What is a network security policy?

A network security policy primarily helps in protecting a computer network from network security threats – both internal and external – from the organization or network. It is generally a broad document and varies based on the underlying environment, organization and/or legal requirements. Typically, a network security policy documents:

* Rules and legal procedures to access the network and to modify its characteristics.
* Governance and management over Web/Internet access
* Implementation of security procedures (access control) on network nodes and devices
* Role/Privilege based policies, such as identifying authorized and unauthorized services/processes any user can perform on the network

A network security policy is usually part of a broader information security policy.

There are different types of network security policies existed in companies and government organizations and these included:

* Firewall. Firewalls control incoming and outgoing traffic on networks, with predetermined security rules. ...
* Network Segmentation. ...
* Remote Access VPN. ...
* Email Security. ...
* Data Loss Prevention (DLP) ...
* Intrusion Prevention Systems (IPS) ...
* Sandboxing. ...
* Hyper scale Network Security.

network security policy delineates guidelines for computer network access, determines policy enforcement, and lays out the architecture of the organization’s network security environment and defines how the security policies are implemented throughout the network architecture.

Network security policies describes an organization’s security controls. It aims to keep malicious users out while also mitigating risky users within your organization. The initial stage to generate a policy is to understand what information and services are available, and to whom, what the potential is for damage, and what protections are already in place.

The security policy should define the policies that will be enforced – this is done by dictating a hierarchy of access permissions – granting users access to only what they need to do their work.

These policies need to be implemented in your organization written security policies and also in your IT infrastructure – your firewall and network controls’ security policies.

Why is network security policy important?

because it prevents cybercriminals from gaining access to valuable data and sensitive information. When hackers get hold of such data, they can cause a variety of problems, including identity theft, stolen assets and reputational harm.

The roles and responsibility of each network security policy team

**Roles Responsibilities**

**Board of Directors-** Oversight/understanding of cyber security risks and Private matters

Consults with Exec team to understand risk appetite and security maturity

**Executive Leadership-** Solid understand of security risks and potential weak points

Continuously evaluate risk assessment against potential threats

Incorporate security into the company strategy

Communication path of security matters to the Board of Directors

**Security Lead-** Aligns Information Security policies and practises based on the level of mission, strategic planning, objectives and risk assessment

Serves as security ambassador across internal and external engagements (i.e. liaison to the exec team, Board of Directors, client facing engagements for security matters)

Defines and runs the security program across the organization

Create an in-depth risk and maturity profile for vulnerability threats and utilize it to plan initiatives

Responsible for oversight of security policies

Responsible for monitoring security risks and creating remediation plans

Communicates information security risks to executive leadership

**Compliance Manager-** Works with applicable executive leadership to establish an information security framework and awareness program

Builds and maintains an Information Security & Enterprise Risk Management Framework

Responsible for compliance to policies and internal controls.

**Control Owners-** Control design in collaboration with the compliance and security team

Control evidence gathering and submission for review

Control maintenance (i.e. as company processes change any dependable controls need to be adjusted)

Control representation for any internal and external audits

**System Owners-** Manage the confidentiality, integrity and availability of the information systems for which they are responsible in compliance with policies on information security and privacy.

Approval of technical access and change requests for non-standard access (annual reviews)

**Employees, Contractors, temporary workers and others-** Acting at all times in a manner which does not place at risk assets

Helping to identify risk as part of the risk management process and implement remediations

Adhering to company policies and standards of conduct

Reporting incidents and observed anomalies or weaknesses

These are the roles and responsibility that each and every individuals plays in protecting, implementing and securing a safer and better network security.

What are the purpose of a network security policy?

Its purpose is to keep malicious users out while also mitigating risky users within your organization. The initial stage to generate a policy is to understand what information and services are available, and to whom, what the potential is for damage, and what protections are already in place.