and maintain up-to-date documentation of network architecture, asset inventories, and system configurations.
Data Inventory & Risk Assessment	Identify and classify critical data and systems, and conduct risk assessments to evaluate potential threats (e.g., malware, hardware failures, natural disasters).
Backup Strategy & Schedule	Define what data will be backed up, how often, and where (including secure off-site storage).
Testing & Recovery Procedures	Document data recovery processes and routinely test them to ensure staff can execute them effectively.
Contingency Planning	Establish procedures for restoring mission-critical functions and verify the integrity of backup data before restoration.

PHASE 2: DETECTION AND ANALYSIS This phase focuses on identifying and confirming that a security event is a genuine incident.	
Event Monitoring	Provide ongoing training and awareness programs for the Incident Response Team (IRT), staff, and students. Conduct tabletop exercises and simulated scenarios (e.g., phishing campaigns, security awareness drills) to test the plan and identify areas for improvement.
Initial Triage (Categorization and Severity)	Ensure firewalls, intrusion detection systems, anti-malware software, and other security tools are properly configured, monitored, and regularly updated.
Incident Confirmation	Analyze data and evidence to confirm the event as a security incident and classify its type and priority.
PHASE 3: CONTAINMENT, FORENSICS, ERADICATION, AND RECOVERY This phase involves a series of coordinated actions to limit the impact, preserve forensic data, and restore normal operations.	
Containment	Immediately implement short-term and long-term strategies to limit the spread of the incident (e.g., network isolation, account deactivation).
Forensics	Collect and store data for post-incident review of scope, origin, and method of compromise.
Eradication	Identify the root cause of the incident, remove all malicious artifacts, and patch vulnerabilities to prevent recurrence.
Recovery	Restore affected systems and data to a validated, secure state, and conduct thorough testing to ensure functionality and security before returning to production. This includes implementing backups and recovery strategies defined in the DR plan.

5. Disaster Recovery

PHASE 1: INITIAL ASSESSMENT	
Prioritize Critical Systems	Restore essential business-critical systems first (e.g., identity services, payment processing, core databases) based on the Business Impact Analysis (BIA).
Determine Recovery Point Objective (RPO)	Identify the last known point in time when systems and data were clean and uncompromised, often requiring forensic analysis to confirm the time of initial breach.
Validate Recovery Environment	Ensure segregated, clean infrastructure (network segments, servers) is ready for restoration, preventing re-infection.
PHASE 2: RESTORATION AND RECONSTRUCTION	
Verify Backup Integrity	Test the accessibility and integrity of backups dating back to the defined RPO. Confirm that backup media has not been tampered with or encrypted by the attacker.
Wipe and Reimage	Instead of attempting to clean compromised systems, securely wipe and reimage affected devices and servers using verified, hardened operating system images.
Restore Data	Transfer validated backup data onto the newly rebuilt systems. Maintain a meticulous log of all restored files and system configurations.
PHASE 3: POST-RESTORATION SECURITY HARDENING	
Apply Patches and Updates	Ensure that all restored systems have the latest security patches and configurations immediately.
Reset Credentials	Force a mass reset of all system and service account passwords, paying special attention to domain administrator and highly privileged accounts. Implement stronger multi-factor authentication (MFA).

Integrity Checks	Run comprehensive antivirus/endpoint detection and response (EDR) scans on all restored data and systems to verify the eradication of the threat.
Enhanced Monitoring	Place all restored systems under intensive monitoring (logging, network traffic analysis, unusual activity alerts) to quickly detect any residual or recurring threat activity.

6. Post-Incident Activity

After-Action Review (AAR)	Hold a formal review with the IRT and key stakeholders to analyze the incident, identify successes, and areas for improvement.
Incident Report	Document a detailed report of the incident's timeline, impact, technical analysis, and the full response effort.
Forensics Review	This involves reviewing logs, traffic, and endpoint data to reconstruct the attack and understand the attacker's behavior. Sound forensic practices preserve evidence for legal or disciplinary use and provide insights to guide eradication, recovery, and prevention.
Plan Updates	Review and update the plan based on the outcomes of exercises and lessons learned from real incidents.