SurfWisely™ Cybersecurity Incident Response Plan Checklist for Schools

Incident Response Team (IRT)

- ☐ Incident Response Coordinator: [Name] - [Contact]
- ☐ IT Security Lead: [Name] - [Contact]
- ☐ School Administration Representative: [Name] - [Contact]
- ☐ Legal/Compliance Officer: [Name] - [Contact]
- ☐ Communications Lead: [Name] - [Contact]
- ☐ Third-Party Cybersecurity Consultant (if applicable): [Name] - [Contact]

Incident Classification

- ☐ Phishing Attack: Attempt to steal credentials via email (Low-Medium)
- ☐ Ransomware Attack: System files encrypted, ransom demanded (High)
- ☐ Data Breach: Unauthorized access to sensitive data (High)
- ☐ DDoS Attack: Overloading school network to disrupt services (Medium-High)
- ☐ Malware Infection: Unauthorized software compromises systems (Medium)

Incident Response Workflow

- ☐ Detection & Identification
  - ☐ Monitor: Use security tools to identify unusual activity.
  - ☐ Report: Staff and students report suspicious activity to [IRT Contact].
  - ☐ Verify: IT team confirms if the activity is a legitimate threat.
- ☐ Containment
  - ☐ Isolate affected systems to prevent further spread.
  - ☐ Disable compromised accounts or credentials.
  - ☐ Limit internet connectivity if necessary.
- ☐ Eradication
  - ☐ Remove malware or unauthorized access.
  - ☐ Patch vulnerabilities and update software.
  - ☐ Revoke stolen credentials and enforce password changes.
- ☐ Recovery
  - ☐ Restore systems from secure backups.
  - ☐ Monitor affected networks for abnormal activity.
  - ☐ Confirm full system integrity before resuming operations.

- ☐ Post-Incident Review
  - ☐ Debrief with IRT to assess response effectiveness.
  - ☐ Document lessons learned and update CIRP.
  - ☐ Conduct staff training to prevent future incidents.

Cybersecurity Incident Response Plan Checklist for Schools

Internal Communication

- ☐ Alert school leadership and IT staff.
- ☐ Notify faculty and staff if necessary.
- ☐ Ensure secure communication channels (e.g., encrypted emails, phone calls).

External Reporting

- ☐ Law enforcement: Contact local cybercrime unit or FBI if necessary.
- ☐ Parents & community: Prepare a clear, non-alarmist statement.
- ☐ Regulatory bodies: Notify state and federal agencies if legally required.

Preventative Measures

- ☐ Cybersecurity awareness training for staff and students.
- ☐ Access Controls: Restrict permissions based on role necessity.
- ☐ Muti-factor Authentication (MFA)
- ☐ Regular system audits and penetration testing.
- ☐ Secure storage of offline backups.

For further questions or to report a cybersecurity issue, contact [insert incident response coordinator here] at [Email/Phone].