[Company Name] Technology Policy

Effective Date: [Date]

1. **Introduction**
    a. Purpose: The purpose of this Technology Policy is to establish guidelines and standards for the appropriate use of technology resources and the protection of sensitive information at [Company Name].
    b. Scope: This policy applies to all employees, contractors, vendors, and any other individuals who have access to [Company Name]'s technology resources, including but not limited to computers, networks, software applications, and data.
2. **Acceptable Use**
    a. Authorized Use: All technology resources provided by [Company Name] are to be used for business purposes only. Employees are expected to use these resources professionally, responsibly, and in compliance with applicable laws and regulations.
    b. Prohibited Use: Unauthorized or inappropriate use of technology resources is strictly prohibited. This includes, but is not limited to:
        1. Accessing or distributing illegal or offensive material.
        2. Introducing malware, viruses, or other harmful software.
        3. Unauthorized access to sensitive information or systems.
        4. Tampering with or altering network settings, configuration, or hardware.
        5. Unauthorized installation of software or hardware.
        6. Unauthorized disclosure of sensitive information.
        7. Infringement of intellectual property rights.
3. **Data Security and Privacy**
    a. Protection of Sensitive Information: Employees must adhere to strict data protection measures to prevent unauthorized access, disclosure, alteration, or destruction of sensitive information. Employees are required to:
        i. Safeguard passwords and access credentials.
        ii. Encrypt sensitive data during transmission and storage.
        iii. Follow secure data storage and disposal practices.
        iv. Adhere to proper data classification and handling guidelines.
        v. Report any suspected data breaches or security incidents immediately.
4. **Network Security**
    a. Access Controls: Employees will be provided with authorized access to the company's network resources based on job role and responsibilities. Unauthorized access attempts, sharing of login credentials, or attempting to bypass security measures are strictly prohibited.
    b. Wireless Network Usage: Employees must adhere to the guidelines and restrictions when connecting to [Company Name]'s wireless network. Personal devices, unless approved by IT, should not be connected to the company's network.
5. **Software Usage**
    a. Licensed Software: Employees must only use software applications that are legally licensed and approved by [Company Name]. Unauthorized installation or use of unlicensed software is strictly prohibited.

b. Regular Updates: Employees are responsible for regularly updating their software applications to the latest approved versions to ensure security patches and enhancements are applied promptly.

6. **Reporting and Compliance**
    a. Security Incidents: Employees must promptly report any suspected security breaches, incidents, or violations of this policy to the IT department or their supervisor. Reporting such incidents enables appropriate investigations and remediation measures to be undertaken.
    b. Compliance: Employees must comply with all relevant laws, regulations, contractual obligations, and internal policies when using [Company Name]'s technology resources.
7. **Enforcement and Consequences**
    a. Violations: Violations of this Technology Policy may result in disciplinary action, up to and including termination of employment. Legal action may also be pursued if necessary.
    b. Review and Updates: This Technology Policy will be reviewed periodically to ensure its relevance and effectiveness. Updates may be made as required, and employees will be notified of any significant changes.

By signing below, I acknowledge that I have read, understood, and agree to adhere to the provisions outlined within this Technology Policy.

Employee Name: _____

Date: _____