SECURITY POLICY CREATION

ABSTRACT

A security policy is a documented set of rules and procedures that govern how an organization manages, protects, and distributes sensitive information and resources, ensuring protection against unauthorized access, misuse, or cyberattacks

Elevate Labs

Cybersecurity

Cybersecurity Project

Security policy :

A security policy is a documented set of rules and procedures that govern how an organization manages, protects, and distributes sensitive information and resources, ensuring protection against unauthorized access, misuse, or cyberattacks

Security Policy Creation :

Creating a security policy involves defining a formal set of rules and guidelines that govern how an organization protects its assets, data, and resources from threats and vulnerabilities. A well-crafted security policy helps ensure the

confidentiality, integrity, and availability of information systems.
Here's a step-by-step explanation of the security policy creation process

Typical Components in Security Policy Creation :

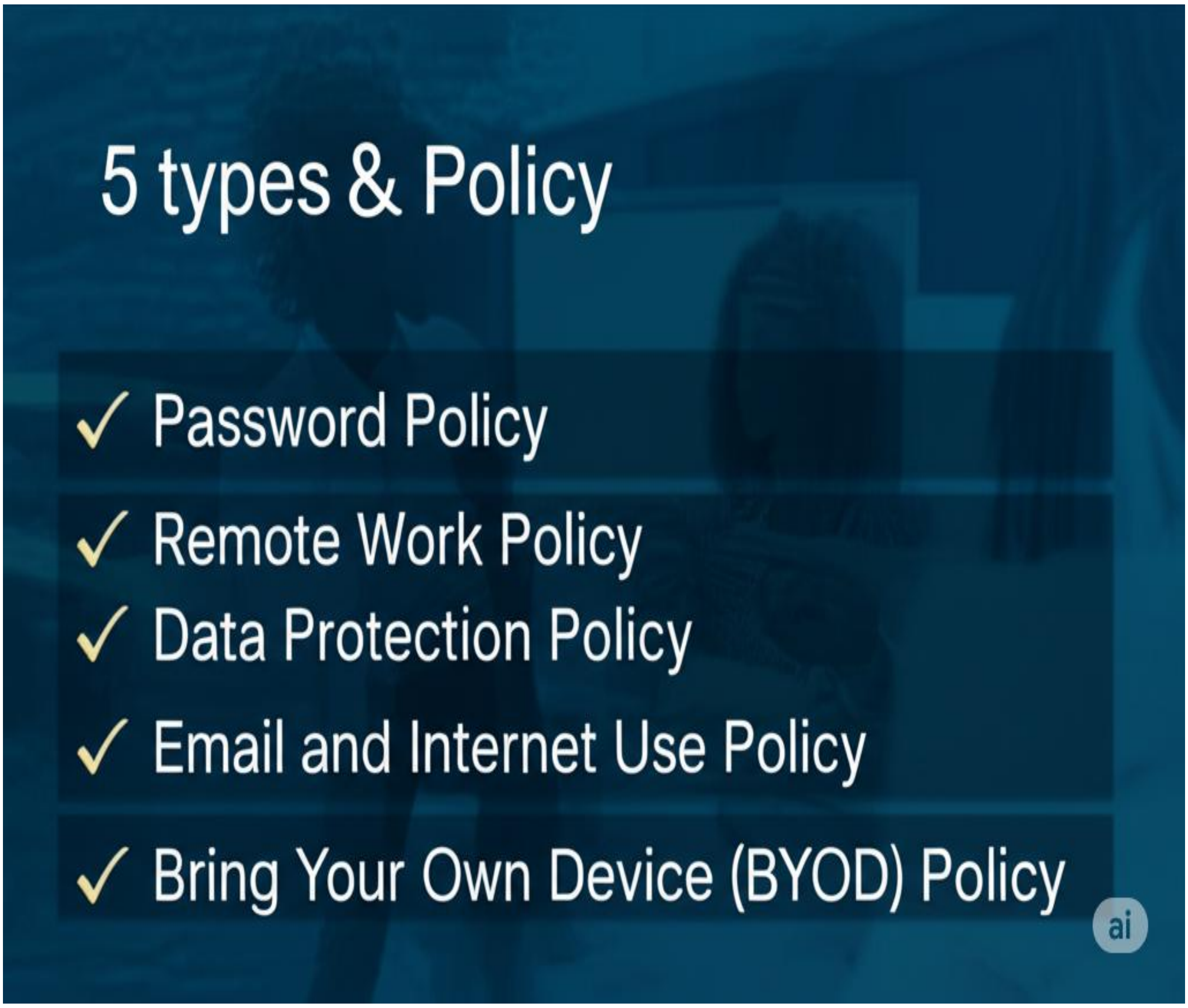
Purpose: Why the policy exists.

