ManageEngine
Endpoint Central

IT Security Policies Checklist for Educational Institutions

1. Access control policy

Identify distinct roles and specify their respective access needs. ☐

Students : Access To Educational Resources, Assignments, And Personal Academic Records.

Teachers/Faculty : Access To Student Records, Course Materials, And Administrative Functions.

Administrative Staff : Access To Administrative Records, Financial Systems, And Student Information.

IT Staff : Access To The Entire IT Infrastructure, Including Network Configurations & Security Systems.

Library Staff : Access To Library Management Systems And Student Borrowing Records.

Researchers : Access To Research Databases And Collaboration Tools.

External Contractors/Vendors : Limited Access To Perform Specific Tasks Or Services.

Assign permissions based on roles rather than individuals. Avoid granting blanket permissions. ☐

Students : View Grades, Submit Assignments, Access Course Materials.

Teachers/Faculty : Edit Grades, Manage Course Content, Communicate With Students.

Administrative Staff : Update Student Records, Manage Financial Transactions, Generate Reports.

IT Staff : Configure Network Settings, Manage User Accounts, Monitor Security Alerts.

Library Staff : Manage Book Inventories, Issue And Return Books, Access Student Borrowing History.

Researchers : Access And Download Research Papers, Submit Research Proposals.

- [ ] Map users to appropriate roles based on their responsibilities and job functions. Ensure you follow the principle of least privilege (PoLP)
- [ ] Create role hierarchies to define relationships between different roles. Higher-level roles inherit permissions from lower-level roles.
- [ ] Implement procedures for requesting and granting temporary access beyond regular privileges, with strict approval processes.
- [ ] Develop and enforce policies for role assignment, role modification, and role revocation.
- [ ] Regularly review and update user roles and access permissions, especially at the beginning and end of academic terms.
- [ ] Regularly review and update access rights and permissions.
- [ ] Detail the procedures for creating, issuing, and managing user accounts.
- [ ] Implement Multi-Factor Authentication (MFA) for staff, faculty, and students
- [ ] Define authentication methods like OTPs, biometrics or hardware tokens, for administrative access.
- [ ] Enforce single sign-on (SSO) where appropriate.
- [ ] Address the procedure for handling transfers and departures, ensuring that access rights are adjusted or revoked as necessary.
- [ ] Define password complexity requirements (length, character types).
- [ ] Set password expiration and rotation policies (e.g., every 90 days).
- [ ] Enforce account lockout after a specified number of failed login attempts.

2. Data protection policy

- [ ] Classify data into categories such as public, internal, confidential, and restricted, considering student records, financial information, and research data.
- [ ] Label data according to its classification
- [ ] Specify how each category should be handled, stored, and transmitted securely
- [ ] Apply appropriate protection measures, ensuring compliance with FERPA and other regulations.
- [ ] Encrypt sensitive data at rest using robust encryption algorithms or BitLocker or FileVault, particularly for student records and research data.
- [ ] Enforce full-disk encryption on all devices.
- [ ] Ensure data in transit is encrypted using SSL/TLS, especially for online courses and remote communications.
- [ ] Regularly back up critical data to off-site or cloud locations.
- [ ] Ensure informed consent is obtained before collecting personal data.
- [ ] Provide clear information about what data is collected and for what purposes.
- [ ] Restrict data access to authorized personnel only.
- [ ] Define strict guidelines and legal frameworks for sharing data with third parties.
- [ ] Where possible, anonymize data to protect individual privacy.
- [ ] Establish and adhere to a data retention schedule that complies with legal and regulatory requirements.

- [ ] Securely delete or destroy data that is no longer needed, using methods such as shredding or degaussing for physical media and secure erase for digital data.
- [ ] Avoid storing data longer than necessary and ensure it remains up to date.
- [ ] Define backup frequency and retention periods for critical data.
- [ ] Store backups in off-site or cloud locations.
- [ ] Regularly test data restoration procedures.

