UNIT-IV

SECURITY POLICIES

Development of Security policies

A **security policy** is a set of rules that apply to activities for the computer and communications resources that belong to an organization. ... These rules include areas such as physical **security**, personnel **security**, administrative **security**, and network **security**.

Developing an Information **Security Policy**. ... It provides employees with clear instructions about acceptable use of company confidential information, explains how the company secures data resources and what it expects of the people who work with this information.

SECURITY POLICIES-RESPONDING TO REQUIREMENTS FOR CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY. The weight given to each of the **three major** requirements describing needs for information **security**—confidentiality, integrity, and availability—depends strongly on circumstances.

Help minimize risk. Help track compliance with regulations and legislation. Ensure the confidentiality, integrity and availability of their data. Provide a framework within which employees can work, are a reference for best practices, and are used to ensure users comply with legal requirements.

A **cybersecurity** policy sets the standards of behavior for activities such as the encryption of email attachments and restrictions on the use of social media. **Cybersecurity policies** are important because cyberattacks and data breaches are potentially costly.

Policies provide guidance, consistency, accountability, efficiency, and clarity on how an organization operates.

1. To ensure that all members of the campus community have the maximum access possible to the new ways of generating, storing, and transmitting information in all forms. Electronic transmission of information is one of the media for accomplishing this objective.

2. To ensure that use of the university's electronic networks for electronic publication and access to information will follow the established communication standards and practices of the university. In addition to recognizing the similarities between the traditional communication media and the electronic publication media, the objective of this policy is to acknowledge that differences do exist between these media, such as speed of availability and transmission of the information.

Email security policies

An **email policy** is a **policy** a business will choose to implement in order to ensure that employee's use their **email** in a way that is aligned with the aims of the business. This means the **policy** will change for different organisations, but there are general terms which are usually standard for most organisations.

Email Security Features

Spam Filters. A significant proportion of **emails** that you receive daily are marketing **emails**. ...

Anti-virus **Protection**. Spam filters play the role of separating the spam **emails** from the regular ones. ...

Image & Content Control. Hackers use **emails** for phishing purposes. ...

Data **Encryption**.

A clear **email policy** helps prevent timewasting, protects data security and minimises the risk of legal problems. As well as setting out how employees can **use email**, the **policy should** cover any **email** monitoring you intend to carry out.

Policy review process-corporate

The purpose of a comprehensive **review** is to take an in depth look at existing administrative **policies** and associated documents such as **procedures**, FAQs, and appendices to: 1) determine whether a **policy** is still needed or if it should be combined with another administrative **policy**; 2) determine whether the purpose.

The best way to proactively tackle policy and procedure **review** is just to build it into the **corporate** calendar. As a general rule, every policy **should** be **reviewed** every one to three years. But most experts recommend **reviewing policies** annually.

Policies-sample security policies

9 policies and procedures you need to know about if you're starting a new security program

Acceptable Use **Policy** (AUP) ...

Access Control **Policy** (ACP) ...

Change Management **Policy**. ...

Information **Security Policy**. ...

Incident Response (IR) **Policy**. ...

Remote Access **Policy**. ...

Email/Communication **Policy**. ...

Disaster Recovery **Policy**.

After the **policies** have been written, they will not do your organization any good if they sit on the shelf collecting dust. Not only should it be a living document, but it also should be accessible to all users.

*****Thank you**********