Scope: Systems, data, and people it applies to.

User Responsibilities: Acceptable use, reporting incidents.

Enforcement: Penalties for non-compliance.

Types of Policies



5 types & Policy

- ✓ Password Policy
- ✓ Remote Work Policy
- ✓ Data Protection Policy
- ✓ Email and Internet Use Policy
- ✓ Bring Your Own Device (BYOD) Policy

1.Password Policy

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. Either the password policy is merely advisory, or the computer systems force users to comply with it. Some governments have national authentication frameworks that define requirements for user authentication to government services, including requirements for passwords.

Purpose

To establish a standard for creating, managing, and protecting passwords to ensure system security.

Scope

Applies to all employees, contractors, and third-party users accessing company systems and services.

User Responsibilities

1. Passwords must Be at least 12 characters long. Include uppercase, lowercase, numbers, and special characters.
2. Passwords must be changed every 90 days
3. Password reuse is prohibited (minimum of 5 previous passwords blocked).
4. Default passwords must be changed immediately upon account setup.
5. Multi-Factor Authentication (MFA) must be enabled wherever possible.
6. Passwords must not be Shared with anyone.
7. Written down or stored in plain text.
8. Users must report suspected password compromise immediately.

Enforcement

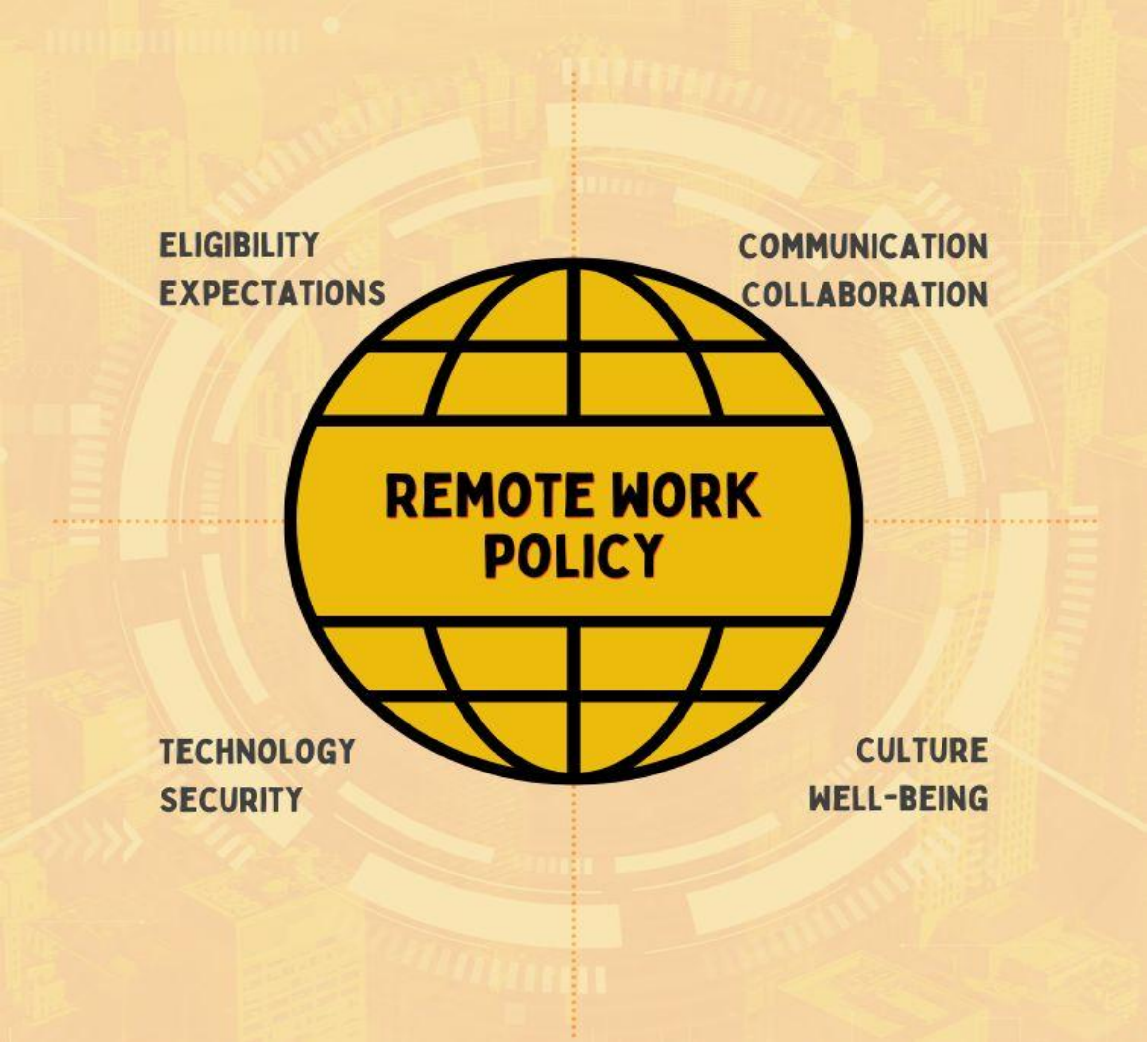
Violations may result in account lockout, security review, and possible disciplinary action.