3. Endpoint security policy

- [ ] Maintain a detailed inventory of all endpoint devices including hardware and software components.
- [ ] Assign ownership and specific responsibilities for managing these assets.
- [ ] Automate provisioning and de-provisioning of accounts.
- [ ] Limit the number of privileged accounts.
- [ ] Have a procedure to immediately deactivate accounts for departed employees and graduated students.
- [ ] Establish minimum security baselines for devices
  - OS versions
  - Antivirus software
  - Firewall configuration
  - Encryption status
  - Backup and recovery
  - Grade/department specific application versions

- [ ] Use a centrally managed UEM solution for consistency and control
- [ ] Allow only approved applications to be installed and run on devices.
- [ ] Standardize settings across all user browsers to minimize vulnerabilities.
- [ ] Regulate the use of browser extensions to prevent potential breaches.
- [ ] Implement measures to detect and block phishing attempts.
- [ ] Monitor and control the opening of email attachments and links to prevent malware.
- [ ] Restrict types or size of files that can be uploaded or downloaded through email.
- [ ] Require the use of antivirus software and schedule regular scans.
- [ ] Mandate the use of Virtual Private Networks (VPNs) for accessing internal resources from external networks.
- [ ] Secure wireless connections with strong encryption protocols like WPA3.
- [ ] Develop a routine to prioritize and patch operating systems, software, firmware, third-party applications, and in-house applications.
- [ ] Test patches in a staging environment before deployment to avoid disrupting educational activities.
- [ ] Schedule regular scans for malware and vulnerabilities.
- [ ] Engage a next-gen malware protection software to identify and defend against threats and zero days
- [ ] Ensure devices comply with security baselines before network access is granted.
- [ ] Regularly back up data and test restoration processes.

- [ ] Keep detailed logs of system and user activities to support post-incident investigations.
- [ ] Control the use of USB and other peripheral devices on institution-owned machines
- [ ] Implement physical access controls such as key cards, biometric scanners, and security guards for sensitive areas, including server rooms, data centers, and labs.
- [ ] Restrict and monitor the use of RDP to authorized users only, such as IT staff and faculty needing remote access to on-campus resources.
- [ ] Use a UEM solution to enforce security policies on remote devices used by staff and students for online learning.
- [ ] Install and maintain surveillance cameras to monitor physical access to sensitive areas.
- [ ] Regularly review surveillance footage for suspicious activity, particularly during off-hours and holidays.

4. Bring Your Own Device (BYOD) policy

- [ ] Require all personal devices accessing institutional resources to be registered with the IT department.
- [ ] Mandate that personal devices comply with institutional security policies.
- [ ] Control the use of USB and other peripheral devices on institution-owned machines
- [ ] Maintain an up-to-date inventory of registered devices.
- [ ] Implement device encryption to protect institutional data on personal devices.
- [ ] Use network segmentation to isolate personal devices from critical systems that require high levels of security, such as accessing financial systems or sensitive research data.

- [ ] Establish clear guidelines for acceptable use of personal devices, including restrictions on accessing and storing sensitive data.
- [ ] Establish a process for reporting security incidents involving personal devices, including lost or stolen devices.
- [ ] Perform remote complete or corporate wipe to protect institutional data on personal devices

5. Email and communication policy

- [ ] Outline acceptable and unacceptable uses of institutional email and communication channels.
- [ ] State the institution's right to monitor email and communications for compliance and security purposes.
- [ ] Implement email filtering solutions to detect and block spam, phishing, and malicious attachments.
- [ ] Regularly update email filtering rules and definitions to protect against new threats.
- [ ] Specify guidelines for handling sensitive information and attachments.
- [ ] Use encrypted communication channels (e.g., secure email, encrypted messaging apps) for transmitting sensitive information, especially for academic and administrative communications.
- [ ] Establish clear guidelines for acceptable use of email and communication tools, including proper handling of sensitive information.
- [ ] Prohibit the sharing of sensitive information through unsecured channels and emphasize the importance of using institutional communication tools.
- [ ] Provide guidelines for appropriate communication etiquette and professionalism.

