Zerotrace

Acceptable Usage Policy

Version 1.0

Effective Date: May, 4 2025

Table of Contents

1. Introduction and Purpose

1.1 Purpose: This Acceptable Usage Policy (AUP) outlines the rules and guidelines for the use of the organization's Information Technology (IT) resources, including networks, systems, devices, software, and data. Its primary purpose is to:

- Protect the confidentiality, integrity, and availability of the organization's information assets.
- Ensure compliance with relevant laws, regulations, and ethical standards.
- Prevent misuse of IT resources that could lead to security risks, such as data exfiltration, virus attacks, unauthorized access, or compromise of network systems.
- Maintain a productive and secure digital environment for all users.
- Define acceptable and prohibited behaviors related to IT resource use.

1.2 Philosophy: Access to the organization's IT resources is a privilege granted to support its mission and objectives. Users are expected to act responsibly and ethically, consistent with the organization's values.

2. Scope

2.1 Applicability: This policy applies to all individuals who access or use the organization's IT resources, including but not limited to:

- Employees (full-time, part-time, temporary)
- Contractors and Consultants
- Volunteers and Interns
- Students (if applicable, particularly regarding academic resources)
- Guests and Visitors granted access
- Any other individual or entity interacting with the organization's IT resources.

2.2 Resources Covered: This policy covers the use of all organization-owned or leased IT resources, as well as personal devices (Bring Your Own Device - BYOD) when connected to the organization's network or used to access/store organizational data. This includes, but is not limited to:

- Computers (desktops, laptops), servers, mobile devices (smartphones, tablets)
- Network infrastructure (wired and wireless)
- Internet access provided by the organization
- Email systems and communication platforms (e.g., instant messaging)
- Software (licensed, developed in-house, cloud-based)
- Data and information stored, processed, or transmitted using organizational resources.
- Peripherals (printers, scanners, storage devices).

3. Authorized and Acceptable Use

3.1 General Use: Users must utilize IT resources primarily for purposes directly related to their job responsibilities, studies (if applicable), or assigned tasks that support the organization's objectives.

3.2 Incidental Personal Use: Limited and occasional personal use of IT resources (e.g., brief personal emails, quick internet searches) may be permissible, provided it:

- Does not interfere with the user's duties or the work of others.
- Does not consume excessive resources (e.g., bandwidth, storage).
- Does not incur direct costs for the organization without approval.
- Does not violate any other terms of this AUP or other organizational policies.
- Is conducted responsibly and professionally.
- Storage of personal files must be nominal.

3.3 Specific Permissions: Access to specific systems, data, or functionalities is granted based on roles and responsibilities. Users must only access resources for which they have explicit authorization.

4. Unacceptable Use

The following activities are strictly prohibited when using the organization's IT resources. This list is not exhaustive:

4.1 Illegal and Unethical Activities:

- Engaging in any activity that violates local, state, federal, or international laws or regulations.
- Violating copyright, patent, trade secret, or other intellectual property rights, including unauthorized copying or distribution of software, music, videos, or documents ("piracy").
- Unauthorized export of software or technical information.
- Fraudulent activities or misrepresentation.

4.2 Security Violations:

- Attempting to bypass or subvert system or network security measures (e.g., firewalls, access controls, authentication).
- Introducing malicious software (viruses, worms, trojans, ransomware, spyware) into the network.
- Unauthorized port scanning, security scanning, or network monitoring.
- Executing denial-of-service attacks or any action intended to interfere with or disable systems or services.
- Unauthorized access, use, or attempted access to data, accounts, systems, or networks. This includes accessing data beyond one's authorized level or job requirements.
- Connecting unauthorized devices to the organization's network.
- Installing unauthorized software or hardware.

- Sharing passwords, access cards, security tokens, or other authentication credentials. Failing to secure access credentials is also prohibited.

