IT and Data Security Policy

1. Purpose

This policy outlines the principles, rules, and responsibilities for protecting the confidentiality, integrity, and availability of the company's information technology systems and data assets. It is intended to mitigate risks related to data breaches, unauthorized access, and misuse of systems, ensuring business continuity and regulatory compliance.

2. Scope

This policy applies to all employees, contractors, consultants, vendors, and any individual with access to the company’s IT systems, including cloud platforms, network infrastructure, and data repositories.

3. Policy Overview

This document covers:

- Access control
- Password and authentication policies
- Device and endpoint security
- Data classification and handling
- Acceptable use of systems
- Email and internet usage
- Incident reporting
- Data backup and recovery
- Mobile and remote access
- Regulatory and legal compliance

4. Access Control

- Access to IT systems must be role-based and granted only upon approval by relevant managers or IT administrators.
- All users must have unique user IDs and passwords.
- Admin privileges are limited to designated IT staff and must be logged and monitored.
- Access is revoked immediately upon employee separation or role change.

5. Password and Authentication Policy

- Passwords must be strong (minimum 8 characters, mix of upper/lower case, numbers, symbols).
- Passwords must be changed every 90 days.
- Multi-factor authentication (MFA) is mandatory for all critical systems and remote access.
- Sharing passwords is strictly prohibited.

6. Device and Endpoint Security

- All company devices must have updated antivirus and firewall software.
- Devices must be locked when unattended.
- Unauthorized software installation is prohibited.
- Personal devices used for work must be registered and comply with the Bring Your Own Device (BYOD) policy.

7. Data Classification and Handling

- **Confidential**: Sensitive company or personal data (e.g., employee records, customer data). Must be encrypted and shared only with authorized personnel.
- **Internal Use**: Company operational documents. Restricted to employees.
- **Public**: Marketing materials and public announcements. No restrictions.

Data Handling Guidelines:

- Confidential data must never be stored on unsecured devices.
- Data must be encrypted during transmission and storage.
- Printed confidential documents must be disposed of via secure shredding.

8. Acceptable Use Policy

- IT systems should only be used for legitimate business purposes.
- Prohibited activities include:
  - Accessing or distributing offensive content
  - Downloading pirated software or media

    - Using company resources for personal profit or illegal activities
- Regular audits may be conducted to ensure compliance.

9. Email and Internet Usage

- Company-provided email accounts must be used for official communication only.
- Phishing emails must be reported immediately to IT or security teams.
- Employees should not click on suspicious links or download attachments from unknown senders.
- Social media usage must align with the company's public image and policy.

10. Incident Reporting

- All actual or suspected security breaches must be reported immediately to the IT Security team.
- Examples include:
    - Lost or stolen devices
    - Suspicious emails or software behavior
    - Unauthorized access or data leaks
- The IT team will initiate an incident response process to investigate and contain threats.

11. Data Backup and Recovery

- Data backups are performed daily and stored securely offsite or on cloud platforms.
- Backup integrity is verified regularly.
- Recovery procedures are tested semi-annually to ensure preparedness in the event of system failure or data loss.

12. Mobile Device and Remote Access

- Remote access must occur via secure VPNs.
- Mobile device access must be secured with passcodes, encryption, and remote wipe capabilities.
- Employees must avoid using public Wi-Fi for work without a VPN.

13. Software and Patch Management

- Only authorized software approved by IT may be installed.
- Regular patches and updates must be applied to all operating systems and software.
- Vulnerability scans are conducted periodically to detect and mitigate threats.

14. Regulatory Compliance

This policy supports compliance with applicable laws and regulations, including:

- **GDPR** – For protection of EU resident data.
- **ISO/IEC 27001** – Information security management.
- **IT Act, 2000** (India) – For cyber law compliance.
- **HIPAA**, **SOC 2**, or other domain-specific standards, if applicable.

15. Training and Awareness

- All employees must undergo annual security awareness training.
- IT will conduct periodic phishing simulations and risk assessment workshops.
- Departmental heads are responsible for ensuring team compliance with this policy.

16. Policy Violations and Consequences

- Violations may lead to disciplinary actions, including termination of access rights, suspension, or legal action.
- Severe violations, such as data theft or intentional sabotage, may result in termination or prosecution.

17. Policy Review

- The IT and Data Security Policy is reviewed annually or as required based on new threats, technologies, or regulatory updates.
- Employees will be notified of any material changes and may be required to acknowledge new policies.