2.Remote Work Policy

A remote work policy is an agreement that outlines expectations and guidelines for working outside the office. This includes who can work from home, what is expected of them, and how performance will be measured. A remote work policy should also define what tools and support are available to employees.

Purpose

To define security requirements and best practices for employees working remotely.



Purpose

To define security requirements and best practices for employees working remotely.

Scope

Applies to all remote workers using personal or company-owned devices to access company systems.

User Responsibilities

1. Devices must have up-to-date antivirus and security patches.
2. Access should be through secure, password-protected Wi-Fi.
3. Company-approved VPN must be used for remote access.
4. Sensitive documents should not be stored locally unless authorized.
5. Work devices must be locked when unattended.
6. Sharing devices with unauthorized users is prohibited.
7. Report lost or stolen devices immediately to the IT team.

Remote work policy best practices

Create SOPs for common tasks

Define your remote hiring and onboarding procedures

Evaluate employees' suitability for remote work with skill assessments

Have each remote employee sign an agreement

Enforcement

Non-compliance may lead to restricted access or disciplinary measures.

3. Data Protection Policy

The terms data protection and data privacy are often used interchangeably, but there is an important difference between the two. Data privacy defines who has access to data, while data protection provides tools and policies to actually restrict access to the data. Compliance regulations help ensure that user's privacy requests are carried out by companies, and companies are responsible to take measures to protect private user data.

Data protection and privacy is typically applied to personal health information (PHI) and personally identifiable information (PII). It plays a vital role in business operations, development, and finances. By protecting data, companies can prevent data breaches, damage to reputation, and can better meet regulatory requirements.

Purpose

To protect company data and ensure compliance with privacy regulations.

Scope

Covers all employees, contractors, and third parties who handle company data.

User Responsibilities

1. Only authorized personnel may access sensitive data.
2. Data should be stored securely using encryption where applicable.
3. Data sharing must follow company-approved methods and contracts.
4. Personal data must not be disclosed without proper consent or legal basis.
5. Regular backups of critical data must be maintained.
6. Security incidents or data breaches must be reported immediately.