4.3 Data Handling and Confidentiality:

- Unauthorized access, copying, downloading, printing, storing, or transmitting of confidential, sensitive, or proprietary information.
- Disclosing confidential information to unauthorized parties, internally or externally.
- Storing confidential data in unsecured locations or on personal devices without proper authorization and security controls.
- Sending confidential information via unsecured email or other communication channels.

4.4 Communication and Content:

- Transmitting or accessing material that is offensive, obscene, pornographic, discriminatory, harassing, threatening, abusive, defamatory, or otherwise objectionable.
- Engaging in harassment, bullying, or creating a hostile environment via electronic communications.
- Sending unsolicited bulk emails ("spam") or chain letters.
- Forging email headers or impersonating others.
- Using IT resources for personal commercial activities, political campaigning (in a way that suggests organizational endorsement), or excessive personal social media use.

4.5 Resource Usage:

- Activities that degrade system or network performance.
- Excessive use of bandwidth (e.g., streaming non-work-related media, large personal file downloads).
- Wasting resources like disk space or printer supplies.

5. Security Practices and User Responsibilities

All users share responsibility for maintaining the security and integrity of the organization's IT resources. Users must:

- **Password Security:** Create strong, unique passwords meeting organizational complexity requirements; change passwords regularly; never share passwords; protect passwords from disclosure.
- **Account Security:** Be responsible for all activities conducted under their user accounts. Log off or lock devices when left unattended.
- **Device Security:** Ensure devices (including personal devices used for work) have up-to-date operating systems, security software (e.g., antivirus), and necessary patches. Protect devices from theft or unauthorized access, especially when off-site.
- **Email and Downloads:** Exercise caution when opening email attachments or clicking links, especially from unknown senders. Do not download or install software from untrusted sources.

- **Data Protection:** Handle confidential and sensitive data according to organizational policies and classifications. Use encryption where required or appropriate. Ensure physical security for printed sensitive documents (e.g., shredding).
- **Reporting:** Promptly report any suspected security incidents, vulnerabilities, policy violations, or loss/theft of devices or data to the designated IT or Security department.
- **Compliance:** Adhere to this AUP and all other related organizational policies and guidelines.

6. Data Privacy and Confidentiality

- Users must respect the privacy of others.
- Users must handle personal and confidential data (related to employees, customers, partners, or the organization itself) with care and only access/use it as required for legitimate organizational purposes.
- Unauthorized collection, use, or disclosure of personal or confidential information is strictly prohibited.
- Users should be aware that electronic communications and activities on organizational IT resources may be monitored for security, compliance, and operational purposes, subject to applicable laws and regulations. There should be no expectation of privacy for activities conducted using organizational IT resources, except as legally mandated.

7. Software and Intellectual Property

- Users must respect all software licensing agreements and copyright laws.
- Only authorized and properly licensed software may be installed and used on organizational devices. Unauthorized installation or use of software is prohibited.
- Intellectual property created using organizational resources may be subject to organizational ownership policies.

8. Monitoring and Enforcement

8.1 Monitoring: The organization reserves the right to monitor the use of its IT resources at any time to ensure compliance with this policy, maintain security, and support operational needs, subject to applicable laws. This may include monitoring network traffic, email, internet usage, and file access.

8.2 Violations: Violations of this AUP may result in disciplinary action, up to and including termination of employment, contract, or relationship with the organization. Penalties may also include suspension or loss of access privileges, legal action, and referral to law enforcement authorities if illegal activities are involved.

8.3 Investigation: The organization reserves the right to investigate suspected violations. This may involve inspecting user devices, accessing user accounts and files stored on organizational systems, and cooperating with law enforcement agencies.

9. Policy Acknowledgment

All users may be required to acknowledge that they have read, understood, and agree to comply with this Acceptable Usage Policy as a condition of being granted access to organizational IT resources.

10. Disclaimer

The organization is not responsible for loss or damage resulting from the misuse of its IT resources or for personal data stored on organizational systems. While the organization takes reasonable security measures, it cannot guarantee the security or privacy of communications or data.