COMPANY: TechSolutions Inc.
POLICY TITLE: Data Security and Incident Response Policy
POLICY ID: TS-DSP-001
VERSION: 2.1
EFFECTIVE DATE: September 1, 2024
REVIEW DATE: September 1, 2025

Section 1.0 - Purpose and Scope

This policy establishes the framework for protecting TechSolutions Inc.'s information assets from unauthorized access, use, disclosure, disruption, modification, or destruction. It applies to all employees, contractors, and third parties with access to company data or systems.

Section 2.0 - Data Classification and Handling

2.1 Confidential Data: All data categorized as 'Confidential' (e.g., customer PII, financial records, proprietary source code) must be encrypted both in transit and at rest. Access to confidential data is strictly on a need-to-know basis.

2.2 Public Data: Information classified as 'Public' (e.g., marketing materials, public website content) may be freely distributed but must adhere to company branding guidelines.

Section 3.0 - Access Control

3.1 Principle of Least Privilege: Access to systems and data shall be granted based on the principle of least privilege, meaning users are given only the minimum access necessary to perform their job functions. Access rights are reviewed quarterly.

3.2 Password Policy: All system passwords must be at least 12 characters long, include a mix of uppercase, lowercase, numbers, and symbols, and be changed every 90 days. Multi-factor authentication (MFA) is mandatory for all remote access.

Section 4.0 - Incident Response Procedures

4.1 Incident Identification: Any suspected security incident (e.g., data breach, malware infection, unauthorized access) must be reported immediately to the IT Security team via helpdesk@techsolutions.com or internal extension 555.

4.2 Notification Requirements: In the event of a confirmed data breach involving personal data, affected individuals and relevant regulatory authorities (e.g., GDPR supervisory authority within 72 hours, CCPA within 30 days) shall be notified without undue delay, as legally required.

Section 5.0 - Compliance and Audit

5.1 Regular Audits: Internal and external security audits shall be conducted annually to assess compliance with this policy and relevant industry standards. Audit findings are to be reported to the Board of Directors.

5.2 Training: All employees must complete mandatory data security and privacy training upon hiring and annually thereafter. Non-compliance with training requirements may result in disciplinary action.

--- End of Policy ---