POLICY #11 – ACCESS CONTROL

11.0.1 PURPOSE

The Access Control Policy provides a structured process for granting user access to accounts, and adhering to the standards of auditors and regulatory agencies. It also outlines a process for CLIENT_NAME to properly and safely protect corporate information that may be accessed and/or stored on individual-liable and corporate-liable devices, as well as ensuring CLIENT_NAME complies with HITRUST guidelines pursuant to safe usage and storage of PHI that may be on the device. These controls may be built into the operating system, incorporated into applications program or major utilities (e.g., database management systems), or implemented through add-on security packages.

CLIENT_NAME will provide all employee, contractor or third-parties with appropriate training and relevant security and privacy policies prior to access to PHI or other sensitive data.

This policy has been implemented to safeguard the confidentiality, integrity, and availability of PHI, business, and proprietary information within CLIENT_NAME information systems/applications by controlling access to the physical buildings/facilities that house these systems/applications.

This policy also reflects CLIENT_NAME's commitment to establishing appropriate controls to protect CLIENT_NAME systems and its network from security threats associated with remote access while ensuring those properly authorized can access resources necessary for their job function.

11.0.2 SCOPE

This policy applies to all CLIENT_NAME associates, contractors, consultants, volunteers, vendors and any other individuals or entities supported by CLIENT_NAME with access to CLIENT_NAME facilities, applications, systems, networks, and/or electronic data.

11.0.3 POLICY

CLIENT_NAME is committed to maintaining an Access Control Policy that protects the organization from the loss of sensitive information and exposure to unauthorized person and to performing procedures and periodic audits to ensure that the policy is effective.

CLIENT_NAME shall document the policy “scope, roles, responsibilities and compliance” in the first section of this document and ensure they are consistent throughout this document. Acceptable use agreements shall be signed by all employees, contractors and documented in all vendor and/or Business Associate Agreements before being allowed access to information assets.

Access control rules shall account for and reflect CLIENT_NAME’s policies for information dissemination and authorization, and these rules shall be supported by formal procedures and clearly defined responsibilities. CLIENT_NAME will create a process to authenticate the customer's identity prior to granting access to covered information.

Access control rules and rights for each user, group of users, contractors, Business Associates or other 3rd parties, and applications shall be clearly stated in the RBAC Matrix. Access controls are both logical and physical and these shall be considered together. Users and service providers shall be given a clear statement of the business requirements to be met by access controls. User registration and de-registration shall formally address establishing, activating, modifying, reviewing, disabling and removing accounts. CLIENT_NAME acknowledges that Privilege Management has been a significant issue in major data breaches and will apply extra scrutiny to application and process related computer privileges, as well as applications to which third-parties have access.

Specifically, the access control program shall take account of the following:

CONFIDENTIAL

1. Security requirements of individual business applications and business units (e.g., separation/segregation either with within a hybrid entity);
2. Information dissemination and authorization such as need-to-know, need to share, and least privilege principles also known in HIPAA as ‘minimum necessary’; security levels; and classification of information.
3. Relevant legislation and any contractual obligations regarding protection of access to data or services;
4. Standard user access profiles (RBAC) for common job roles in the organization;
5. Requirements for formal authorization of access requests;
6. Requirements for emergency access;
7. Requirements for periodic review of access controls; and
8. Removal of access rights and termination of relationships.

All information related to the business applications, data classification, and the risks the information is facing shall be identified. The access control and information classification policies shall be consistent.

Access rights shall be managed using Role Bases Access Control (RBAC) in a networked environment ensuring all types of connections available are technically secure and recognized. RBAC roles shall ensure that access requests, authorizations, and administration shall employ Separation of Duty. Access rights to information assets and facilities is reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors. If necessary, physical and logical access rights are immediately removed or modified following employee, contractor or third-party user termination, and allow for immediate escorting from the site.

11.0.3.1 Business Requirement for Access Control

11.0.3.2 Network Access Controls

11.0.3.3 User Authorization Access

11.0.3.4 Application and Information Access Control

11.0.3.6 Workstation Security

11.0.3.7 Log-on Procedures

11.0.3.8 VPN, Extranet, and Remote Access

11.0.3.9 Administrative and Privileged Access to Computer Systems

Users who performed privileged functions (e.g., system administration) use separate accounts when performing those privileged functions. Non- built-in administrative accounts require renewal and auditing on an annual basis where operationally and technologically feasible. Elevated privileges are assigned to a different user ID from those used for normal business use, all users access privileged services in a single role, and such privileged access is minimized.

Annually, ePHI application system owners will produce or request a report listing administrative and privileged user accounts within the system.

1. The system owner or business owner will review the list of users who are assigned administrative access, noting for each account whether their current access is appropriate.
2. The system owner or business owner will submit a request to modify users found with inappropriate access either via a Service Desk Request or the User Account Provisioning process.

