**Cybersecurity Templates**

**Cybersecurity Readiness Checklist**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Permissible use of Assets** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** |  | **Approved By:** |  |
| **Last Review Date:** |  | **Next Review Date:** |  |

Contents

[1. Permissible Use of Assets Policy 3](#_Toc206632540)

[**1.1.Authority** 4](#_Toc206632541)

[**1.2.Purpose** 4](#_Toc206632542)

[**1.3.Scope** 4](#_Toc206632543)

[**1.4.General Principles** 4](#_Toc206632544)

[**1.5.Permissible Use** 4](#_Toc206632545)

[**1.6.Prohibited Use** 5](#_Toc206632546)

[**1.7.Special Considerations** 5](#_Toc206632547)

[**1.8.Roles and Responsibilities** 5](#_Toc206632548)

[**1.9.Enforcement & Disciplinary Action** 6](#_Toc206632549)

[**1.10.Policy Review & Maintenance** 6](#_Toc206632550)

[**1.11.Acknowledgement** 6](#_Toc206632551)

# Permissible Use of Assets Policy

|  |  |
| --- | --- |
| **Title:** Cybersecuritypolicy | |
| **Department:** | **Version:** Original |
| **Approved by:** | **Approval date:** |
| **Senior management approval:** | |
| **Effective date:** | **Last updated:** |
| **Author:** | |
| This policy applies to <company name>, <enter address>. | |
| **1.1.Authority**  This policy is hereby approved and authorized.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_  Name Title Date  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_  Name Title Date | |
| **1.2.Purpose**  This policy establishes the rules governing the permissible use of organizational assets, including information, technology, and physical resources. Its objective is to protect confidentiality, integrity, and availability while ensuring assets are used responsibly, securely, and in alignment with organizational values and regulatory obligations. | |
| **1.3.Scope** This policy applies to:   * All employees, contractors, interns, and third parties with access to organizational assets. * All forms of assets: information (digital or physical), IT systems, devices, networks, cloud services, communication tools, and physical equipment. | |
| **1.4.General Principles**  1. **Business Use Priority**: Organizational assets must be used primarily for business purposes. Limited personal use is permissible if it does not interfere with productivity, security, or compliance. 2. **Compliance**: All use of assets must comply with internal policies, contracts, and external legal/regulatory requirements. 3. **Monitoring**: The organization reserves the right to monitor asset use to ensure compliance, subject to applicable privacy laws. 4. **Ownership**: All information created, stored, transmitted, or processed using organizational assets is considered the property of the organization. | |
| **1.5.Permissible Use** Employees and authorized users may:   * Access organizational systems and data only within the scope of their role. * Use email, collaboration tools, and communication platforms for legitimate business purposes. * Store and process data in line with data classification and protection standards. * Install or use approved software and applications relevant to their work. * Access cloud services authorized by the organization. | |
| **1.6.Prohibited Use** Users must not:   * Engage in unlawful, harassing, discriminatory, or offensive activities. * Download, share, or distribute pirated, copyrighted, or unlicensed material. * Bypass or disable security controls such as firewalls, antivirus, or monitoring systems. * Access or attempt to access data, systems, or networks without authorization. * Store or transmit sensitive company data using unauthorized storage or email services. * Use organizational assets for personal commercial gain, political activity, or religious solicitation. * Install unapproved hardware, software, or peer-to-peer applications. * Deliberately introduce malware or malicious code. * Share or disclose confidential information without proper authorization. * Use organizational communication systems for mass unsolicited emails (“spam”). | |
| **1.7.Special Considerations** **Physical Assets**   * Keep organizational devices (laptops, mobiles, tablets) secured and lock devices when unattended. * Do not remove physical assets from organizational premises without approval. * Report loss or theft of assets immediately.   **Information Handling**   * Follow information classification and handling procedures. * Use encryption when transmitting sensitive data. * Avoid discussing confidential matters in public or unsecured environments.   **Cloud and Remote Work**   * Only use authorized cloud services for business purposes. * Maintain secure connections (e.g., VPN) when accessing organizational resources remotely. * Do not mix personal and corporate accounts for storing or transmitting organizational data.   **Email and Communications**   * Use corporate email only for business-related communications. * Refrain from sending inappropriate, offensive, or confidential data to unauthorized recipients. * Treat suspicious emails with caution and report phishing attempts.   **Passwords and Authentication**   * Use strong, unique passwords as per organizational password policy. * Do not share passwords under any circumstances. * Enable multi-factor authentication (MFA) where available. | |
| **1.8.Roles and Responsibilities**  * **Employees/Users**: Responsible for adhering to this policy and reporting any violations or suspicious activities. * **Managers**: Ensure team members understand and comply with this policy. * **IT & Cybersecurity Team**: Provide secure systems, monitor compliance, and respond to violations. * **HR & Legal**: Enforce disciplinary measures for violations, aligned with contracts and law. | |
| **1.9.Enforcement & Disciplinary Action** Violations of this policy may result in disciplinary action up to and including termination of employment or contracts, legal prosecution, and financial liability, depending on severity and impact. | |
| **1.10.Policy Review & Maintenance** This policy will be reviewed at least annually, or sooner if significant regulatory, technological, or organizational changes occur. | |
| **1.11.Acknowledgement** I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, acknowledge that I have read, understood, and agree to comply with the **Permissible Use of Assets Policy**. I understand that violations may lead to disciplinary action.  **Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |