CORPORATE POLICIES

Data Protection & Technology

CONFIDENTIAL - INTERNAL USE ONLY

TABLE OF CONTENTS

1. INTRODUCTION AND SCOPE

This document establishes the comprehensive framework for data protection and technology usage within our organization. These policies are designed to safeguard sensitive information, ensure regulatory compliance, and maintain the integrity of our technological infrastructure.

All employees, contractors, consultants, temporary workers, and other personnel with access to company systems and data are required to comply with these policies. Non-compliance may result in disciplinary action, up to and including termination of employment or contractual relationship.

1.1 Policy Objectives

- Protect confidential business information and personal data from unauthorized access, disclosure,alteration, or destruction.
- Ensure compliance with applicable data protection laws and regulations, including GDPR, CCPA, andindustry-specific requirements.
- Establish clear guidelines for the responsible use of technology resources.
- Define roles and responsibilities for data protection and information security.
- Provide a framework for incident response and business continuity.

2. DATA PROTECTION POLICY

The organization is committed to protecting personal data in accordance with applicable privacy laws and ethical standards. This policy applies to all personal data collected, processed, stored, or transmitted by the organization.

2.1 Data Protection Principles

All data processing activities must adhere to the following principles:

- **Lawfulness, Fairness, and Transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose Limitation:** Data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimization:** Personal data collected shall be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure inaccurate data is erased or rectified without delay.
- **Storage Limitation:** Personal data shall be kept in a form that permits identification of data subjects for no longer than necessary.
- **Integrity and Confidentiality:** Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing.

2.2 Data Subject Rights

The organization recognizes and upholds the rights of data subjects. All requests from data subjects exercising their rights must be forwarded to the Data Protection Officer within 24 hours of receipt. Data subjects have the

right to access their personal data, request rectification of inaccurate data, request erasure of data under certain circumstances, restrict processing, data portability, and object to processing.

2.3 Consent Management

Where consent is the legal basis for processing, such consent must be freely given, specific, informed, and unambiguous. Records of consent must be maintained and made available upon request. Data subjects must be able to withdraw consent at any time through a process that is as easy as giving consent.

3. INFORMATION SECURITY POLICY

Information security is essential to protecting company assets, maintaining stakeholder trust, and ensuring business continuity. This policy establishes the security controls and measures required to protect information assets.

3.1 Security Controls

- All systems must implement multi-factor authentication (MFA) for user access.
- Encryption must be applied to all data at rest and in transit using industry-standard algorithms (AES-256minimum for data at rest, TLS 1.2+ for data in transit).
- Systems must be configured according to security hardening guidelines and regularly audited forcompliance.
- All security events must be logged and retained for a minimum of 12 months.
- Vulnerability assessments must be conducted quarterly, and penetration testing annually.

3.2 Password Requirements

Passwords must be a minimum of 14 characters in length and contain a combination of uppercase letters, lowercase letters, numbers, and special characters. Passwords must be changed every 90 days and cannot be reused within 12 password cycles. Password sharing is strictly prohibited.

4. ACCEPTABLE USE OF TECHNOLOGY

This section defines the acceptable use of company technology resources, including but not limited to computers, networks, software, email systems, and mobile devices.

4.1 General Guidelines

- Technology resources are provided primarily for business purposes. Limited personal use is permittedprovided it does not interfere with work responsibilities or violate any company policies.
- Users must not attempt to bypass security controls or access systems, files, or data they are notauthorized to use.
- Installation of unauthorized software is prohibited. All software must be approved by the IT department.
- Users must not use company resources for illegal activities, harassment, or distribution of offensivecontent.

4.2 Email and Communication

Company email systems are to be used primarily for business communications. Users should be aware that email communications may be monitored and are subject to legal discovery. Confidential information should only be transmitted via encrypted channels. Users must exercise caution when opening attachments or clicking links in emails to prevent malware infections and phishing attacks.

4.3 Internet Usage

Internet access is provided for business purposes. Streaming media services, social media, and other bandwidth-intensive applications should be used sparingly during business hours. Accessing or downloading inappropriate, illegal, or malicious content is strictly prohibited. The organization reserves the right to monitor and log internet activity.

5. DATA CLASSIFICATION AND HANDLING

All information assets must be classified according to their sensitivity and criticality. Data classification determines the security controls required for protection.

5.1 Classification Levels

Level	Description	Examples
Public	Information intended for public release	Marketing materials, press releases
Internal	General business information	Internal memos, procedures
Confidential	Sensitive business information	Financial data, contracts
Restricted	Highly sensitive data requiring maximum pr	otectionPersonal data, trade secrets

5.2 Handling Requirements

Confidential and Restricted data must be encrypted when stored or transmitted. Access to such data must be limited to personnel with a legitimate business need. Physical documents containing sensitive information must be stored in locked containers when not in use and shredded when no longer needed.

6. ACCESS CONTROL POLICY

Access to information systems and data must be controlled to ensure only authorized personnel can access resources necessary for their job functions.

6.1 Principle of Least Privilege

Users shall be granted the minimum level of access required to perform their job functions. Access rights must be reviewed quarterly and revoked immediately upon termination of employment or change in job responsibilities. Privileged accounts must be used only for administrative tasks and never for routine activities.

6.2 Account Management

- User accounts must be uniquely identifiable and not shared between individuals.
- Service accounts must be documented and have designated owners responsible for their security.
- Accounts inactive for more than 60 days shall be automatically disabled.
- Emergency access procedures must be documented and tested annually.

7. NETWORK SECURITY POLICY

The organization's network infrastructure must be protected from unauthorized access, misuse, and malicious activity.

7.1 Network Architecture

- Networks must be segmented based on security requirements and business function.
- Firewalls must be deployed at all network boundaries with explicit deny-all policies.
- Intrusion detection and prevention systems must be implemented to monitor network traffic.
- Wireless networks must use WPA3 encryption and require authentication.

7.2 Remote Access

Remote access to the corporate network must be established through approved VPN solutions with multi-factor authentication. Split tunneling is prohibited on corporate-managed devices. All remote access sessions must be logged and monitored.

8. INCIDENT RESPONSE PROCEDURES

Security incidents must be reported immediately and handled according to established procedures to minimize impact and ensure proper documentation.

8.1 Incident Reporting

All personnel must report suspected security incidents immediately to the IT Security team via the designated reporting channels. Incidents include but are not limited to: unauthorized access attempts, malware infections, data breaches, lost or stolen devices, and suspicious activities.

8.2 Response Process

- **Identification:** Confirm the incident and assess initial scope and severity.
- **Containment:** Implement measures to prevent further damage or data loss.
- **Eradication:** Remove the threat and restore affected systems to a secure state.
- **Recovery:** Return systems to normal operation with enhanced monitoring.
- **Lessons Learned:** Document findings and implement improvements to prevent recurrence.

8.3 Data Breach Notification

In the event of a data breach involving personal data, the Data Protection Officer must be notified immediately. Regulatory authorities must be notified within 72 hours where required by law. Affected data subjects must be notified without undue delay when the breach is likely to result in high risk to their rights and freedoms.

9. DATA RETENTION AND DISPOSAL

Data must be retained only for as long as necessary to fulfill the purpose for which it was collected or as required by law. Proper disposal procedures must be followed to ensure data cannot be recovered.

9.1 Retention Periods

Retention periods are determined based on legal requirements, business needs, and data classification. The Records Management team maintains the official retention schedule. Data owners are responsible for ensuring data is disposed of according to the schedule.

9.2 Secure Disposal

- Electronic media must be sanitized using approved methods (degaussing, overwriting, or physicaldestruction) before disposal.
- Paper documents containing confidential information must be cross-cut shredded.
- Certificates of destruction must be obtained for all media containing Confidential or Restricted data.

10. REMOTE WORK SECURITY

Employees working remotely must maintain the same level of security as when working on company premises.

10.1 Device Security

- Only company-approved devices may be used to access company systems and data.
- Full disk encryption must be enabled on all devices used for remote work.
- Automatic screen lock must be configured to activate after 5 minutes of inactivity.
- Anti-malware software must be installed and kept up to date.

10.2 Physical Security

Remote workers must ensure their workspace provides adequate privacy and security. Confidential documents must not be left unattended. Video calls involving sensitive information should be conducted in private areas where the screen and conversation cannot be observed or overheard.