CyberSphere SOLUTIONS

Cybersecurity Plan Template for Schools

Building a Culture of Safety and Responsibility in Education

1. Policy Overview & Scope

This cybersecurity plan outlines the measures and practices our school will follow to safeguard its digital infrastructure, protect sensitive data, and ensure the continuity of learning.

The purpose of this plan is to:

- Define clear responsibilities for managing cybersecurity.
- Protect systems, data, and communication tools from unauthorized access.
- Reduce risk through prevention, detection, and recovery strategies.
- Comply with **FERPA** and applicable **Florida data protection laws**.

Applies to:
All staff, faculty, students, volunteers, and contractors who use or manage the school's network, computers, cloud systems, or digital records.

2. Roles and Responsibilities

Cybersecurity is a shared responsibility. The following roles define who is accountable for maintaining and enforcing security measures.

IT Department / Managed IT Provider

- Maintain security tools, monitoring systems, and patch management.
- Manage user accounts, access control, and backups.
- Respond to incidents and coordinate with external vendors as needed.

School Administration

- Approve cybersecurity policies and ensure staff compliance.
- Allocate resources for training and infrastructure updates.
- Support incident response communication when needed.

Teachers and Staff

- Follow password and data handling guidelines.
- Report suspicious emails or activity immediately.
- Protect classroom technology and shared devices.

Students

- Use technology responsibly according to the school's acceptable use policy.
- Do not share passwords or access restricted systems.

3. Access Control Measures

Managing access is one of the most effective ways to prevent unauthorized activity.

Key Practices:

- Require **Multi-Factor Authentication (MFA)** for all staff and administrative accounts.
- Enforce strong passwords with expiration periods.
- Separate **student, staff, and guest** Wi-Fi networks.
- Review user accounts every semester and remove inactive users.
- Limit administrative privileges to authorized personnel only.
- Maintain a list of devices connected to the network.

4. Incident Detection & Response

Early detection and clear procedures can minimize the impact of cyber incidents.

Detection:

- Enable real-time monitoring and alerts for network and account activity.
- Educate staff on recognizing phishing, suspicious links, and unusual device behavior.

Response Steps:

1. Identify and contain the threat (disconnect affected devices if necessary).
2. Notify IT and administration immediately.
3. Record details of the incident (date, time, affected systems).
4. Eradicate the threat by removing malicious files or users.
5. Recover data from verified backups if needed.
6. Communicate transparently with affected stakeholders.
7. Conduct a post-incident review to improve prevention.

5. Backup & Recovery Strategy

Data loss prevention is essential for school operations.

Backup Guidelines:

- Follow the **3-2-1 rule**: three copies of data, on two media types, with one stored off-site or in the cloud.
- Schedule automatic backups daily or weekly depending on system criticality.
- Test backup restoration quarterly to ensure data integrity.
- Protect backup files with encryption and restricted access.
- Document recovery time objectives (RTO) and recovery point objectives (RPO).

6. Vendor and Third-Party Management

Vendors play a key role in maintaining network and data security. Schools should verify that all partners meet necessary cybersecurity standards.

Recommendations:

- Work only with vendors who comply with FERPA and relevant state laws.
- Review data privacy and breach notification clauses in contracts.
- Require vendors to notify the school immediately in case of a security incident.
- Keep an updated list of approved vendors with contact details.
- Conduct an annual review of third-party performance and compliance.

7. Annual Review Checklist

This plan should be reviewed and updated every year — or sooner if major system, policy, or staffing changes occur.

Item	Completed	Date Reviewed	Notes
Review of all user accounts and permissions	☐		
Firewall and security software updates verified	☐		
Backup and recovery test completed	☐		
Staff cybersecurity training conducted	☐		
Vendor compliance review completed	☐		
Cybersecurity policy approved by administration	☐		
Incident response plan updated	☐		

Conclusion

A strong cybersecurity plan helps schools prepare, prevent, and respond effectively to threats.

By defining roles, maintaining clear procedures, and fostering awareness among staff and students, schools can create a secure and resilient digital environment that supports their mission to educate and protect every learner.