IT Policies Directory

Information Security & Governance Policies

1. Information Security Policy

Description: Establishes comprehensive framework for protecting organizational information assets, defining security principles, roles, responsibilities, and governance structure.

2. IT Governance Policy

Description: Defines IT decision-making processes, strategic alignment procedures, and oversight mechanisms to ensure technology investments support business objectives.

3. Risk Management Policy

Description: Establishes procedures for identifying, assessing, and mitigating IT-related risks including cybersecurity threats, system failures, and data breaches.

4. Compliance and Regulatory Policy

Description: Ensures adherence to applicable laws, regulations, and industry standards including GDPR, HIPAA, SOX, and other relevant compliance requirements.

5. IT Audit and Assessment Policy

Description: Defines internal and external audit procedures, vulnerability assessments, and compliance monitoring to ensure security controls effectiveness.

Access Control & Identity Management Policies

6. User Access Management Policy

Description: Establishes procedures for user account creation, modification, and termination, including role-based access controls and principle of least privilege.

7. Password and Authentication Policy

Description: Defines password complexity requirements, multi-factor authentication standards, and account lockout procedures to protect against unauthorized access.

8. Privileged Access Management Policy

Description: Controls administrative and privileged account access through enhanced security measures, monitoring, and approval processes for high-risk operations.

9. Remote Access Policy

Description: Establishes secure connection requirements, VPN usage guidelines, and security controls for employees accessing systems from outside the office.

10. Third-Party Access Policy

Description: Defines security requirements and approval processes for vendors, contractors, and partners accessing organizational systems and data.

Data Management & Protection Policies

11. Data Classification and Handling Policy

Description: Establishes data classification levels, handling requirements, and protection measures based on sensitivity and business impact of information assets.

12. Data Privacy and Protection Policy

Description: Ensures compliance with privacy regulations through proper data collection, processing, storage, and deletion procedures for personal information.

13. Data Backup and Recovery Policy

Description: Defines backup schedules, retention periods, recovery procedures, and testing requirements to ensure business continuity and data availability.

14. Data Retention and Disposal Policy

Description: Establishes retention schedules and secure disposal procedures for different data types to ensure compliance and minimize storage costs.

15. Database Security Policy

Description: Defines security controls for database systems including access controls, encryption, monitoring, and maintenance procedures to protect critical data.

Network & Infrastructure Security Policies

16. Network Security Policy

Description: Establishes network architecture standards, firewall configurations, intrusion detection systems, and network monitoring procedures to protect against threats.

17. Wireless Network Security Policy

Description: Defines security requirements for wireless networks including encryption standards, access controls, and monitoring procedures for Wi-Fi and mobile connections.

18. Server and Infrastructure Security Policy

Description: Establishes security controls for physical and virtual servers including hardening standards, patch management, and monitoring requirements.

19. Cloud Security Policy

Description: Defines security requirements for cloud services including vendor assessment, data protection, access controls, and compliance monitoring.

20. Network Monitoring and Incident Response Policy

Description: Establishes procedures for continuous network monitoring, threat detection, and incident response to quickly identify and mitigate security threats.

Application & Software Management Policies

21. Software Development Security Policy

Description: Defines secure coding practices, code review procedures, and testing requirements to ensure applications are developed with security built-in.

22. Software Asset Management Policy

Description: Establishes procedures for software licensing, inventory management, and compliance monitoring to prevent legal and security risks.

23. Application Security Policy

Description: Defines security requirements for web applications, mobile apps, and custom software including authentication, authorization, and data validation.

24. Software Installation and Updates Policy

Description: Controls software installation, patch management, and update procedures to maintain system security and prevent unauthorized software.

25. API Security Policy

Description: Establishes security controls for application programming interfaces including authentication, rate limiting, and data validation to protect against API attacks.

Device & Endpoint Management Policies

26. Device Management Policy

Description: Defines security requirements for corporate devices including laptops, desktops, mobile devices, and IoT equipment throughout their lifecycle.

27. Mobile Device Management (MDM) Policy

Description: Establishes controls for corporate and personal mobile devices accessing company resources including encryption, remote wipe, and application management.

28. Bring Your Own Device (BYOD) Policy

Description: Defines security requirements and acceptable use guidelines for personal devices used for business purposes including data protection measures.

29. USB and Removable Media Policy

Description: Controls the use of USB drives, external storage devices, and removable media to prevent data theft and malware introduction.

30. Asset Management Policy

Description: Establishes procedures for tracking, maintaining, and disposing of IT assets including hardware inventory, maintenance schedules, and secure disposal.

Communication & Internet Usage Policies

31. Email and Communication Security Policy

Description: Defines secure email practices, encryption requirements, and guidelines for protecting sensitive information in electronic communications.

32. Internet and Web Usage Policy

Description: Establishes acceptable use guidelines for internet access, web browsing, and online activities to maintain productivity and security.

33. Social Media Policy

Description: Defines guidelines for social media use in business context including brand protection, confidentiality, and professional conduct requirements.

34. Video Conferencing and Collaboration Policy

Description: Establishes security requirements for video meetings, file sharing, and collaboration tools to protect confidential information.

Business Continuity & Disaster Recovery Policies

35. Business Continuity Policy

Description: Defines procedures for maintaining critical business operations during disruptions including alternative work arrangements and resource allocation.

36. Disaster Recovery Policy

Description: Establishes procedures for recovering IT systems and data following disasters including recovery time objectives and testing requirements.

37. Incident Response Policy

Description: Defines procedures for detecting, responding to, and recovering from security incidents including notification requirements and containment measures.

38. Change Management Policy

Description: Establishes controlled procedures for implementing system changes including testing, approval, and rollback procedures to minimize disruption.

Vendor & Third-Party Management Policies

39. Vendor Risk Management Policy

Description: Defines procedures for assessing and managing security risks associated with third-party vendors and service providers.

40. Contract and SLA Management Policy

Description: Establishes requirements for IT contracts including service level agreements, security clauses, and vendor performance monitoring.

41. Outsourcing Security Policy

Description: Defines security requirements and oversight procedures for outsourced IT services to ensure consistent security standards.

Training & Awareness Policies

42. Security Awareness Training Policy

Description: Establishes mandatory security training programs for all employees including phishing awareness, data protection, and incident reporting.

43. IT Training and Certification Policy

Description: Defines training requirements and certification standards for IT staff to maintain technical competency and security knowledge.

Implementation Guidelines

Policy Development Process

Each policy should be developed with input from security professionals, reviewed by IT management, and approved by executive leadership before implementation.

Policy Review Schedule

All policies should be reviewed annually or when technology changes, security threats evolve, or regulations are updated. Changes must be communicated within 30 days.

Training and Awareness

New employees must complete IT security training during onboarding. Annual refresher training should be conducted for all staff with completion tracking.

Compliance Monitoring

Regular security assessments and audits should be conducted to ensure policy compliance. Violations should be addressed through established disciplinary procedures.

Metrics and Reporting

Key performance indicators should be established to measure policy effectiveness including incident rates, compliance scores, and training completion rates.

This directory provides a comprehensive framework for organizational IT policies. Each policy should be developed in detail with specific procedures, technical standards, and compliance requirements appropriate to your organization's technology environment and risk profile.