Information Security Policy

1. Purpose

The purpose of this Information Security Policy is to protect the organization's information assets from unauthorized access, misuse, disclosure, alteration, or destruction. This policy establishes clear security requirements to ensure confidentiality, integrity, and availability of company data.

---

2. Scope

This policy applies to all employees, contractors, interns, and third parties who access company systems, networks, or data. Compliance with this policy is mandatory regardless of work location, including on-site and remote work environments.

---

3. Use of Company-Approved Devices

3.1 Authorized Devices

- All employees must use **company-approved devices** to access company systems, applications, and data.
- Personal devices are not permitted unless explicitly approved by the IT department.
- Devices must be configured according to company security standards.

3.2 Device Responsibility

Employees are responsible for:

- Safeguarding assigned devices
- Preventing unauthorized access
- Reporting loss, theft, or damage immediately to IT or management

---

4. Access Control and Authentication

4.1 User Accounts

- Each employee is assigned a unique user ID.
- User accounts must only be used by the assigned individual.
- Shared or generic accounts are strictly prohibited unless approved for specific business needs.

4.2 Password Management

- Passwords must be changed **every 90 days**.
- Passwords must meet complexity requirements, including a combination of letters, numbers, and special characters.
- Reusing previous passwords is discouraged.
- Passwords must not be written down or stored in unsecured locations.

---

5. Credential Sharing

- **Sharing credentials is strictly prohibited** under all circumstances.
- Employees must not disclose passwords, PINs, or authentication codes to anyone, including colleagues or managers.
- IT personnel will never request passwords directly.
- Any suspected credential compromise must be reported immediately.

---

6. Data Protection and Confidentiality

- Employees must handle company data in accordance with confidentiality requirements.
- Sensitive information must only be accessed on a need-to-know basis.
- Confidential data must not be copied, transferred, or stored on unauthorized devices or platforms.
- Data must be securely deleted when no longer required.

---

7. Network and System Security

- Employees must connect only to secure and trusted networks.
- Use of public or unsecured Wi-Fi networks for company work is discouraged.
- Antivirus software, firewalls, and security updates must remain enabled at all times.
- Unauthorized software installation is prohibited.

---

8. Remote Work Security

Employees working remotely must:

- Use company-approved VPNs where required
- Ensure devices are locked when unattended
- Prevent unauthorized individuals from viewing company information
- Follow all security policies applicable to on-site employees

---

9. Incident Reporting

Employees must immediately report:

- Lost or stolen devices
- Suspected data breaches
- Phishing attempts or suspicious emails
- Unauthorized access or unusual system behavior

Timely reporting helps reduce potential damage and security risks.

---

10. Monitoring and Compliance

- The organization reserves the right to monitor system usage to ensure compliance.
- Monitoring will be conducted in accordance with applicable laws and regulations.
- Failure to comply with this policy may result in disciplinary action.

---

11. Policy Violations and Disciplinary Action

Violations of this policy may lead to:

- Temporary or permanent suspension of system access
- Disciplinary action up to and including termination
- Legal action where applicable

---

12. Training and Awareness

- Employees are required to complete security awareness training.
- Periodic refresher training may be conducted.
- Employees are expected to stay informed about security best practices.

---

13. Policy Review and Amendments

This policy will be reviewed periodically to address evolving security risks and regulatory requirements. Management reserves the right to update this policy at any time with appropriate notice.

---

14. Acknowledgment

All employees are required to acknowledge that they have read, understood, and agreed to comply with this Information Security Policy.