Enforcement

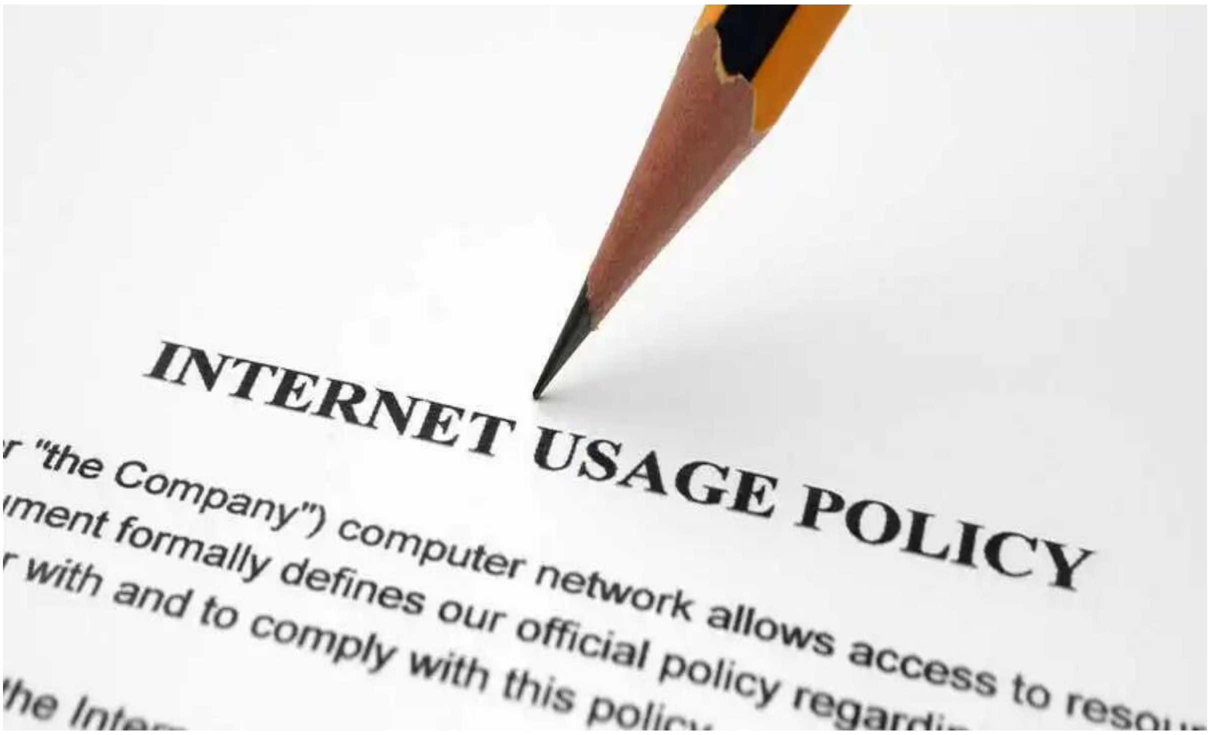
Violations may result in legal action, financial penalties, or employment termination.

4. Email and Internet Use Policy

Internet and email policies are not only meant for IT people but also required to be conveyed to all employees on the importance of its usage, handling and managing it.

A comprehensively defined and charted internet policy helps employees enjoy the vast benefits of the internet, while being wary of its potential risks. It ensures that employees use the internet effectively, states what is allowed and what is not with procedures to minimize risks.

The use of the email system and the internet within this organisation is encouraged, as this use facilitates communication and improves efficiency. Inappropriate use, however, causes problems ranging from lack of productivity to legal claims against the organisation. This policy sets out the organisation’s guidelines on the correct use of email and the internet, and the organisation’s response to inappropriate use.



INTERNET USAGE POLICY

r "the Company") computer network allows access to resou

ment formally defines our official policy regardi

r with and to comply with this polic

he Inter

Purpose

To ensure proper and secure use of company email and internet resources.

Scope

Applies to all employees, contractors, and users with company-provided internet and email access.

User Responsibilities

1. Email should be used for professional, work-related communication.
2. Do not open suspicious emails or click unknown links.
3. Downloading unauthorized software is strictly prohibited.
4. Personal use of company email and internet should be minimal.
5. Accessing illegal or inappropriate websites is prohibited.
6. All email communications are subject to monitoring as per local laws.

