

Example Acceptable Use Policy

This is an example acceptable use policy. Use this as a guide to write or revise the acceptable use policy for your organization.

~~~~~

## Acceptable Use Policy

### 1.0 Purpose

The purpose of this policy is to describe the acceptable use of computer equipment, software, operating systems, data storage media, and computer network resources owned, leased, or otherwise provided by [Organization Name] or devices that connect to a(n) [Organization Name] network or reside at an organization site. These rules are in place to protect our employees, our customers, and the organization from harm caused by misuse, either deliberate or inadvertent, of [Organization Name] systems and data.

### 2.0 Scope

This policy applies to all employees, contractors, and third-party vendors who have access to the organization's systems. Public access to the organization's externally reachable systems, such as its corporate website or public web applications, is excluded from this policy.

### 3.0 Policy

#### 3.1 Access and Authentication

- **Authorized use:** Information systems and data must be used only for legitimate business purposes.
- **Access control:** Users must use their own login credentials and not share them with others. Access should be granted based on the principle of least privilege.
- **Access restrictions:** Users should not access systems, network data, files, or information not directly related to their job function. Having access capabilities does not imply permission to use them.
- **Remote access:** Remote access to the organization's systems is permitted only through approved methods and must comply with all security protocols.

#### 3.2 Data Protection

- **Data protection:** Sensitive data must be encrypted and handled in accordance with organizational guidelines.

- **Password-protected screen savers:** All computers connected to the organization's network must be secured with a password-protected screen saver with the automatic activation feature set at 15 minutes or less. Users must lock the screen or log off when the device is unattended.

### 3.3 Monitoring and Auditing

- **Activity monitoring:** To maintain the security and integrity of our systems, the organization will monitor the use of all technology assets, including personal devices connected to the organization's network. Users should understand that privacy is not guaranteed when using the corporate network or organizational resources.
- **Periodic audits:** The organization reserves the right to periodically audit equipment, networks, and systems to ensure adherence to this policy and uphold its security standards.

### 3.4 Use of Devices and Equipment

- **Use of personal devices:** Users must obtain written permission before connecting personal devices to the organization's network. These devices must comply with the organization's security standards.
- **Personal use:** Users are responsible for exercising good judgment regarding the personal use of the organization's technology assets, ensuring it does not negatively impact the organization or their job performance. Departments should create guidelines for personal use, and users should consult their manager if uncertain.
- **Physical security:** Users must ensure that all portable devices are secured and not left unattended in public places.

### 3.5 Internet and Communication

- **Internet usage:** Users should use the internet responsibly and avoid accessing inappropriate websites. Streaming media should be limited to business purposes.
- **Email and communication activities:** Users must use organization email for business purposes and should not send unsolicited emails, spam, or chain letters.

### 3.6 Incident Reporting

Any security incidents or suspicious activities must be reported immediately to the IT department.

### 3.7 Prohibited Activities

Including but not limited to:

- **Engaging in illegal activities:** engaging in illegal activities or those that violate organizational policies
- **Security breach or network disruption:** engaging in activities that could lead to a security breach or network disruption

- **Introducing malicious programs:** introducing malicious programs, such as viruses, worms, or trojans, into the network
- **Unauthorized access:** revealing passwords or allowing unauthorized access to the organization's systems
- **Unauthorized copying of copyrighted material:** copying or distributing copyrighted material without proper authorization
- **Misuse of communication tools:** Using organization email or messaging systems to send unsolicited emails, spam, chain letters, or harassing messages
- **Misrepresentation:** impersonating another user or misrepresenting oneself while using the organization's systems
- **Inappropriate use of systems:** using the organization's systems to gamble, visit inappropriate websites, or download unauthorized content
- **Unapproved hardware:** connecting unauthorized hardware or devices to the organization's network
- **Unauthorized software:** installing or using software that has not been approved by the IT department
- **Tampering with security measures:** attempting to bypass or disable any security measures implemented by the organization
- **Personal gain:** using the organization's systems or information for personal gain or to conduct personal business

## 4.0 Responsibilities

### Employees

- Follow security protocols, report security incidents, and use information systems responsibly

### IT Department

- Implement security controls, monitor compliance, and provide technical support

### Managers

- Ensure their teams adhere to the security policy and support compliance efforts

### Security Officer

- Oversee the security strategy, enforce the policy, and investigate any violations or incidents

## 5.0 Compliance

Compliance with this policy is mandatory for all employees, contractors, and stakeholders. Noncompliance may result in disciplinary actions, including termination of employment, and could lead to legal consequences if it involves violations of laws and regulations.

## 6.0 Enforcement

This policy will be enforced with regular audits and continuous monitoring conducted by the security officer. Any violations of the policy will be subject to thorough investigation, and appropriate disciplinary measures will be taken based on the severity of the noncompliance. Actions may include warnings, retraining, suspension, or termination, depending on the nature of the violation.

## 7.0 Definitions

- **Sensitive data:** information that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization
- **Least privilege:** a principle that restricts users' access rights to the minimum necessary to perform their job functions
- **Encryption:** the process of converting information into a secure format that can only be accessed by authorized users

## 8.0 Review and Updates

This policy will be reviewed annually or as needed to ensure its relevance and effectiveness. The security officer is responsible for coordinating the review and update process. A revision history will be maintained to document changes and updates.

### Revision History

| Date       | Description of Change                    | Changed By     |
|------------|------------------------------------------|----------------|
| YYYY-MM-DD | [Initial draft or specific changes made] | [Name or role] |