6. User education and training policy

- [ ] Provide mandatory security awareness training for all staff, faculty, and students.
- [ ] Cover topics such as phishing, social engineering, password security, and data protection, emphasizing scenarios relevant to the educational context.
- [ ] Conduct periodic phishing simulations to educate users on identifying and avoiding phishing attempts.
- [ ] Provide feedback and additional training to users who fall for phishing tests, with a focus on common education-related phishing tactics.
- [ ] Require users to acknowledge understanding and compliance with security policies.
- [ ] Keep records of acknowledgments for audit purposes, ensuring all members of the institution are aware of their responsibilities.

7. Third-party vendor management policy:

- [ ] Assess and monitor the security practices of third-party vendors.
- [ ] Define security requirements and contractual obligations for vendors.
- [ ] Limit and monitor third-party access to institutional systems and data
- [ ] Require NDAs from vendors handling sensitive information to protect confidentiality and data integrity.
- [ ] Maintain a compliance matrix to track and manage compliance requirements, and regularly review policies for updates.

8. Incident response policy:

- [ ] Identify key roles and responsibilities for incident response (e.g., incident response team members, IT staff, administrators).
- [ ] Define decision-making authority during incident response.
- [ ] Establish a classification scheme for incident types (e.g., phishing, malware, data breach).
- [ ] Establish a dedicated Incident Response Team (IRT) from IT, legal, communications, and other relevant departments, with clear roles and responsibilities.
- [ ] If needed, identify external resources or services (e.g., cybersecurity firms, law enforcement) that may assist during incident response.
- [ ] Form an incident response team with representatives
- [ ] Outline procedures for reporting incidents promptly (including who to report to and how).
- [ ] Describe initial steps to be taken upon discovering or receiving a report of an incident (e.g., containment, preservation of evidence).
- [ ] Provide guidance on assessing the scope and impact of the incident.
- [ ] Maintain a chain of custody for digital evidence.
- [ ] Specify actions to mitigate the effects of the incident and prevent further damage.
- [ ] Include procedures for containment, eradication and communication.
- [ ] Outline procedures for restoring affected systems and services to normal operation.
- [ ] Require documentation of all incident response activities, including timelines, actions taken, and outcomes.
- [ ] Establish procedures for post-incident analysis and reporting to identify lessons learned and areas for improvement.

- [ ] Establish a schedule for testing the Incident Response Plan through simulations (e.g., tabletop exercises, penetration testing).
- [ ] Conduct regular training and simulation exercises.

9. Change management policy:

- [ ] Create a framework for all changes to IT systems, including hardware, software, applications, network configurations, and data management processes within the institution.
- [ ] Define procedures for requesting, evaluating, approving, and implementing changes.
- [ ] Identify key performance indicators (KPIs) to measure the success of change initiatives.
- [ ] Implement a standardized change request form to capture essential details such as the description, rationale, and expected impact of the change.
- [ ] Use a centralized system to log and track all change requests, ensuring transparency and accountability.
- [ ] Assign a unique identifier to each change request for easy reference and tracking.
- [ ] Maintain a change log for auditing purposes.
- [ ] Establish a Change Advisory Board (CAB) comprising representatives from IT, academic departments, administration, and other relevant stakeholders.
- [ ] Define the CAB's roles and responsibilities, including evaluating and approving change requests based on their impact and risk.
- [ ] Define clear criteria for approving or rejecting change requests, including the need for CAB approval for significant changes.

- [ ] Establish a hierarchy of approval levels based on the nature and scope of the change.
- [ ] Develop a detailed implementation plan for approved changes, including timelines, resource allocation, budget, and roles and responsibilities.
- [ ] Ensure the plan includes steps for communication, training, and user support as needed.
- [ ] Conduct thorough testing of the functionality, security, and performance of the change.
- [ ] Develop a detailed deployment plan outlining the steps for rolling out the change, including fallback procedures in case of issues.
- [ ] Monitor the change implementation closely to identify and address any issues promptly.
- [ ] Conduct regular reviews of the change management policy and process to ensure they remain aligned with institutional goals.