Acceptable Use Policy

Effective Date: April 7, 2025

Last Revised: April 7, 2025

Policy Owner: Information Technology Department

Purpose

This policy establishes guidelines for the appropriate use of [Company Name]'s technology resources, including computer equipment, software, networks, internet access, email, and other information systems.

Scope

This policy applies to all users of company technology resources, including employees, contractors, consultants, temporary workers, and other authorized individuals.

Authorized Use

1. Company technology resources are provided for business purposes.
2. Limited personal use is permitted provided it:
   - Does not interfere with job performance
   - Does not incur significant cost
   - Does not violate any company policies or laws
   - Does not negatively impact system performance
3. Users may not use company resources to:
   - Operate a personal business
   - Engage in political activities
   - Conduct illegal activities
   - Access inappropriate content

User Responsibilities

Account and Password Security

1. Users are responsible for all activities performed using their accounts.
2. Users must:

- Use strong, unique passwords
- Change passwords every 90 days
- Not share passwords or access credentials
- Lock workstations when unattended
- Report any suspected unauthorized access immediately

Software and Hardware

1. Only authorized software may be installed on company systems.
2. Users may not:
   - Install unauthorized software
   - Download software from untrusted sources
   - Connect unauthorized devices to company networks
   - Disable security controls (antivirus, firewalls, etc.)
   - Modify hardware configurations without IT approval

Data Protection

1. Users must handle company data according to its classification level.
2. Users are responsible for:
   - Storing sensitive data only on approved company systems
   - Using encryption when handling confidential information
   - Properly disposing of sensitive information
   - Not sharing sensitive information with unauthorized parties
   - Reporting data security incidents promptly

Email and Communication

1. Company email and messaging systems are primarily for business purposes.
2. Users must exercise caution when:
   - Opening email attachments
   - Clicking on links in emails
   - Providing company information via email
3. Email communications should be professional and appropriate.
4. Users may not use company email or messaging systems to:

- Send harassing or discriminatory messages
- Send unauthorized mass mailings
- Forward chain letters
- Impersonate others
- Send confidential information without proper protection

Internet Usage

1. Internet access is provided for business purposes.
2. Incidental personal use is permitted with reasonable limits.
3. Users may not use company internet access to:
   - Access, download, or distribute inappropriate content (pornography, hate speech, etc.)
   - Engage in illegal activities
   - Stream non-business videos, music, or games that consume significant bandwidth
   - Use peer-to-peer file sharing applications
   - Circumvent security measures

Remote Access

1. Remote access to company systems must be conducted through approved methods only.
2. Users must:
   - Use the company VPN when accessing internal resources
   - Ensure their remote devices meet company security standards
   - Not access sensitive information on public networks without proper security measures
   - Protect company information from unauthorized viewing

Monitoring and Privacy

1. [Company Name] reserves the right to monitor all technology resource usage.
2. Users should have no expectation of privacy when using company systems.
3. Monitoring may include:
   - Email content and metadata
   - Internet browsing history
   - File access and transfers
   - Software and application usage

- Network traffic

Social Media

1. When using social media, users must:
   - Not disclose confidential company information
   - Make it clear personal opinions are not company positions
   - Not engage in harassment or discrimination
   - Comply with the company's Social Media Policy

Mobile Devices

1. Company-owned mobile devices must:
   - Be password protected
   - Have remote wipe capability enabled
   - Be encrypted
   - Have approved security software installed
2. Personal devices used for business purposes must comply with the Bring Your Own Device (BYOD) Policy.

Compliance and Violations

1. Violations of this policy may result in:
   - Restriction of technology access
   - Disciplinary action up to and including termination
   - Legal action if applicable
2. Users must report suspected violations to:
   - Their manager
   - IT Department
   - HR Department
   - Anonymous ethics hotline: [Phone Number]

Exceptions

Exceptions to this policy require written approval from the Chief Information Officer or designee.

Related Policies

- Information Security Policy
- Data Classification Policy
- Password Policy
- Social Media Policy
- Bring Your Own Device (BYOD) Policy
- Email Policy

User Acknowledgment

I acknowledge that I have read and understand this Acceptable Use Policy. I agree to adhere to all the rules and guidelines contained herein.

User Signature Date

User Name (Printed)