

Cyber Incident Response Guidance

Due to the sensitive nature of school data collection combined with limited resources for cybersecurity and gaps in digital defenses, cyber-attacks on schools are becoming increasingly common. **The best way to limit the impact of such attacks is to have a robust incident response plan in place and practice it as regularly as a fire drill.** An incident response plan provides a structured approach to detecting, containing, and recovering from cyber incidents, ensuring schools can act quickly to protect sensitive information, minimize downtime, and prevent future breaches.

ACT NOW

A - Assess the Situation: Evaluate the scope and severity of the attack as quickly as possible.

C - Contain the Breach: Isolate affected systems to stop unauthorized access or data loss. (if applicable)

T - Tell Authorities: Notify leadership, and relevant cybersecurity (i.e. the Cybersecurity & Infrastructure Security Agency – CISA) and law enforcement agencies if there is possible criminal activity involved.

N - Notify Stakeholders: Inform parents, students, and staff about the breach.

O - Organize Recovery: Secure systems, restore backups, and patch vulnerabilities to resume operations.

W - Work on Prevention: Review the incident, update policies, and strengthen defenses to prevent future incidents.

The graphic is a dark blue poster with white and light blue text and icons. It is divided into two main sections: 'ACT' and 'NOW'. The 'ACT' section is at the top and contains three items: 'Assess the Situation' (with a magnifying glass icon), 'Contain the Breach' (with a folder icon), and 'Tell Authorities' (with a scale icon). The 'NOW' section is at the bottom and contains three items: 'Notify Stakeholders' (with a speech bubble icon), 'Organize Recovery' (with a network icon), and 'Work on Prevention' (with a hand icon). The text 'ACT NOW: Cyber Incident Response Guide' is prominently displayed in the center, with the Maine DOE logo to the right. At the bottom, there is a small line of text: 'For additional information, contact: DOE-LTT@maine.gov | Maine Department of Education'.

ACT

Assess the Situation
Evaluate the scope and severity of the attack as quickly as possible.

Contain the Breach
Isolate affected systems to stop unauthorized access or data loss.

Tell Authorities
Notify leadership and relevant cybersecurity and/or law authorities.

ACT NOW: Cyber Incident Response Guide Maine DOE

NOW

Notify Stakeholders
Inform parents, students, and staff about the breach.

Organize Recovery
Secure systems, restore backups, and patch vulnerabilities to resume operations.

Work on Prevention
Review the incident, update policies, and strengthen defenses.

For additional information, contact: DOE-LTT@maine.gov | Maine Department of Education

[Link to Graphic](#)

Additional Resources

- [CISA K12 Cybersecurity](#)
- [Infrastructure Support | Department of Education](#)
- [K12 CyberStorm! \(2024 CISA/DOE/METDA Incident Response Planning Webinar\)](#)

For further information on developing an annex or exercising an incident response plan, contact the Maine School Safety Center (MSSC) and Maine DOE's Infrastructure Specialist at: james.chasse@maine.gov. You can also report incidents to the Maine Information Analysis Center, (MIAC) via MIAC.MSP@Maine.gov