**Information Security Policy: Acceptable Use Policy**

**Policy Statement:**

This Acceptable Use Policy outlines the guidelines and expectations for the acceptable use of company information technology resources. It is imperative that all users exercise responsible and ethical behavior while utilizing these resources to ensure the security, confidentiality, and integrity of the company's information assets.

**1. Authorized Use:**

a. **Permitted Activities:** Users are authorized to use company IT resources for work-related activities that contribute to the achievement of business objectives.

b. **Access Control:** Users are granted access only to the systems and data necessary for the performance of their job duties.

**2. Prohibited Activities:**

a. **Unauthorized Access:** Users must not attempt to access, modify, or delete information for which they do not have proper authorization.

b. **Malicious Software:** Users are prohibited from introducing or spreading malicious software, including viruses, malware, and other harmful programs.

c. **Illegal Activities:** Any engagement in illegal or unethical activities using company IT resources is strictly prohibited.

d. **Personal Use:** Limited personal use of company IT resources is acceptable, but it should not interfere with work responsibilities, consume excessive resources, or violate other policies.

**3. Data Protection and Confidentiality:**

a. **Data Classification:** Users must be aware of and comply with data classification policies, handling sensitive information with the appropriate level of confidentiality.

b. **Data Sharing:** Sharing company data externally must be done in accordance with company policies and applicable laws.

**4. Email and Communication:**

a. **Professional Conduct:** Users are expected to communicate professionally and ethically through company email and other communication channels.

b. **Avoiding Misinformation:** Users should exercise caution when forwarding emails or sharing information to prevent the spread of misinformation or malicious content.

**5. Social Media:**

a. **Responsible Use:** If using social media for work-related activities, users must do so responsibly and in accordance with company guidelines.

**6. Remote Access:**

a. **Secure Connection:** When accessing company resources remotely, users must use secure and approved methods to ensure the confidentiality and integrity of data.

b. **Protection of Devices:** Users are responsible for the security of their devices used for remote access, including implementing appropriate security measures.

**7. Reporting Security Incidents:**

a. **Prompt Reporting:** Users must promptly report any suspected or actual security incidents, including unauthorized access or the loss of company devices, to the IT department.

**8. Consequences of Violation:**

a. **Disciplinary Action:** Violation of this Acceptable Use Policy may result in disciplinary action, including but not limited to account suspension, access restrictions, or termination of employment.

**9. Policy Review:**

This policy will be subject to periodic review and updates to align with industry best practices and emerging cybersecurity threats.

**Acknowledgment:**

By using company IT resources, users acknowledge their understanding of and commitment to complying with this Acceptable Use Policy.

*Date of Policy Implementation: (DATE)*

*Policy Owner: (COMPANY NAME)*