#	Policy	Description
1	**INFORMATION PROTECTION PROGRAM** 1.0.3.1 Information Security Management Program 1.0.3.2 Information Security Policy Document 1.0.3.3 Review of the Information Security Policies 1.0.3.4 Roles and Responsibilities 1.0.3.5 Screening 1.0.3.6 Terms and Conditions of Employment 1.0.3.7 Management Responsibilities 1.0.3.8 Disciplinary Process 1.0.3.9 Management Commitment to Information Security 1.0.3.10 Information Security Coordination 1.0.3.11 Allocation of Information Security Responsibilities 1.0.3.12 Independent Review of Information Security 1.0.3.13 Identification of Applicable Legislation 1.0.3.14 Ownership of Assets 1.0.3.15 Documented Operations Procedures	Provides a framework for management direction and support for information security to protect all covered information for all business activities according to business requirements, relevant laws, and federal and state regulations.
2	**ENDPOINT PROTECTION** 2.0.3.1 Unattended User Equipment 2.0.3.2 Controls Against Malicious Code 2.0.3.3 Controls Against Mobile Code 2.0.3.4 Network Controls	Ensures the organization complies with the regulations that govern safe usage and storage of PII. The organization commits to protect the confidentiality, integrity, and availability of covered information in a secure manner in compliance with these laws and regulations.
3	**PORTABLE MEDIA SECURITY** 3.0.3.1 Management of Removable Media 3.0.3.2 Information Labeling and Handling 3.0.3.3 Information Handling Procedure 3.0.3.4 Physical Media in Transit	Ensures the organization complies with laws and regulations governing the use of portable media. The policy outlines the organization's process to protect corporate information that may be accessed and/or, stored on, or transmitted from, such portable/removable data storage devices according to the guidelines.
4	**MOBILE DEVICE SECURITY** 4.0.3.1 Mobile Computing and Communications 4.0.3.2 Teleworking	Ensures the organization complies with regulations regarding safe usage and storage of PII that may be on a mobile device. The policy outlines the process for the organization to protect corporate information that may be accessed and/or, stored on individual-liable and corporate-liable devices.

#	Policy	Description
5	**WIRELESS SECURITY** 5.0.3.1 Network Controls	Defines the essential rules regarding the management and maintenance of switches, routers and firewalls at the organization.
6	**CONFIGURATION MANAGEMENT** 6.0.3.1 Compliance with Security Policies and Standards 6.0.3.2 Technical Compliance Checking 6.0.3.3 Change Management 6.0.3.4 Separation of Development, Test, and Operational Environments 6.0.3.5 Control of Internal Processing 6.0.3.6 Control of Operational Software 6.0.3.7 Access Control to Program Source Code 6.0.3.8 Change Control Procedures	Demonstrates the organization's commitment to respect all computer software copyrights and to adhere to the terms of all software licenses.
7	**VULNERABILITY MANAGEMENT** 7.0.3.1 Inventory of Assets 7.0.3.2 Security of System Documentation 7.0.3.3 Input Data Validation 7.0.3.4 Control of Technical Vulnerabilities	Establishes the organization's commitment to an information security risk management process in compliance with applicable laws and regulations regarding safe usage and storage of PII on a device.
8	**NETWORK PROTECTION** 8.0.3.1 Policy on the Use of Network Services 8.0.3.2 User Authentication for External Connections 8.0.3.3 Segregation in Networks 8.0.3.4 Network Connection Control 8.0.3.5 Network Routing Control 8.0.3.6 Sensitive System Isolation 8.0.3.7 Network Controls 8.0.3.8 Security of Network Services 8.0.3.9 Input Data Validation	Protects the confidentiality, integrity, and availability of organization's covered information in compliance with applicable laws and regulations. The policy reflects the organization's commitment to establishing appropriate controls that protect its systems, network, and networking devices from security threats.
9	**TRANSMISSION PROTECTION** 9.0.3.1 Network Controls 9.0.3.2 Information Exchange Policies and Procedures 9.0.3.3 Electronic Messaging 9.0.3.4 Interconnected Business Information Systems 9.0.3.5 Electronic Commerce Services 9.0.3.6 Online Transactions 9.0.3.7 Message Integrity 9.0.3.8 Policy on the Use of Cryptographic Controls	Demonstrates organization's commitment to protecting the confidentiality, integrity, and availability of covered information in compliance with laws and regulations regarding data in transit. The organization also addresses the requirements for electronic signatures and e-commerce.

