## Technology Use Policy Template

**Effective Date**: [Insert Date]
**Revision Date**: [Insert Date]
**Approved By**: [Insert Approving Body]

**1. Purpose**

To establish guidelines for the use, security, and management of [ORGANIZATION NAME]’s technology resources to protect data, maintain operational efficiency, and ensure compliance with legal and regulatory requirements.

**2. Scope**

This policy applies to all employees, contractors, volunteers, and any other individuals who have access to the organization’s technology systems, devices, or data.

**3. Technology Use Guidelines**

1. **Acceptable Use**:
	* Technology resources must be used for organizational purposes only.
	* Personal use is limited and must not interfere with work responsibilities or system performance.
2. **Prohibited Activities**:
	* Accessing inappropriate or illegal content.
	* Downloading unauthorized software.
	* Sharing confidential organizational data without proper authorization.

**4. Password Security**

1. Passwords must:
	* Be at least [INSERT NUMBER] characters long.
	* Include uppercase and lowercase letters, numbers, and special characters.
	* Be updated every [INSERT TIMEFRAME, E.G., 90 DAYS].
2. Password sharing is prohibited.
3. Default passwords on all devices and accounts must be changed immediately upon setup.

**5. Data Protection**

1. **Confidential Data**:
	* Must be encrypted during transmission and storage.
	* Access is limited to authorized personnel based on role-specific needs.
2. **Data Backup**:
	* All critical data must be backed up daily using [INSERT METHOD, E.G., cloud-based systems].
	* Backups must be stored securely and tested periodically for recovery.
3. **Data Disposal**:
	* Electronic devices must be wiped clean of all data before disposal or repurposing.

**6. Cybersecurity Measures**

1. **Antivirus and Firewalls**:
	* All devices must have up-to-date antivirus software and firewalls enabled.
2. **System Updates**:
	* Operating systems, software, and applications must be updated regularly to address security vulnerabilities.
3. **Monitoring and Logging**:
	* Technology use and network activity may be monitored to detect unauthorized access or suspicious behavior.

**7. Incident Reporting and Response**

1. **Reporting Security Incidents**:
	* All security incidents, such as phishing attempts, malware infections, or unauthorized access, must be reported immediately to [INSERT POSITION, E.G., IT Manager].
2. **Response Plan**:
	* Isolate affected systems to prevent the spread of threats.
	* Investigate and document the incident.
	* Notify relevant stakeholders, including regulatory authorities if required.
3. **Recovery**:
	* Restore data and systems from the most recent backup.
	* Evaluate and enhance cybersecurity measures to prevent future incidents.

**8. Remote Work Security**

1. Employees working remotely must:
	* Use secure, organization-provided VPN connections.
	* Avoid accessing organizational systems over public Wi-Fi unless using a secure hotspot or VPN.
2. Organizational devices used remotely must:
	* Be password-protected and encrypted.
	* Have remote-wipe capabilities enabled in case of loss or theft.

**9. Training and Awareness**

1. All employees must complete annual cybersecurity training covering:
	* Recognizing phishing and other social engineering attacks.
	* Best practices for password and data protection.
	* Incident reporting procedures.
2. New hires must complete cybersecurity training within their first [INSERT TIMEFRAME, E.G., 30 DAYS] of employment.

**10. Policy Review and Updates**

1. The [INSERT POSITION, E.G., IT Manager] will review this policy annually.
2. Revisions will be submitted to the board for approval.

**11. Approval and Adoption**

This policy was approved by the Board of Directors on [Insert Date].

Approved by: [Insert Name or Position]
Date: [Insert Date]
Review Date: [Insert Date]
Next Review Date: [Insert Date]