HITRUST Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

ABC Company has strong relationships with our health care customers, service providers, and regulators. Managing compliance requirements helps us maximize our opportunities in the market, enhances our competitive position, and helps build trust.

# II. Purpose

Security controls and safeguards are part of ABC Company’s risk management process to mitigate, eliminate, and transfer risks that can impact business operations. A strong health care compliance program provides our organization with a competitive advantage, helps protect our image and reputation, and reduces our costs.

# III. Scope

This policy applies to all ABC Company Staff who have access to or manage Information Resources that collect, transmit, process, or store health care related data.

# IV. Policy

HITRUST’s Common Security Framework (CSF) helps organizations create, access, store, and exchange Protected Health Information (PHI) in a safe and secure manner. The CSF is based on health care security regulations, standards, and frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and International Standards Organization (ISO) 27799:2008 Health informatics, information security management in health using ISO/IEC 27002.

CSF consolidates relevant globally recognized standards, regulations, and business requirements into a risk-based approach to security, privacy, and regulatory challenges. CSF includes Control Categories which contain Control Objectives and Control Specifications.

The table below summarizes ABC Company policies and plans that implement and maintain specific Safeguards to help meet HITRUST compliance requirements.

|  |  |
| --- | --- |
| **Control Category** | **Policy/Plan/Procedure** |
| Information Security Management Program | Context and Alignment Policy  Cybersecurity Framework Policy Cybersecurity Policy  Information Security Policy  Mergers and Acquisitions Policy  Standard Operating Procedure Policy  System Security Plan  Terms and Definitions Policy |
| Access Control | Access Control Policy  Access Control Procedure  Admin Special Access Policy  Bring Your Own Device Policy and Technology  Clear Desk Policy  Database Security Policy  Guest Access Policy  Identification and Authentication Policy  Logical Access Controls Policy  Mobile Device Policy  Password Policy  Portable Computing Policy  Remote Access Policy  Securing Information Systems Policy  Securing Sensitive Information Policy  Smartphone Policy  System Update Policy  User Privilege Policy  Wearable Computing Device Policy  Web Policy  Wireless Access Policy |
| Human Resources Security | Health Safety Policy  Outsourcing Policy  Security Awareness and Training Plan  Security Awareness and Training Policy  Staffing Policy  Social Networking Policy  Third Party Service Providers Policy |
| Risk Management | Business Impact Analysis  Cybersecurity Policy  Cybersecurity Framework Policy  Risk Assessment Policy  Risk Management Policy |
| Security Policy | Security Policy |
| Organization of Information Security | Audit Policy  Cloud Service Provider Policy  IT Governance Policy  IT Management Policy  Security Self Assessment Policy |
| Compliance | Business Associates Agreement  Certification and Accreditation Policy  Compliance Policy  Data Retention Policy  Ethics Policy  HIPAA and HITECH Policy  HITRUST Policy  PCI Policy  Security Controls Review Policy  Software Licensing Policy  System Organization Controls SOC2 Policy  Vulnerability and Penetration Testing Policy |
| Asset Management | Acceptable Use Policy  Asset Management Policy  Data Classification Policy |
| Physical and Environmental Security | Facility Security Plan  Personnel Security Policy  Physical Access Policy  Physical Security Policy |
| Communications and Operations Management | Account Management Policy  Anti-Malware Policy  Backup Plan  Backup Policy  Bluetooth Policy  Capacity and Utilization Policy  Configuration and Management Plan  Configuration Management Policy  Data Analytics Policy  Data Integrity Policy  Data Marking Policy  Disposal Policy  Documentation Policy  Domain Controller Policy  Domain Name System Policy  E-commerce Policy  E-mail Policy  Firewall Policy  Guess Access Policy  Internet Connection Policy  Intrusion Detection Policy  Logging Policy  Mass Communication Policy  Network Address Policy  Network Configuration Policy  Network Documentation Policy  Network Security Policy  Problem Management Policy  Removable Media Policy  Router Security Policy  Security Monitoring Policy  Server Hardening Policy  Vendor Access Policy  Workstation Hardening Policy  Workstation Security Policy |
| Information Systems Acquisition, Development and Maintenance | Acquisition and Procurement Policy  Application Implementation Policy  Approved Application Policy  Audit Trails Policy  Change Management Policy  Encryption Policy  Green Computing Policy  Hardware and Software Maintenance Policy  Patch Management Policy  Production Input Output Controls Policy  Secure Software Development Lifecycle Policy  Server Certificates Policy  Software Development Policy  VPN Policy  Web Site Policy |
| Information Security Incident Management | Identity Theft Protection Policy  Incident Response Policy  Incident Response Plan  Reporting Violations Policy |
| Business Continuity Management | Business Continuity Plan  Business Continuity Policy  Business Resumption Plan  Continuity Communications Plan  Department Continuity of Operations Plan  IS Disaster Recovery Plan  Resilience Policy |
| Privacy Practices | Data Privacy Policy  GDPR EU Privacy and Data Protection Policy  Privacy Policy  Quality Assurance Policy  Web Site Privacy Policy |

Note: Policy/Plan names listed above may provide guidance and direction over more than one control category.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff who have access to or manage Information Resources that collect, transmit, process, or store health care related data.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.03, APO09.05, APO12.02, APO13.07, DSS04.05, MEA03.01, MEA04.11

GDPR Article 25, 32

HIPAA 164.308, 164.310, 164.312, 164.314, 164.316, 164.502, ARRA 13402, 13404, 13405

ISO 27001:2013 6.1.2, A5, A7.2.2, A8.1.3, A8.2.1, A9-14, A16-18

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29

NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2

PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8, PCI Software Security Framework