**IT POLICIES**

An IT (Information Technology) policy is a set of guidelines and rules that define how an organization manages, uses and secures its information technology resources. These policies are designed to ensure the effective and secure use of technology within an organization.

**IT Policies:**

**Acceptable Use Policies (AUP):** These outline the acceptable and unacceptable uses of the organization’s IT resources. This may include guidelines on internet usage, email communication, and proper handling of sensitive information.

**Data Management Policies:** These policies address how data is collected, stored, processed and shared within the organization. This includes data retention, backup procedures and data privacy considerations.

**InfoSec Policy:** An Information Security (InfoSec) Policy is a comprehensive set of guidelines and rules that an organization establishes to ensure the confidentiality, integrity and availability of its information assets. The goal of an InfoSec Policy is to define the organization’s approach to information security and guide employees, contractors and other stakeholders in handling information responsibly.

**Network Policies:** These define rules for the organization’s computer network, covering aspects such as network access, bandwidth usage and network security.

**BYOD (Bring Your Own Device) Policies:** In organizations that allow employees to use their personal devices for work, BYOD policies specify the rules and security measures to be followed.

**Software Usage Policies:** In organizations that allow employees to use their personal devices for work, BYOD policies govern the installation, use and licensing of software withing the organization.

**Incident response and Disaster Recovery policies:** These outline the procedures to be followed in case of IT security incidents, data breaches, or other emergencies. They also include plans for recovering IT systems in the event of a disaster.

**Cloud and App Use Policy:** A Cloud and App use policy should outline approved cloud and mobile apps for handling business data and restrict the use of unauthorized applications. It should also provide a channel for employees to suggest apps that could improve productivity.

**Security Awareness and Training Policy:** Goals for the security awareness and training policy should include education about the security policy and help develop business, employees and customers. The policy must also highlight personnel that is responsible for creating and maintaining recognize changes in technology that impact security and the organization.

**Change Management Policy:** An organization’s change management policy ensures that changes to an information system are managed, approved all changes are made in a thoughtful war that minimizes negative impact to services and customers. The change management policy covers SDLC, hardware, software, database, and application changes to system configurations including moves, adds, and deletes.

**Vendor Management Policy:** The vendor management policy validates a vendor’s compliance and information security abilities. The policy should address the process to acquire vendors and how to manage all of a company’s vendors. The company should trust that the third-party vendor will appropriately safeguard the information that it is given.

The policy should cover procedures for selecting a vendor, risk management, due diligence, contractual standards, and reporting and ongoing monitoring. Additionally, the policy should address the relationship to other areas of the risk management and compliance management practices.

**Password Creation and Management Policy:** The password creation and management policy provides guidance on developing, implementing and reviewing documented process for appropriately creating, changing and safeguarding strong and secure passwords used to verify user identities and obtain access for company systems or information. The policy should touch on training and awareness as to why it is so important to choose a strong password. It should include rules for changing passwords.

**Security Policy:** These define measures and protocols to protect the organization’s IT infrastructure, data and systems from unauthorized access, data breaches and other security.

It may include:

* Cybersecurity
* Data Protection
* Multi-Factor Authentication
* Security Training
* BYOD
* Portable data storage
* Antivirus requirements
* Patch Management
* Disaster Recovery
* Incident response

**Data Governance Policy:** Easy access to critical data can help your employees make informed decisions, delight customers, and increase revenue. A data governance policy protects your data to improve its security, integrity, confidentiality, accuracy and availability.

**Software Development and Deployment Policy:** A Software Development and Deployment Policies is to govern the process of creating, testing, deploying and maintaining software applications. This policy aims to ensure the efficient and secure development and deployment of software while aligning with the organization’s goals and compliance requirements.

**Remote Access Policy:** A Remote Access Policy is a set of guidelines and rules established by an organization to govern the secure and appropriate use of remote access to its computer systems and networks. The purpose of this policy is to ensure that remote access is conducted in a manner that protects the organization’s information assets, maintains the confidentiality and integrity of data and complies with relevant legal and regulatory requirements.

**Physical Security Policy:** A Physical Security Policy is a set of guidelines and rules by an organization to govern the measures and practices employed to secure its physical assets, facilities and information. The purpose of this policy is to protect the organization’s people, property and information from unauthorized access, theft, damage or other physical threats.

**IT compliance policy:** An IT compliance policy is a set of guidelines and rules established by an organization to ensure that its information technology practices adhere to relevant laws, regulations, industry standards and internal requirements. The purpose of this policy is to mitigate risks, protect sensitive data, and demonstrate a commitment to legal and regulatory compliance.

**Cloud Computing Policy:** A Cloud Computing Policy is a set of guidelines and rules to govern the secure and effective use of cloud computing services. The purpose of this policy is to ensure that the organization leverages cloud resources in a manner that aligns with business objectives, complies with relevant regulations and maintains the security and privacy of data.

**Asset Management Policy:** An Asset management policy is to govern the acquisition, use, maintenance and disposal of its assets. The purpose of this policy is to ensure effective and efficient management of assets throughout their lifecycle, maximize their value and comply with relevant regulations.

**Environmental and Green IT policy:** An Environmental and Green IT policy is by an organization to govern its commitment to environmentally sustainable and energy-efficient practices within the realm of information technology (IT). The purpose of this policy is to reduce the environmental impact of IT operations, promote responsible resource usage and contribute to a more sustainable and eco-friendly business environment.

**Intellectual Property Policy:** Intellectual Property is to govern the creation, protection and management of intellectual property assets. Intellectual property includes inventions, patents, trademarks, copyrights, trade secrets and other intangible assets that are crucial to the organization’s innovation and competitive advantage.