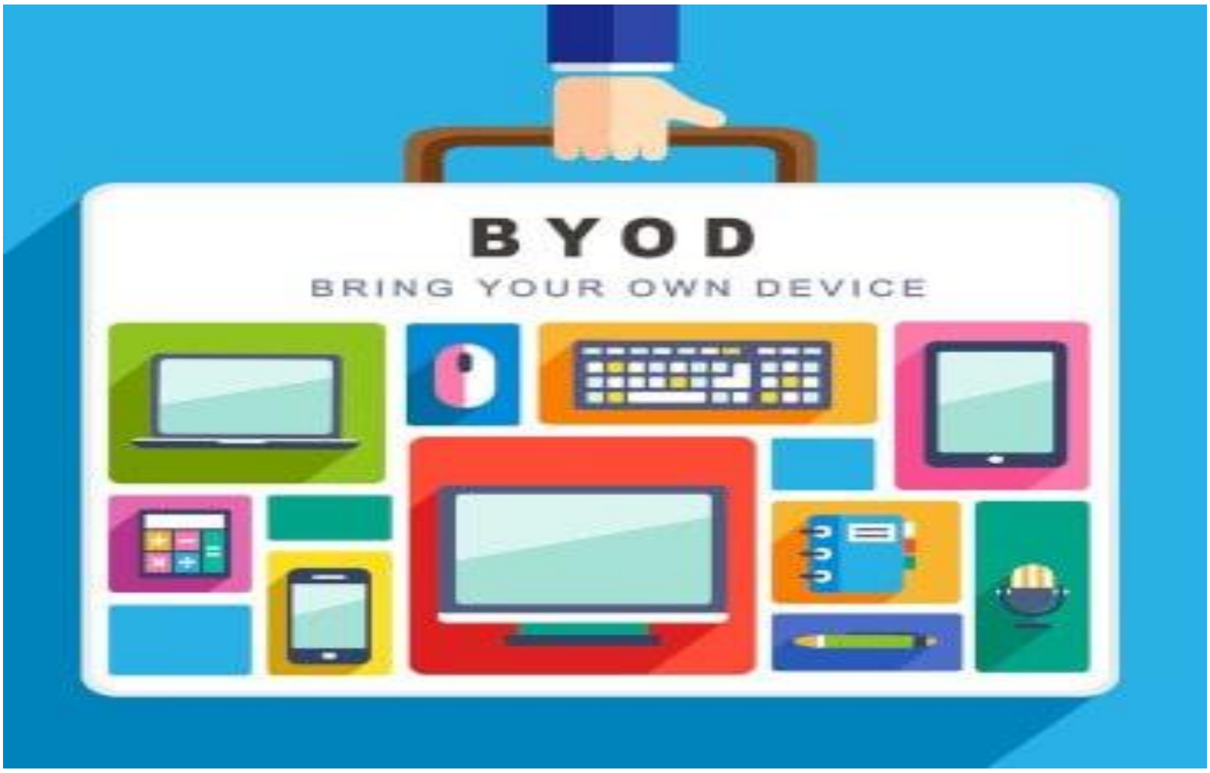
Enforcement

Inappropriate use may lead to account restrictions, security investigation, or disciplinary action.

5. Bring Your Own Device (BYOD) Policy

BYOD stands for bring your own device, and the most commonly accepted BYOD meaning is when employees use their own personal devices to connect to the organization's network and access what they need to do their jobs. This includes data and information that could be potentially sensitive or confidential.

The devices used for BYOD could include smartphones, tablets, personal computers, laptops, or USB drives. This offers employees more freedom to use the devices that make them better able to perform day-to-day tasks, which, in the long run, saves employers money. However, BYOD has to be carefully managed with a focus on maintaining security and productivity.



Purpose

To manage security risks associated with employees using personal devices for work purposes.

Scope

Covers all employees and contractors who use personal smartphones, laptops, or tablets to access company systems.

User Responsibilities

1. Devices must have password protection and be kept updated.
2. Company-approved security software must be installed (if required).
3. Users must report loss or theft of devices immediately.
4. Company reserves the right to remotely wipe company data from personal devices.
5. Personal devices may only access approved applications and systems.
6. Employees must not share their personal devices with unauthorized users.

Enforcement

Non-compliance may lead to removal of BYOD access and potential disciplinary action.

Conclusion for Security Policy Creation

The development and implementation of security policies are essential to maintaining the confidentiality, integrity, and availability of organizational data. By establishing clear security guidelines, organizations can proactively reduce risks, improve user awareness, and strengthen overall cybersecurity posture.

The five security policies created-password policy, remote work policy, data protection policy, email and internet use policy, and bring your own device (byod) policy-address key areas of security where users interact with sensitive systems daily. These policies not only guide user behaviour but also form a strong foundation for building a security-conscious organizational culture.

1.Password Policy

Establishes strong password requirements and promotes safe password practices to prevent unauthorized access.

2.Remote Work Policy

Provides guidelines for securely accessing company systems while working remotely to protect data outside the office environment.

3.Data Protection Policy

Ensures sensitive company and personal data are handled, stored, and shared securely, in compliance with regulations.

4.Email and Internet Use Policy

Defines acceptable use of email and internet resources to prevent misuse and reduce exposure to phishing and malware.

5.Bring Your Own Device (BYOD) Policy

Sets security requirements for employees using personal devices for work to control potential security risks.

Special Thanks

Elevate Labs

Thank You

Venkata Siva Sai Kumar Adimulam

Cybersecurity Aspirant.