#	Policy	Description
	9.0.3.9 Key Management	
10	**PASSWORD MANAGEMENT** 10.0.3.1 User Password Management 10.0.3.2 Password Use 10.0.3.3 Password Management System	Outlines a process for the organization to possess secure passwords and user IDs in compliance with applicable laws and regulations.
11	**ACCESS CONTROL** 11.0.3.1 Access Control Policy 11.0.3.2 User Registration 11.0.3.3 Privilege Management 11.0.3.4 Review of User Access Rights 11.0.3.5 Clear Desk and Clear Screen Policy 11.0.3.6 User Authentication for External Connections 11.0.3.7 Equipment Identification in Networks 11.0.3.8 Remote Diagnostic and Configuration Port Protection 11.0.3.9 Secure Log-on Procedures 11.0.3.10 User Identification and Authentication 11.0.3.11 Use of System Utilities 11.0.3.12 Session Time-out 11.0.3.13 Limitation of Connection Time 11.0.3.14 Information Access Restriction 11.0.3.15 Termination or Change Responsibilities 11.0.3.16 Return of Assets 11.0.3.17 Removal of Access Rights 11.0.3.18 Prevention of Misuse of Information Assets 11.0.3.19 Monitoring System Use	Demonstrates the organization's commitment to HITRUST guidelines and other applicable laws and regulations that protect covered information.
12	**AUDIT LOGGING & MONITORING** 12.0.3.1 Protection of Organizational Records 12.0.3.2 Prevention of Misuse of Information Assets 12.0.3.3 Protection of Information Systems Audit Tools 12.0.3.4 Audit Logging 12.0.3.5 Monitoring System Use 12.0.3.6 Protection of Log Information 12.0.3.7 Administrator and Operator Logs 12.0.3.8 Fault Logging 12.0.3.9 Clock Synchronization 12.0.3.10 Segregation of Duties 12.0.3.11 Electronic Commerce Services	Ensures the organization complies with applicable guidelines regarding safe usage and storage of PII by outlining a process for regularly auditing user access.

#	Policy	Description
	12.0.3.12 Required Uses and Disclosures	
13	**EDUCATION, TRAINING & AWARENESS** 13.0.3.1 Secure Log-on Procedures 13.0.3.2 Mobile Computing and Communications 13.0.3.3 Teleworking 13.0.3.4 Information Security Awareness, Education, and Training 13.0.3.5 Prevention of Misuse of Information Assets 13.0.3.6 Acceptable Use of Assets 13.0.3.7 Controls Against Malicious Code 13.0.3.8 Information Exchange Policies and Procedures 13.0.3.9 Developing and Implementing Continuity Plans Including Information Security	Outlines the organization's program to properly educate staff on matters of security and privacy awareness in compliance with applicable laws and regulations.
14	**THIRD PARTY ASSURANCE** 14.0.3.1 Identification of Risks Related to External Parties 14.0.3.2 Addressing Security When Dealing with Customers 14.0.3.3 Addressing Security in Third Party Agreements 14.0.3.4 Service Delivery 14.0.3.5 Monitoring and Review of Third-Party Services 14.0.3.6 Managing Changes to Third-Party Services 14.0.3.7 Exchange Agreements 14.0.3.8 Outsourced Software Development	Demonstrates the organization's compliance with guidelines regarding safe usage and storage of PII/sensitive information on the organization's systems and devices.
15	**INCIDENT MANAGEMENT** 15.0.3.1 Disciplinary Process 15.0.3.2 Prevention of Misuse of Information Assets 15.0.3.3 Control of Internal Processing 15.0.3.4 Reporting Information Security Events 15.0.3.5 Reporting a Security Weakness 15.0.3.6 Responsibilities and Procedures 15.0.3.7 Learning from Information Security Incidents 15.0.3.8 Collection of Evidence	Outlines the organization's commitment to protect the confidentiality, integrity, and availability of data and information systems from adverse incidents, whether intentional or accidental. The organization will develop a framework to address these incidents, maintain industry-standard security measures, and continually assess potential risks and vulnerabilities to PII/sensitive information.
16	**BUSINESS CONTINUITY & DISASTER RECOVERY POLICY**	Demonstrates the organization's commitment to protect PII/sensitive information from an

