**Information Security Policy: Required Software for Systems Accessing Company Data**

**Policy Statement:**

All computers and systems accessing company data, including but not limited to files, emails, and sensitive information, must adhere to the following requirements. This policy is crucial for safeguarding the confidentiality, integrity, and availability of our company's information assets.

**1. Remote Management and Cybersecurity Software Requirement:**

All devices (computers, laptops, servers, etc.) that connect to the company's network and access company data must have the designated remote management and cybersecurity software installed and operational. This software is essential for monitoring, managing, and securing systems against potential threats, vulnerabilities, and unauthorized access.

**2. Installation Guidelines:**

a. **Pre-Access Requirement:** It is mandatory that the designated remote management and cybersecurity software is installed on any new system before it is granted access to company data or email services.

b. **Timely Updates:** Ensure that the software is kept up-to-date with the latest security patches and updates. Regularly scheduled updates are essential to address emerging threats and vulnerabilities. The remote management software installed by (COMPANY NAME) keeps the operating system, and key third part applications up to date. You maybe notified from time to time via a message when the system requires a restart to complete updates. It is required that you perform the restart when convenient, or within 24 hours of receiving the notification.

**3. Importance of Compliance:**

a. **Protecting Company Assets:** The designated software serves as a critical component in our overall cybersecurity strategy, actively working to protect company data from unauthorized access, malware, and other cyber threats.

b. **Monitoring and Response:** The remote management features allow our IT team to monitor system health, detect potential issues, and respond promptly to security incidents, minimizing the impact on company operations.

**4. Compliance Verification:**

a. **Regular Audits:** Periodic audits will be conducted to ensure compliance with this policy. Non-compliance may result in access restrictions or other disciplinary actions.

b. **Documentation:** Users and IT administrators are required to maintain documentation confirming the installation and proper functioning of the designated software on each system.

**5. Reporting Security Incidents:**

In the event of any suspicious activity, security incidents, or concerns related to the designated software, users must promptly report such incidents to the IT department for investigation and resolution.

**6. Policy Review:**

This policy will be subject to periodic review and updates to align with emerging cybersecurity threats and changes in technology. Users will be notified of any amendments to this policy.

**Acknowledgment:**

By accessing company data, users acknowledge their understanding and commitment to complying with this policy. Failure to adhere to these requirements may result in disciplinary action, including but not limited to access restrictions and termination of access privileges.

*Date of Policy Implementation: (DATE)*

*Policy Owner: (COMPANY NAME)*