Chapter-#03

Cyber Security Policies

Cyber Security Policies

- It’s important to create a cyber security policy for your business – particularly if you have employees. It helps your employees to understand their role in protecting the technology and information assets of your business.
- Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.
- It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur.
- A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Need of Security policies-

1) It increases efficiency.

The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

Cyber Security Policies

- **2) It upholds discipline and accountability**
- When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.
- **3) It can make or break a business deal**
- It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.
- **4) Set password requirements**
- Your cyber security policy should explain:
- requirements to create strong passphrases
- how to store passphrases correctly
- how often you need to update passphrases
- the importance of having unique passphrases for different logins

Cyber Security Policies

- **5) Email Security.**
- Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, **[company name]** requires all employees to:
- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid click bait titles and links.
- Contact the IT department regarding any suspicious emails.
- Include guidelines on:
- when it’s appropriate to share your work email address
- only opening email attachments from trusted contacts and businesses
- blocking junk, spam and scam emails
- identifying, deleting and reporting suspicious looking emails.

Cyber Security Policies

- **6) It helps to educate employees on security literacy**
- A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data. It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.
- We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment. There are some important cyber security policies recommendations describe below-
- **1. Virus and Spyware Protection policy**
- This policy provides the following protection:
- It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.
- It helps to detect the applications that exhibit suspicious behaviour by using SONAR heuristics and reputation data.

Cyber Security Policies

- **2. Firewall Policy**
- This policy provides the following protection:
- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic.
- **3. Intrusion Prevention policy**
- This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware which is coming through legal ways.
- **4. Live Update policy**
- This policy can be categorized into two types one is Live Update Content policy, and another is Live Update Setting Policy. The Live Update policy contains the setting which determines when and how client computers download the content updates from Live Update. We can define the computer that clients contact to check for updates and schedule when and how often clients computer check for updates.

Cyber Security Policies

- **5. Application and Device Control**
- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system. The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.
- **6. Exceptions policy**
- This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.
- **7. Host Integrity policy**
- This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. We use this policy to ensure that the client's computers who access our network are protected and compliant with companies? securities policies. This policy requires that the client system must have installed antivirus.

Cyber Security Policies

- **7). Explain how to handle sensitive data**
- When it comes to handling sensitive data, outline:
- when staff may share sensitive data with others
- ways they should store physical files with sensitive data, such as in a locked room or drawer
- ways to properly identify sensitive data
- ways to destroy any sensitive data when it is no longer needed
- **8). Set rules around handling technology**
- Rules around technology should include:
- where employees can access their devices such as a business laptop away from the workplace
- how to store devices when they aren’t in use
- how to report a theft or loss of a work device
- how system updates such as IT patches and spam filter updates will be rolled out to employee devices
- when to physically shut down computers and mobile devices if not in use

Cyber Security Policies

- The need to lock screens when computers and devices are left unattended
- How to protect data stored on devices like USB sticks
- restrictions on use of removable devices to prevent malware being installed
- the need to scan all removable devices for viruses before they may be connected to your business systems
- **9). Prepare for an incident**
- If a cyber security incident occurs, you should minimise the impact and get back to business as soon as possible. You'll need to consider:
- how to respond to a cyber incident
- what actions to take
- staff roles and responsibilities for dealing with a cyber attack

Cyber Security Policies

Prepare and prevent

- Prepare your business and employees to be ready to handle cyber incidents.
- Develop policies and procedures to help employees understand how to prevent an attack and to identify potential incidents.
- Identify the assets that are important to your business – financial, information and technology assets.
- Consider the risks to these and the steps you need to take to reduce the effects of an incident.
- Create roles and responsibilities so everyone knows who to report to if an incident occurs, and what to do next.

Respond

- Limit further damage of the cyber incident by isolating the affected systems. If necessary, disconnect from the network and turn off your computer to stop the threat from spreading.
- Remove the threat.
- Recover from the incident by repairing and restoring your systems to business as usual.

Cyber Security Policies

Check and detect

- Check and identify any unusual activities that may damage your business information and systems. Unusual activity may include:
- accounts and your network not accessible
- passwords no longer working
- data is missing or altered
- your hard drive runs out of space
- your computer keeps crashing
- your customers receive spam from your business account
- you receive numerous pop-up ads

Identify and assess

- Find the initial cause of the incident and assess the impact so you can contain it quickly.
- Determine the impact the incident has had on your business.
- Determine its effects on your business and assets if not immediately contained.