CYBER SECURITY FRAMEWORK FOR ABC UNIVERSITY

4.2 Policies

Cyber security policies are a set of guidelines and procedures implemented by an organization to protect its information systems, network, and data from unauthorized access, cyber threats, and potential vulnerabilities. These policies serve as a roadmap for establishing a secure and resilient cyber security framework within an organization.

For ABC University we are using the ISO 27001 framework, ISO 27001 is an internationally recognized standard for information security management systems (ISMS). The term ISO stands for International Organization for standardization. It provides a systematic approach to managing sensitive information and ensuring the confidentiality, integrity, and availability of that information

Purpose:

The purpose of cybersecurity policies based on ISO 27001 to ABC University is to establish a framework for managing and protecting information assets within the University. These policies help ensure the confidentiality, integrity, and availability of information by implementing appropriate security controls, risk management processes, and continuous improvement measures. These policies aim to safeguard sensitive information, including student records, research data, financial information, and intellectual property, while complying with relevant laws, regulations, and industry best practices.

Scope:

The cybersecurity policies of ABC University apply to all university faculty, staff, students, contractors, and any other individuals who have access to university information systems and assets. The scope encompasses all information assets owned, leased, or controlled by the university, regardless of the medium or format in which they are stored or transmitted. This includes computer networks, servers, databases, applications, websites, mobile devices, and physical infrastructure.

Applicability based on ISO 27001:

ABC University's cybersecurity policies align with the ISO 27001 standard, which defines the requirements for establishing an ISMS. The ISMS provides a systematic approach to managing information security risks, ensuring the confidentiality, integrity, and availability of information, and continually improving the effectiveness of security controls.

The policies cover various aspects of information security, including:

1. Information Security Governance: The policies establish the roles and responsibilities of information security management, define the governance structure, and ensure senior management commitment and support.

2. Risk Management: ABC University identifies and assesses information security risks, implements appropriate controls to mitigate the identified risks, and regularly reviews and monitors the effectiveness of these controls.

3. Asset Management: The policies define the procedures for the inventory, classification, and protection of information assets throughout their lifecycle, including acquisition, use, storage, and disposal.

4. Access Control: The policies establish guidelines for granting access rights to users based on their roles and responsibilities, implementing strong authentication mechanisms, and regularly reviewing user access privileges.

5. Information Security Incident Management: The policies outline the procedures for detecting, responding to, and recovering from security incidents, including incident reporting, analysis, and communication.

6. Business Continuity Management: ABC University ensures the continuity of its operations by establishing plans, procedures, and resources to maintain critical business functions during and after disruptive incidents.

7. Compliance: The policies ensure compliance with legal, regulatory, and contractual requirements related to information security, privacy, and data protection.

8. Awareness and Training: ABC University provides ongoing awareness and training programs to educate its stakeholders about information security risks, policies, and best practices.

By adhering to these cybersecurity policies based on ISO 27001, ABC University aims to establish a robust information security posture, protect its information assets, and maintain the trust and confidence of its stakeholders in an increasingly digital and interconnected environment.