# Acceptable Use Policy

**Purpose**

The purpose of the (Company) Acceptable Use Policy is to establish acceptable practices regarding the use of (Company) Information Resources to protect the confidentiality, integrity, and availability of information created, collected, and maintained.

**Scope**

This policy applies to all employees, contractors, consultants, temporary workers, and other individuals or entities using (Company) Information Resources. It covers all devices, systems, networks, software, and data owned, leased, or managed by (Company).

**Policy**

1. **General Use**
   * Information Resources are provided to support business activities and must be used in compliance with company policies, standards, and applicable laws.
   * Users must:
     + Use Information Resources in a manner that aligns with their job responsibilities and promotes productivity.
     + Exercise reasonable care to ensure resources are not wasted or misused.
     + Refrain from any personal use that could interfere with business operations or violate this policy.
   * Users are prohibited from:
     + Accessing, creating, or transmitting materials that are illegal, unethical, discriminatory, harassing, or otherwise inappropriate.
     + Using Information Resources for personal financial gain, political campaigning, or other non-business-related activities.
     + Deliberately accessing unauthorized systems, files, or data.
2. **Account and Access Management**
   * Users must:
     + Keep their authentication credentials (e.g., usernames, passwords, tokens) secure and not share them with others.
     + Use multi-factor authentication (MFA) where required.
     + Log out of systems or lock devices when not in use.
   * Access rights must be:
     + Granted based on job roles and responsibilities following the principle of least privilege.
     + Regularly reviewed and revoked promptly when no longer needed.
3. **Data Protection**
   * Users must:
     + Handle sensitive information (e.g., personal data, trade secrets) in accordance with company policies and relevant regulations.
     + Encrypt sensitive data during storage and transmission where required.
     + Securely delete or dispose of data when it is no longer needed.
     + Avoid sharing sensitive information with unauthorized individuals or third parties without proper approval.
   * Users must immediately report any suspected data breaches or accidental disclosures to the IT department.
4. **Prohibited Activities**
   * Users must not engage in:
     + Unauthorized access, use, or modification of systems, data, or resources.
     + Distributing or storing pirated software, copyrighted material, or unlicensed media.
     + Downloading or installing unapproved applications or software that could compromise system integrity.
     + Using company systems to spread malware, spam, or engage in phishing activities.
     + Activities that disrupt network operations, including excessive use of bandwidth for non-business purposes.
5. **Device Usage**
   * Only company-approved devices may connect to the corporate network.
   * Personal devices used for business purposes must comply with:
     + Company security standards, including installation of approved security software.
     + Encryption of business-related data stored on personal devices.
   * Users are responsible for securing devices against theft, loss, or unauthorized access.
6. **Monitoring and Privacy**
   * The company reserves the right to monitor and log:
     + Network traffic, email, and data usage for security, operational, and compliance purposes.
     + Use of company devices to ensure adherence to this policy.
   * Monitoring will be conducted in accordance with applicable laws and company guidelines.
7. **Incident Reporting**
   * Users must report any:
     + Suspected security incidents, including malware infections, phishing attempts, or unauthorized access.
     + Policy violations or misuse of Information Resources.
   * Reports must be made promptly to the IT department or designated authority.

**Compliance and Enforcement**

Failure to comply with this policy may result in:

* Disciplinary action, up to and including termination of employment.
* Termination of contracts for third-party entities.
* Legal action if violations involve illegal activities or significant breaches of trust.

**Review and Updates**

This policy will be reviewed annually and updated as necessary to ensure its continued relevance and effectiveness in addressing security and operational needs.

**Acknowledgment**

All users must acknowledge that they have read, understood, and agree to comply with this policy. Non-compliance may result in restricted access or other penalties.

**Effective Date:** [Insert Date]  
**Last Review Date:** [Insert Date]  
**Policy Owner:** [Insert Department or Role]

By signing below, I acknowledge that I have read and understood the (Company) Acceptable Use Policy and agree to adhere to its terms:

**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_