Document 2: Information Security Policy

Title: Information Security and Data Protection Policy

Department: Company-Wide

Effective Date: January 1, 2024

Document ID: ISP-2024-002

1. Policy Statement

TechInnovate Solutions is committed to protecting information assets from unauthorized access, disclosure, modification, or destruction. This policy applies to all employees, contractors, and third parties accessing company information.

2. Information Classification

2.1 Classification Levels

Public (Green Label)

Information approved for public release

Examples: Marketing materials, job postings, press releases

Storage: Public websites, shared drives

Internal Use Only (Yellow Label)

Business information for employees only

Examples: Internal memos, meeting minutes, policies

Storage: Internal servers, access-controlled

Confidential (Orange Label)

Sensitive business information

Examples: Financial data, business plans, client lists

Storage: Encrypted, access logging required

Restricted (Red Label)

Highly sensitive information

Examples: Passwords, encryption keys, trade secrets

Storage: Air-gapped systems, multi-factor authentication

3. Access Control Policy

3.1 User Access Management

Principle of least privilege

Role-based access control (RBAC)

Regular access reviews quarterly

Immediate revocation upon termination

3.2 Authentication Requirements

Minimum password length: 12 characters

Multi-factor authentication for critical systems

Password rotation every 90 days

No password sharing or reuse

3.3 Remote Access

VPN required for external access

Company-managed devices only

Session timeout: 15 minutes inactivity

Log all remote access attempts

4. Data Protection Measures

4.1 Encryption Standards

Data at rest: AES-256 encryption

Data in transit: TLS 1.2 or higher

Email encryption for sensitive information

Full disk encryption on all mobile devices

4.2 Data Loss Prevention (DLP)

Monitor data transfers

Block unauthorized external transfers

Encrypt removable media

Log all file transfers

4.3 Backup and Recovery

Daily incremental backups

Weekly full backups

Off-site storage for critical data

Test restoration quarterly

5. Network Security

5.1 Network Segmentation

Separate network zones: DMZ, internal, management

Firewall between all zones

Intrusion Detection System (IDS) monitoring

Regular vulnerability scans

5.2 Wireless Security

WPA3 encryption for Wi-Fi

Separate guest network

MAC address filtering for IoT devices

Regular access point audits

5.3 Email Security

Spam and phishing filters

Attachment scanning

URL rewriting for suspicious links

Email archiving for 7 years

6. Device Security

6.1 Endpoint Protection

Anti-virus on all devices

Regular security updates

Device encryption mandatory

Remote wipe capability

6.2 Mobile Device Management

Company-owned devices preferred

Containerization for BYOD

Application whitelisting

GPS tracking for company devices

6.3 Removable Media

Encrypted USB drives only

Approval required for external media

Scan all external media for malware

Log all media usage

7. Application Security

7.1 Secure Development

Security requirements in SDLC

Code reviews for security vulnerabilities

Regular penetration testing

Vulnerability management program

7.2 Third-Party Software

Security assessment before procurement

Regular patch management

Monitor for vulnerabilities

Vendor security certifications

8. Incident Response

8.1 Incident Classification

Level 1 (Critical): Data breach, system compromise

Level 2 (High): Malware infection, unauthorized access

Level 3 (Medium): Policy violation, suspicious activity

Level 4 (Low): Security alerts, minor issues

8.2 Response Procedures

Contain: Isolate affected systems

Assess: Determine scope and impact

Notify: Contact Security team immediately

Eradicate: Remove threat

Recover: Restore systems

Review: Post-incident analysis

8.3 Reporting Timeline

Critical incidents: Report within 15 minutes

High incidents: Report within 1 hour

Medium incidents: Report within 4 hours

All incidents: Document in ticketing system

9. Physical Security

9.1 Office Access

Badge access for all entry points

Visitor escort required

After-hours access logging

Regular access right reviews

9.2 Data Center Security

Biometric access control

24/7 surveillance

Environmental monitoring

Fire suppression systems

10. Training and Awareness

10.1 Mandatory Training

New hire security orientation

Annual security awareness training

Phishing simulation exercises

Social engineering awareness

10.2 Role-Specific Training

Developers: Secure coding practices

Administrators: System hardening

Management: Security governance

All employees: Data handling

11. Compliance and Monitoring

11.1 Regular Audits

Internal security audits quarterly

External penetration testing annually

Compliance audits for regulations

Third-party security assessments

11.2 Monitoring Activities

24/7 Security Operations Center (SOC)

Log aggregation and analysis

User behavior analytics

Threat intelligence feeds

12. Policy Enforcement

12.1 Violation Consequences

Unauthorized access: Immediate termination

Data mishandling: Disciplinary action

Policy violation: Training or warning

Repeated violations: Escalation to termination

12.2 Exception Process

Submit written exception request

Risk assessment required

Management approval

Time-bound exceptions only

13. Policy Review

This policy will be reviewed:

Annually for updates

After security incidents

When regulations change

With new technology adoption