

Acceptable Use Policy (AUP)

1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to define the acceptable use of [Organization Name]'s information technology (IT) resources, including but not limited to computers, networks, email, internet access, and software. This policy aims to ensure the security, integrity, and availability of these resources while promoting responsible and ethical use.

2. Scope

This policy applies to all employees, contractors, interns, and third parties who access or use [Organization Name]'s IT resources. It covers all devices, whether owned by the organization or personally owned, that connect to the organization's network or systems.

3. Acceptable Use

Users are expected to use [Organization Name]'s IT resources responsibly and in accordance with the following guidelines:

- **Work-Related Use:** IT resources are provided primarily for work-related purposes. Personal use is permitted only if it does not interfere with work responsibilities or violate this policy.
 - **Compliance with Laws:** Users must comply with all applicable laws, regulations, and organizational policies.
 - **Respect for Others:** Users must not engage in activities that harass, intimidate, or discriminate against others.
 - **Protection of Resources:** Users must take reasonable steps to protect IT resources from unauthorized access, misuse, or damage.
-

4. Unacceptable Use

The following activities are strictly prohibited:

- **Unauthorized Access:** Attempting to access systems, data, or networks without proper authorization.
 - **Malware Distribution:** Introducing malware, viruses, or other harmful software into the organization's systems.
 - **Data Theft:** Copying, transferring, or disclosing sensitive or confidential information without authorization.
 - **Illegal Activities:** Using IT resources for illegal purposes, such as hacking, fraud, or piracy.
 - **Inappropriate Content:** Accessing, storing, or distributing offensive, obscene, or inappropriate content.
 - **Resource Abuse:** Excessive use of bandwidth, storage, or other resources that negatively impacts system performance.
 - **Impersonation:** Pretending to be someone else or using someone else's credentials.
-

5. Email and Internet Use

- **Email:**
 - Use company email for work-related communication.
 - Do not open email attachments from unknown or untrusted sources.
 - Report suspicious emails to the IT department.
 - **Internet:**
 - Use the internet for work-related research and tasks.
 - Avoid visiting websites that are unrelated to work or pose security risks (e.g., gambling, adult content).
-

6. Password Security

- **Strong Passwords:** Use strong, unique passwords for all accounts (e.g., at least 12 characters with a mix of letters, numbers, and symbols).
 - **Password Sharing:** Do not share passwords with anyone, including colleagues.
 - **Password Changes:** Change passwords every 90 days or immediately if a breach is suspected.
-

7. Software and Hardware

- **Authorized Software:** Install only software approved by the IT department.
 - **Licensing:** Ensure all software is properly licensed.
 - **Hardware:** Use only company-approved hardware. Do not connect personal devices without prior approval.
-

8. Monitoring and Enforcement

- **Monitoring:** [Organization Name] reserves the right to monitor the use of IT resources to ensure compliance with this policy.
 - **Violations:** Violations of this policy may result in disciplinary action, up to and including termination of employment or legal action.
 - **Reporting:** Report any suspected violations or security incidents to the IT department immediately.
-

9. Acknowledgment

All users must acknowledge that they have read, understood, and agree to comply with this Acceptable Use Policy. Failure to comply may result in disciplinary action.

10. Review and Updates

This policy will be reviewed annually or as needed to ensure its relevance and effectiveness. Updates will be communicated to all users.

Acknowledgment Form

I, [Full Name], acknowledge that I have read, understood, and agree to comply with [Organization Name]'s Acceptable Use Policy. I understand that violations of this policy may result in disciplinary action, up to and including termination of employment or legal action.

Signature: _____

Date: _____

How to Use This AUP

1. **Customize:** Replace placeholders like [Organization Name] with your organization's details.
2. **Distribute:** Share the AUP with all employees and require them to sign the acknowledgment form.
3. **Enforce:** Ensure compliance by monitoring IT resource usage and addressing violations promptly.