**WRITING IT POLICIES**

**Steps to write IT policies:**

**1) Specify the purpose –** The first thing is need to do when writing the IT Policy is to specify the purpose of the document.

**Consider the following questions:**

What is the purpose of the IT policy?

Why is it necessary?

How is it going to be used?

The IT policy of a company defines the rules, regulations and guidelines for the proper usage, security an maintenance of the company’s technological assts including the computers, mobile devices, servers, internet, applications, etc. It establishes guidelines for the acceptable and ethical use of the company’s IT infrastructure to ensure the safety,

security and integrity of the data, products and/or services used by the company as well as of those offered to its customers.

**2) Define the scope of the policy –** The scope of the document tells exactly what is included and what isn’t. Don’t leave any ambiguity in the policies. Correctly defining the scope allows the IT managers to calculate the resources required for implementation as well as to establish controls and monitoring systems.

**Consider the following questions:**

Who has to comply with this IT policy- employees, contractors, vendors, etc?

Which devices are covered-company issued, personal devices?

Which applications and tools are covered-installed on company devices, installed on personal devices?

**3) Components of the IT Policy –**

**I) Purchase and Installation Policy:**

The purpose of purchase and installation guidelines for the organization is to ensure that all hardware and software used are appropriate, provide value for money, and integrate with other technologies used within the organization.

**Consider the following questions:**

Is there an approval process?

Who is responsible for the purchasing-procurement team, office manager, or IT team?

Where will they buy from-authorized resellers, pre-identified vendors?

Are there any standardized configurations for devices?

Who can install software on devices?

Is a whitelist of approved software applications and maintained by the organization?

**II) Usage Policy:**

The usage policy sets the guidelines for the allocation, usage and maintenance of all company-owned equipment, data and technology. IT defines the guidelines that are important for every employee to understand to be able to use the company’s technological resources responsibly, safely and legally.

* **Device Usage Policy:**

**Consider the following questions:**

* What devices and peripherals are allocated to employees? Clearly define if there are differences based on the departments, seniority, etc
* Are there preconditions for the allocation of mobile devices such as laptops and smartphones?
* Is personal use of the devices allowed? If yes, clearly define the stipulations, for example, when is such use allowed, what are their responsibilities with regards to maintenance and security of the devices.
* In case of loss or theft of the device, what procedure must be followed by the employee?
* What’s the procedure for the replacement of the devices?
* What’s the procedure for the return of the devices, for example, when leaving the organization.
* **Email Usage Policy:**

A clearly defined email usage policy reduces the security and business risks faced by the organization. It describes the rules for the use of the company provided email and helps satisfy the legal obligations as well as protects the organization from liabilities.

For drafting your email usage policy, consider the following questions:

* Define the scope of the policy, Is it applicable when the email exchange is done:
* Using a personal device or company-issued device,
* On-premises, off-premises, on business trips, vacations, etc.
* Is personal use of company email allowed? , If yes, clearly describe the stipulations.
* Clearly define the data confidentiality and privacy obligations of the email users.
* Is there a standard email signature format? Is it required to get approval for customized email signatures?
* In the case of an email security breach, who should be notified and how?
* Clearly defne the ownership of the contents within the company emails.
* Define the email security obligations
* **Internet Usage Policy:**

The Internet usage policy describes the rules governing internet use at your organization. It is necessary to ensure that all employees understand how to use the internet responsibly, safely and legally. A clearly defined internet usage policy reduces cybersecurity risks and satisfies the legal obligations regarding internet use.

For drafting your internet usage policy, consider the following:

* Define the scope- locations and devices covered
* Is personal use of the internet allowed? If yes, then clearly describe the stipulations.
* Employees must not attempt to disable or circumvent the firewall.
* Is there any restriction on visiting websites or downloading content? If yes, clearly describe those restrictions.
* Clearly define appropriate use and any prohibited activities such as
* Playing Online games
* Downloading pirated media
* Define the privacy and security obligations the employees must adhere to while using the internet.

**IT Security Policy:**

IT security is a vast topic and it is easily possible to draft a separate IT security Policy document. However for most small companies, it is sufficient to cover the basic IT security components within your larger IT policy document.

* **Physical Security:** Physical security is an important part of IT security because it offers a simple way of mitigating many security risks. For example, simple access restrictions and sign-in logs can prevent threat actors form physically accessing your servers, routers, switches, etc,
* **Network Security:** Network security requires special attention as it is a common target for cyber attacks. Describe the tools, processes and procedures in place for ensuring the security of the organization’s computer network.
* **Cybersecurity:** Consider how the organization will mitigate cybersecurity risks and enumerate those provisions here. Draft clauses around the following points:
* Use of software, application and browser extensions
* Use of USBs and external hard drives.
* Data backup, disaster recovery and business continuity.
* Who to contact and what to do in case of a cybersecurity incident.
* Conducting training on IT and Security Policies and their frequency.
* Password policy and use of a password manager.
* Use of Multi-Factor Authentication
* Use of Mobile Device Management tools
* **Audits:** An IT security audit assesses the security of your organization’s IT systems. It covers the entire IT infrastructure including personal computers servers, network routers, switches, etc. Audits are an iterative process and need to be reviewed and updated regularly.
* **4) Data Security Policy:**

Running a business requires to gather certain information about individuals including employees, clients, business partners, vendors, etc. Therefore you will need a policy that provides guidelines on how this data must be collected, stored and handled to ensure that all involved parties are protected from risks of data breaches.

For drafting the data security policy, consider the following:

* Define the scope- who does this policy apply to and what data is included?
* Set guidelines regarding the storage, access, usage, modification, sharing as well as how to ensure data accuracy, integrity and security.
* Describe the methods in place for ensuring data security such as access control., authentication, monitoring, etc.
* **Policy Enforcement and Sanctions for Violation:**

The IT policy isn’t just a document that employees read once during onboarding and then forget about it. The IT policy is a document that should be referred to whenever there is any doubt or ambiguity about the usage, maintenance and security of the information technology infrastructure of the organization.