**BYOD Security Policy**

# 1. Introduction

This security policy provides the best practices and guidelines to all the contractors and employees who use their devices to access, transmits and store company data and resources. The major aim of this policy is to protect company data while allowing all employees to access them on personal devices.

# 2. Scope

This policy applies to all the workforce in the company, including employees, contractors, and third parties who can access the company resources through their own devices. It includes all the devices through which data can be accessed, and it is not limited to laptops and phones.

# 3. Policy Statement

# 3.1 Acceptable Usage

All the employees are allowed to work on their devices for work-related purposes only, strictly following the security guidelines and practices.

# 3.2 Registration of Devices

All personal devices used while working should be registered with the IT department. To follow this policy, sufficient data must be provided, including device identification and user consent.

# 3.3 Security Policy

All the employees are responsible for securing their devices by using strong passwords, enabling biometric authentications, and using updated security patches and anti-virus software. All the devices should be encrypted to protect sensitive data.

# 3.4 Protection of data

Sensitive company business information should be stored in secured cloud services and accessed through authorized devices and applications. Data backups are mandatory, and all employees are responsible for regular backups of their data

# 3.5 Remote Wipe and Management

The IT department reserves the right to remotely wipe company data from any personal device stolen or compromised.

# 3.6 Timely Reporting of Security Incidents

All the employees must report any security incident and issues immediately to the IT department so that prompt action can be taken.

# 3.7 Exit Procedure

All the relevant information and business data will be removed if an employee leaves the organization.

# 4. Compliance

Failure to follow this security policy may result in serious disciplinary action, including termination and legal action.

# 5. Review and Revision

This policy will be reviewed and revised annually or as needed to ensure its effectiveness and alignment with changing security protocols.

# 6. Acknowledgement

I have read and understood the security policy, and I agree to comply with its provisions and understand the consequences of non-compliance

# Social Media Security Policy

# Policy Statement

This security policy outlines all the guidelines for safe and responsible social media usage by employees and associates to protect the company's reputation and data.

# 1. Purpose

Ensure safe and reliable social media usage to protect sensitive information, maintain consistent branding, and comply with legal requirements.

# 2. Scope

Applicable to all the employees, contractors, and consultants using social media that could impact the company's business and reputation.

# 3. Guidelines for Secure Social Media Usage

# 3.1 Accounts Management

* Use separate accounts for both personal and professional
* Always use strong and unique passwords and turn on the multi-factor authentication.

# 3.2 Content Posting

* Never use any social media accounts to save sensitive information.
* Only share sensitive information with the company's proper approval.
* In shared content, always use professional language to avoid disputes.

# 3.3 Privacy and Data Protection

* Always obtain consent before sharing any other personal information.
* Avoid unnecessary location sharing.

# 3.4 Security Awareness

* Be active and vigilant for phishing attempts
* Provide social media security training.

# 3.5 Reporting Security Accidents

Report security incidents immediately to the relevant department.

# 4. Compliance

Failure to follow this security policy may result in serious disciplinary action, including termination and legal action.

# 5. Review and Revision

This policy will be reviewed and revised annually or as needed to ensure its effectiveness and alignment with changing security protocols.

# 6. Acknowledgement

I have read and understood the security policy, and I agree to comply with its provisions and understand the consequences of non-compliance.