# Technology Security

Provide adequate resources to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction while keeping them highly available for student learning and education administration.

## What is the issue and why is it important? What if SREB states do not make adequate progress on this issue?

Technology security is a global issue for education, government, military, business and private individuals. Today all technology systems, from learning management systems to institutional networks, access points, wi-fi networks, enterprise resource planning, and student information systems, need technology security extending from the user level to the network, institution and beyond, including vendor partners. More schools and institutions now use third-party vendor networks, cloud-based services and online educational tools than ever before, which makes them vulnerable to external access. If they have multiple devices and sensors (known as the Internet of Things or IOT) connected to their network, they create additional risk of unauthorized network access. More than 72 percent of IOT devices are hackable and expose risks for unauthorized access to larger systems.

Security risks from breaches of network or individual systems, whether from hacking, malware, ransomware, third-party system vulnerabilities or mistakes by employees, have heightened public concern over the safety of their personal information. Malicious emails, generally disguised as trustworthy — known as Phishing attacks — have increased exponentially. Hackers use such attacks to obtain login credentials and access to technology systems, and hold systems and data for ransom for untraceable bitcoin.

State agencies, schools and colleges should create multiple layers of security to ensure that technology equipment, software, and security services are up-to-date and available at all times. They should provide user education to their constituents and update it regularly. If states fail to support strong policies on technology security, or to provide adequate training and sustainable funding, students and staff will eventually suffer the loss or corruption of private information and institutions will lose operational information and services, in addition to the related costs of identity theft protection and lawsuits.

One SREB state recommends the following practices to ensure technology security:

- **Do the Basics –** To reduce number of incidences and exposure, promote awareness of basic, but extremely important, security and privacy policies. Use strong passwords and change them often. Keep a password, PIN or passcode on all devices. Whenever staff depart, change security entry codes and locks for buildings or rooms containing sensitive information. Remove old or unused user accounts from all systems and keep up with employee training and communications.
- **Keep Accurate and Updated Data Inventories –** Inventory all records systems (e.g., electronic and paper storage media) to identify those containing personal information. This will help determine what level of protection is necessary for each system, and what priority it has. Classify information in each paper and electronic records system according to sensitivity and the organizational risk if that information was accidentally or intentionally accessed by anyone without a need to know. A rule of thumb to identify sensitivity and confidentiality in an organization would be to reflect on whether the data could be posted on a public website or viewed by anyone making an open records request.
- **Have a Healthy Data Diet –** Collect the minimum amount of personal information necessary to accomplish the educational purposes and retain it for the minimum time necessary.
- **Intruder Detection –** Use appropriate physical and technological safeguards, such as video surveillance or alarms, to protect personal information, particularly higher-risk information, in paper and electronic records.
- **Vendor Management –** Require service providers and partners who handle personal information on behalf of the organization to follow the institution's security policies and procedures as well as state and federal laws (such as COPPA, FERPA). Develop security protocols for inclusion in contracts.
- **Encryption –** For devices used to host or access high-risk information, use data encryption in combination with host protection and access control. Pay particular attention to protecting high-risk personal information on laptops and mobile storage devices (e.g., tablets, smartphones, CDs, thumb drives).
- **Records Retention –** Dispose of records and equipment containing protected information in a secure manner.
- **Document Your Security –** Document security plans and revise annually or whenever there is a material change in practices for data delivery, storage and access.