**Social Media Security Policy**

**Policy Statement**

This Social Media Security Policy will elaborate the guidelines and best ways to ensure the secure and safe use of social media within our premisis. It is important to safeguard sensitive information and maintain the reputation and integrity of our company.

**Policy Guidelines**

**Privacy Settings:** Set privacy settings on personal accounts to limit access to personal information. Do not accept requests from unknown individuals.

**Reporting Incidents:** It is very important to report the suspicious activity or security breaches involving social media accounts promptly to the IT department.

**Authorized Usage:** Employees can use social media for business purposes only when it is their role and has been approved by their department head.

**Protection of Information:** Employees must refrain from sharing confidential or sensitive company information with public.

**Password Security:** Maintain strong and unique passwords for all social media accounts, and enable two-factor authentication where available.

**Endorsements and Representations:** Clearly distinguish personal opinions from those representing the company. Do not claim to speak on behalf of the company unless allowed.

**Phishing Awareness:** Be vigilant for phishing attempts and do not click on suspicious links or download files from unverified sources.

**BYOD (Bring Your Own Device) Policy**

**Policy Statement**

This BYOD (Bring Your Own Device) Policy implements the use of personally-owned devices for work activities, ensuring security, data protection, and compliance with company policies.

**Policy Guidelines**

**Eligible Devices:** Employees may use personally-owned devices (laptops, smartphones, tablets) for work if they meet the company's minimum security standards, as determined by the IT department for example using a laptop with a more secure hardware architecture.

**Security Measures:** Devices must have up-to-date antivirus software, encryption, and strong, unique passwords.

**Access Control:** Employees are granted access to company resources on a need-to-know basis, and only through secure, authorized methods.

**Compliance:** All employees using BYOD must adhere to company policies, as well as relevant laws and regulations, to protect company data and privacy.

**Termination or Resignation:** Upon termination or resignation, employees must cooperate with the IT department to remove company data and applications from their personally-owned devices.

**Data Protection:** Employees must follow data handling and confidentiality policies, ensuring that company data is secure and for example: not stored locally on personal devices.

**Reporting Loss or Theft:** Employees must report the loss or theft of their personally-owned devices used for work immediately to the IT department and follow company procedures for remote wiping if necessary.

By adhering to this BYOD policy, employees contribute to the secure and responsible use of personally-owned devices within the organization, maintaining the integrity of our data and operations.