ATLIS
Association of Technology Leaders in Independent Schools

Cybersecurity Recommendations for Independent Schools

Independent schools are increasingly relying on technology and electronic data to manage every aspect of school operations, including many that involve protected information. Activities that involve protected or sensitive data include; making admission and financial aid decisions, guiding college searches, managing payroll, and reaching alumni. Independent school leaders **must** act to protect the school's resources and information. The risks of reputational harm and financial losses following a cybersecurity breach have been made clear in recent years. Further, independent school leaders must monitor developments in state laws requiring that school-collected data be safeguarded. The primary obligation for protecting data is assigned to the school, not to the company or organization the school selects for storing or managing data (e.g. a software company, data backup service, offsite storage, etc.).

Each school must take into consideration the security needs of the school community, the resources available, and the overall risk-management stance of the school. ATLIS recommends that heads of school and technology directors work together to form a cybersecurity team serving as a standing group that includes:

- Technology department leadership
- Risk management leadership from both the administration and the board
- Key employees who handle secure and/or privileged data
- School counsel.

Responsibilities of the team:

1. Assess the school's current cybersecurity plans, resources, and measures.
2. Assess and update the knowledge level of the team members.
3. Conduct an annual review of the school's cybersecurity stance, policies and procedures, the threat landscape, training program, and insurance coverage.
4. Periodically, but at minimum every 3 years, oversee and respond to an external audit of the school's cybersecurity.

First Steps:
ATLIS recommends that the cybersecurity team review the school's needs and determine what level of security the school has currently, where the school needs to be in the short-term, and what the long-term goals are for the school. The levels below spell out guidelines to help schools prioritize. Many schools may choose to implement level one across the board and then add in selected higher-level recommendations based on the school's specific circumstances. The intent of the below document is to provide guidance in more accessible language that the school's IT staff will be able to use in discussions with colleagues and the campus cybersecurity team.

Links to sites with more technical information and term definitions can be found using the resources at the bottom of this chart.

Security	Configuration/Technical	Personnel Procedures	General Policies
First Steps	A plan for making and securing data backups (offsite) at determined levels of frequency to enable disaster recovery and provide options in the event of a cyber attack. Antivirus and malware protection software provided campus-wide.	In-person training for all privileged data users.	Develop baseline business continuity and disaster recovery plans.

Security	Configuration/Technical	Personnel Procedures	General Policies
Level One	Multi-factor authentication for campus users with access to secure or sensitive data Total drive encryption on laptops for employees with access to privileged data such as admission, advancement, finance, medical, etc. A firewall providing dynamic packet filtering The security configuration of all devices on campus are deliberately set, implemented, and actively managed to meet campus security needs.	Background checks upon hire. Baseline simulated phishing attack. Administrative privilege/access managed and limited. Password policies (regarding complexity and scheduled changes) communicated and enforced. General awareness training periodically (annually at minimum) provided to entire faculty and staff in groups. Offboarding procedures designed to remove access to all school technology resources upon departure. Internal privacy and confidentiality policies that are published, enforced, and updated that focus on handling of secure data.	Cyber insurance or similar coverage and services. Determine, communicate, and enforce controls about what devices and software programs are permitted to connect to the campus network. Analyze the school's need for PCI compliance; review and implement accordingly. Review data security policies for all software purchases that involve protected data. Policy on third party remote access to systems, e.g. HVAC, POS, security. Ensure technology department leader undergoes annual cybersecurity professional development. Physical controls for data center and network closets with locked, secured areas for key network resources.

Security	Configuration/Technical	Personnel Procedures	General Policies
Level Two	Network segmentation separates mission-critical network from other areas. Baseline network scans with reviews of the results performed semi-annually (at minimum) to determine vulnerabilities Create logs of network activity that can be analyzed to detect, prevent, or recover from an attack. Whole disk encryption for all employee laptops. Firewall: minimum level plus intrusion prevention Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers	Specific employee designated as responsible for cybersecurity. Cybersecurity training included as part of employee onboarding. Additional offboarding procedures identified with the departure of technology employees. Students digital citizenship curriculum includes cybersecurity training at an age-appropriate level. Regular training and ongoing briefings for key data stewards. Testing of employee responses in simulated cybersecurity scenarios. Follow-up training for those identified as needing it through the testing. Password vaults for admin users to protect key systems.	Annual review of cloud based security agreements Third party audit of cybersecurity stance Business continuity and disaster recovery plans fully developed in writing. Incident response plan developed and shared in writing. Review data security policies for all software purchases. Access logs maintained for key physical network resources. Remote working policies determining who can work remotely and when VPN encryption is needed.

Security	Configuration/Technical	Personnel Procedures	General Policies
Level Three	Periodic internal and external network security scans. Whole disk encryption for all employee laptops and desktops. Firewall: Next generation firewall with configuration evaluation and review taking place semi-annually (at minimum).	Regular and varied training activities and drills to refresh skills for all users. Formal certification for individual charged with overseeing cybersecurity within the technology department.	Business continuity plans tested in a drill. Single tunnel VPN required when users work remotely. Meet and/or address top 20 controls defined by the Center for Internet Security,

Further resources:

www.theatlis.org
ATLIS: Sample policies, templates, how-to webinars
Center for Internet Security: Comprehensive site including certification processes for cybersecurity professionals
US Computer Emergency Readiness Team offers mailing lists and feeds for a variety of products, including the National Cyber Awareness System and Current Activity updates.
National Initiative for Cybersecurity Careers and Studies: glossary of cybersecurity technical terms and definitions