CyberSphere SOLUTIONS

Incident Response Flowchart for Schools

A Step-by-Step Guide to Managing Cybersecurity Incidents

01 DETECT

Goal: Identify unusual or suspicious activity as early as possible.
Examples:

- Unexpected file encryption or pop-ups (ransomware)
- Reports of phishing emails
- Slow network performance or system lockouts
- Unauthorized access attempts

Actions:

- Monitor alerts from security tools, firewalls, and endpoint protection.
- Verify the issue by checking system logs and user reports.
- Notify the IT lead immediately.

02 CONTAIN

Goal: Prevent the spread of the threat.
Actions:

- Disconnect infected or suspicious devices from the network.
- Disable compromised user accounts.
- Block malicious domains or IPs on the firewall.
- Preserve evidence — do not wipe or reimage devices yet.

03 ERADICATE

Goal: Remove the source of the incident and ensure it cannot return.
Actions:

- Remove malware or unauthorized software.
- Apply patches or firmware updates that address vulnerabilities.
- Reset passwords and enable Multi-Factor Authentication (MFA) if not already active.
- Verify that backup systems and other endpoints are unaffected.

04 RECOVER

Goal: Safely restore systems, data, and services to normal operation.
Actions:

- Restore data from verified, clean backups.
- Reconnect systems to the network gradually, monitoring performance and security logs.
- Test core functions (email, Wi-Fi, SIS, etc.) to confirm stability.
- Continue monitoring for several days after recovery.

05 REPORT

Goal: Ensure transparency and accountability following an incident.
Actions:

- Document all actions taken, times, and individuals involved.
- Notify school leadership and administration.
- If student or staff data is affected, inform parents as required by policy and Florida data protection laws.
- Report significant incidents to local authorities or the Archdiocese IT leadership if applicable.
- Conduct a post-incident review to identify lessons learned.

POST-INCIDENT-FOLLOW UP

- Conduct a post-mortem review with IT and leadership within one week.
- Update security configurations and policies to prevent recurrence.
- Provide refresher training to staff and faculty if human error contributed.
- Archive incident documentation for recordkeeping and compliance.

305-518-1788
cyberspheresolutions.tech
info@cyberspheresolutions.tech