Marion Community Unit School District # 2
Rebecca Moss, Superintendent
1700 West Cherry Street
Marion, IL 62959
Ofc. 618-993-2321 Fax 618-997-0943

Cybersecurity Incident Response Plan (CIRP) for Marion CUSD #2

1. Introduction
Marion CUSD #2 recognizes that cybersecurity threats pose a significant risk to the confidentiality, integrity, and availability of digital systems, data, and operations. This Cybersecurity Incident Response Plan (CIRP) provides a structured framework for detecting, responding to, managing, and recovering from network or cyber incidents, including ransomware attacks, data breaches, unauthorized access, phishing attempts, and denial-of-service (DoS) attacks. This plan ensures timely and coordinated action to minimize impact, restore services, and maintain trust.

2. Objectives
• Protect Critical Assets: Safeguard student and staff data, networks, and technology systems.
• Minimize Disruption: Quickly contain and recover from cyber incidents to reduce disruption to educational services.
• Ensure Effective Communication: Provide timely, clear, and accurate information to stakeholders.
• Promote Compliance: Adhere to federal and state laws including FERPA, HIPAA, and cybersecurity standards.
• Enable Continuous Improvement: Identify lessons learned to strengthen future preparedness and defenses.

3. Cyber Incident Response Team (CIRT)
The Cyber Incident Response Team (CIRT) is responsible for executing this plan. Key roles include:
• Incident Commander (IC): District Technology Director or Superintendent's designee. Leads all cyber incident response activities.
• IT Security Lead: Manages technical diagnosis, containment, eradication, and recovery processes. (Third Party Team supplied by Cyber Insurance Company or by Marion CUSD #2)
• Public Information Officer (PIO): Handles communication with parents, staff, media, and the community.
• Compliance Officer: Ensures regulatory requirements (FERPA, HIPAA, etc.) are met during the response.
• Legal Advisor: Provides legal guidance and support for breach notification and liability issues.
• Backup and Recovery Lead: Oversees data restoration and infrastructure recovery efforts. (Third Party Team supplied by Cyber Insurance Company or by Marion CUSD #2)

4. Incident Identification and Classification
Cyber incidents will be categorized by severity:
• Low: Suspicious emails, non-malicious policy violations.
• Moderate: Malware infections, failed login attempts, internal privilege misuse.
• High: Ransomware, major data breach, successful phishing attack with data exposure.
• Critical: Widespread system compromise, exfiltration of sensitive student/staff data, or attack on critical infrastructure.
All suspected incidents must be reported immediately to the Technology Department.

Marion Community Unit School District # 2
Rebecca Moss, Superintendent
1700 West Cherry Street
Marion, IL 62959
Ofc. 618-993-2321 Fax 618-997-0943

5. Cyber Incident Response Procedures
5.1 Detection and Initial Response
• Identify and validate indicators of compromise (e.g., system anomalies, alerts).
• Notify the Incident Commander and activate the CIRT if escalation is warranted.
• Begin incident logging and time-stamped documentation.

5.2 Containment
• Isolate affected systems from the network.
• Disable compromised accounts and services.
• Apply temporary firewall rules or network segmentation as needed.

5.3 Eradication
• Remove malicious code and backdoors.
• Patch vulnerabilities and change credentials.
• Perform a thorough forensic investigation if data theft is suspected.

5.4 Recovery
• Restore systems from clean backups.
• Test all systems to verify integrity before reconnecting to the network.
• Monitor for signs of reinfection or ongoing compromise.

5.5 Communication
• The PIO will issue stakeholder notifications per compliance guidelines (e.g., data breach notification laws).
• Communicate only verified facts; avoid speculation.
• Use secure and approved communication channels for internal briefings.

5.6 Post-Incident Review
• Conduct a full after-action review within 10 business days.
• Document lessons learned, update the CIRP, and retrain staff if necessary.

6. Training and Awareness
• Annual Cybersecurity Training: Mandatory for all staff to recognize threats like phishing, ransomware, and social engineering.
• Simulated Attacks: Periodic phishing simulations and tabletop exercises for CIRT members.
• Policy Review: Annual review of acceptable use policies and incident procedures.

7. Communication Protocols
During a cyber-incident:
• Internal Alerts: Secure messaging/email systems for internal updates.
• External Messaging: District website and phone system for public notifications.
• Press Management: The PIO coordinates media responses to avoid misinformation.
• Data Breach Notifications: Issued per Illinois breach notification laws and FERPA/HIPAA regulations.

8. Legal and Regulatory Compliance
All actions must comply with:

Marion Community Unit School District # 2
Rebecca Moss, Superintendent
1700 West Cherry Street
Marion, IL 62959
Ofc. 618-993-2321 Fax 618-997-0943

- FERPA – Ensuring the protection of student educational records.
- HIPAA – Safeguarding any protected health information.
- Illinois Personal Information Protection Act (PIPA) – Governing breach notifications.
- Children's Internet Protection Act (CIPA) – Enforcing safe and secure internet use in schools.
- NIST Cybersecurity Framework – Serving as the reference standard for security controls and incident handling.

9. Plan Maintenance and Review
- This CIRP will be reviewed annually or following any significant cyber event.
- Updates will be made based on threat landscape changes, legal requirements, and technological advancements.