#	Policy	Description
	16.0.3.1 Capacity Management 16.0.3.2 Back-up 16.0.3.3 Including Information Security in the Business Continuity Management Process 16.0.3.4 Business Continuity and Risk Assessment 16.0.3.5 Developing and Implementing Continuity Plans Including Information Security 16.0.3.6 Business Continuity Planning Framework 16.0.3.7 Testing, Maintaining, and Re-Assessing Business Continuity Plans	unexpected event to the physical facilities or within information systems.
17	**RISK MANAGEMENT** 17.0.3.1 Risk Management Program Development 17.0.3.2 Performing Risk Assessments 17.0.3.3 Risk Mitigation 17.0.3.4 Risk Evaluation 17.0.3.5 Authorization Process for Information Assets and Facilities 17.0.3.6 Contact with Authorities 17.0.3.7 Contact with Special Interest Groups 17.0.3.8 Information Systems Audit Controls 17.0.3.9 Classification Guidelines 17.0.3.10 System Acceptance 17.0.3.11 Security Requirements Analysis and Specification 17.0.3.12 Opportunity Required	Demonstrates the organization's compliance with applicable laws and regulations.
18	**PHYSICAL & ENVIRONMENTAL SECURITY** 18.0.3.1 Physical Security Perimeter 18.0.3.2 Physical Entry Controls 18.0.3.3 Securing Offices, Rooms, and Facilities 18.0.3.4 Protecting Against External and Environmental Threats 18.0.3.5 Working in Secure Areas 18.0.3.6 Public Access, Delivery, and Loading Areas 18.0.3.7 Equipment Siting and Protection 18.0.3.8 Supporting Utilities 18.0.3.9 Cabling Security 18.0.3.10 Equipment Maintenance 18.0.3.11 Security of Equipment Off-Premises	Demonstrates the organization's commitment to compliance with applicable laws and regulations related to physical security. The organization controls access to its information systems/applications. Access to physical buildings/facilities that house these systems/applications is granted only to authorized users.

#	Policy	Description
	18.0.3.12 Secure Disposal or Re-Use of Equipment 18.0.3.13 Removal of Property 18.0.3.14 Disposal of Media	
19	**DATA PROTECTION & PRIVACY** 19.0.3.1 Privilege Management 19.0.3.2 Confidentiality Agreements 19.0.3.3 Addressing Security When Dealing with Customers 19.0.3.4 Intellectual Property Rights 19.0.3.5 Protection of Organizational Records 19.0.3.6 Data Protection and Privacy of Covered Information 19.0.3.7 Prevention of Misuse of Information Assets 19.0.3.8 Regulation of Cryptographic Controls 19.0.3.9 Information Labeling and Handling 19.0.3.10 Management of Removable Media 19.0.3.11 Publicly Available Information 19.0.3.12 Control of Internal Processing 19.0.3.13 Output Data Validation 19.0.3.14 Key Management 19.0.3.15 Protection of System Test Data 19.0.3.16 Notice of Privacy Practices 19.0.3.17 Rights to Protection and Confidentiality 19.0.3.18 Authorization Required 19.0.3.19 Opportunity Required 19.0.3.20 Authorization or Opportunity Not Required 19.0.3.21 Access to Individual Information 19.0.3.22 Accounting of Disclosures 19.0.3.23 Correction of Records 19.0.3.24 Required Uses and Disclosures 19.0.3.25 Permitted Uses and Disclosures 19.0.3.26 Prohibited or Restricted Uses and Disclosures 19.0.3.27 Minimum Necessary Use 19.0.3.28 Confidential Communications 19.0.3.29 Organizational Requirements	Establishes the organization's compliance with federal and other applicable privacy laws.