Action Plan 3 for Policies and Procedures

By following this action plan and checklist, higher education institutions can develop and implement comprehensive cybersecurity policies and procedures that align with best practices, regulatory requirements, and the specific needs of the institution. These policies will serve as essential guidelines for maintaining a secure and resilient cybersecurity environment.

1. Assemble a Policy Development Team: Form a multidisciplinary team comprising cybersecurity experts, IT personnel, legal and compliance representatives, and relevant stakeholders to collaborate on policy development.
2. Identify Policy Requirements: Conduct a thorough analysis of the institution's cybersecurity needs and compliance obligations. Identify areas that require policies and procedures, such as data protection, incident response, access controls, password management, and handling of sensitive information.
3. Review Existing Policies: Assess the institution's existing policies and procedures related to cybersecurity. Identify gaps, redundancies, or inconsistencies that need to be addressed in the new policy framework.
4. Research Best Practices: Research industry best practices and relevant legal and regulatory requirements pertaining to cybersecurity in higher education. Ensure that the policies align with recognised standards and frameworks, such as NIST, ISO, and GDPR.
5. Policy Drafting and Review: Develop comprehensive and clear policies and procedures tailored to the higher education environment. Collaborate with stakeholders to review and refine the drafts to ensure they are practical and achievable.
6. Incident Response Plan: Develop an incident response plan that outlines the step-by-step actions to be taken in the event of a cybersecurity incident. Define roles, responsibilities, and communication protocols during incidents.
7. Data Protection Policy: Create a data protection policy that outlines how sensitive data, including student records, research data, and financial information, will be collected, processed, stored, and shared in a secure manner.
8. Access Controls and Password Policies: Implement policies that define user access privileges, role-based access controls, and guidelines for password complexity, rotation, and storage.
9. Sensitive Information Handling: Establish guidelines for handling and transmitting sensitive information securely, including data encryption, secure file sharing, and data disposal procedures.
10. User Training and Awareness: Develop policies that promote regular cybersecurity training and awareness programs for faculty, staff, and students. Emphasise the importance of cybersecurity hygiene and safe computing practices.
11. Policy Approval and Adoption: Present the policies and procedures to senior leadership, the cybersecurity committee, and relevant stakeholders for review and approval. Ensure that policies align with the institution's risk appetite and strategic objectives.
12. Policy Implementation and Communication: Implement the approved policies and procedures across the institution. Develop a communication plan to ensure that all employees are aware of the policies and their responsibilities in adhering to them.
13. Regular Policy Review: Establish a regular review process for policies and procedures to keep them up-to-date with evolving threats, regulatory changes, and organisational needs.
14. Policy Enforcement and Compliance: Monitor policy adherence and enforce consequences for non-compliance. Conduct periodic audits and assessments to ensure policies are being followed effectively.

Action Plan 3 Checklist

✅ Assembled a policy development team.

✅ Identified cybersecurity policy requirements.

✅ Reviewed existing policies and procedures.

✅ Researched best practices and legal requirements.

✅ Drafted comprehensive policies and procedures.

✅ Developed an incident response plan.

✅ Created a data protection policy.

✅ Implemented access controls and password policies.

✅ Established guidelines for sensitive information handling.

✅ Developed user training and awareness policies.

✅ Obtained approval for policies from relevant stakeholders.

✅ Implemented policies across the institution.

✅ Communicated policies to all employees.

✅ Established a regular policy review process.

✅ Ensured policy enforcement and compliance.