CONFIDENTIAL

3. The system owner or business owner will submit a report of the results of the review, and actions taken to the Information Security mailbox at xxx@xxx.com.
4. Information Security will perform periodic reviews of third-party, application, and process machine access to data and will submit a report of the results of the review, and actions taken to the system owner or business owner for review.
5. Information Security will maintain flow charts of applications and process related machines indicating data access solely based on Privileged Access and review quarterly or upon any change to privileges.
6. Information Security will retain these reports according to the CLIENT_NAME HIPAA Document Time Limit Retention.

11.0.3.10 Access to Program Source Code

11.0.3.11 Operating System Access Control

11.0.3.13 Internet Acceptable Use and Web Filtering

11.0.4 DEFINITIONS

Access Control List (ACL): A list of users, programs, and/or processes and the specifications of access categories to which each is assigned.

Application: An executable software program, or group of programs, that is designed to deliver some or all of a series of steps needed to create, update, manage, calculate or display information for a specific business purpose.

CLIENT_NAME-owned device: A device that is owned by the organization. In reference to VPN connectivity, a CLIENT_NAME owned device will be equipped with the proper software and configuration requirements necessary for VPN connectivity.

Availability: The ability of an authorized person to use or access objects, resources, data or information when needed, without undue delay.

B2B VPN Access: A secure, private, unshared Internet based connection used for direct network access to or from external partner. The connection is made between network devices such as a VPN concentrator, firewall or router.

Business Owner: The person or specified role responsible for the business results of that system or the business use of the information provided from a system. When appropriate, ownership may be shared by roles within CLIENT_NAME. The Business Owner shall describe and clarify business processes and terminology to help Information Services understand the business benefits of the application.

Client VPN Access: A secure Internet based connection used for network access from an endpoint computing device to a host network.

Computer Systems: Hardware and software components that operate together to process, store, manipulate, or use data or information.

Confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.

CONFIDENTIAL

Cryptographic Keys: An electronic string of characters used by a software program to convert data from a state of "not encrypted" to "encrypted" to "not encrypted".

Cryptosystem: All pieces that make up a proper encryption mechanism or system including applications, hardware, keys, key strengths, ciphers, etc.

Data at Rest: Data that is sitting on a piece of equipment (a USB key, a laptop, a desktop, a server, a cart on wheels, etc.)

Data in Transit: Data that is being sent from one destination to another through electronic means (sending information in an email, uploading information to a FTP server, transferring it from one workstation to another, etc.).

Decryption: The process of converting an encrypted data into its original "human readable form".

ePHI: All individually identifiable health information that is transmitted by or maintained in electronic media.

EMR: Electronic Medical Records.

Encrypt: To encode data so that only someone with a key can read it.

Encryption: The act of obscuring data in such a way that it is indecipherable and unreadable to anyone who does not possess the proper key to unlock the data.

ePHI Application: Any application that creates, modifies, processes or stores electronic PHI.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): Established to enforce standards for electronic health information, enhance the security and privacy of health information, curtail healthcare fraud and abuse, and assure health insurance portability for employed persons.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): HIPAA has been established to enforce standards for electronic health information, enhance the security and privacy of health information, curtail healthcare fraud and abuse, and assure health insurance portability for employed persons.

Information Security Officer (ISO): Person who is responsible for implementing, managing and maintaining the Data Security Program.

Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. (42 C.F.R Section 160.103.).

Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.

CONFIDENTIAL

Key: A piece of information which is used to turn encrypted data into non-encrypted data, or non-encrypted data into encrypted data.

Magnetic Stripe Data (Track Data): Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization.

Specifically, subsequent to authorization, service codes, discretionary data/ Card Validation Value/Code, and proprietary reserved values must be purged; however, account number, expiration data, name, and service code may be extracted and retained, if needed for business.

Minimum Necessary Information: PHI that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The “minimum necessary” standard applies to all PHI in any form.

Open Networks: Networks that provide for public access with no or limited access controls and which are isolated via firewalls and other protection methods from Networks maintained by and for the use of CLIENT_NAME.

Personal device: A computing device owned by an associate, such as a PC, laptop or mobile device. For VPN connectivity, the device must be compatible with the CLIENT_NAME VPN client or other approved Remote Access applications.

Pre-Boot: A mechanism within encryption applications which allows for an operating system to be paused before it can be loaded and require a key to unlock the operating system loading.

Primary Account Number (PAN): Payment card number (credit or debit) that identifies the issuer and the particular cardholder account; also called Account Number.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, which identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

1. Past, present or future physical or mental health or condition of an individual.
2. The provision of health care to an individual.
3. The past, present, or future payment for the provision of health care to an individual.

Public Data: Information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage.

Public Network: All systems, servers, routers and lines not owned or controlled by CLIENT_NAME that can be accessed through public access methods, including dial-up, DSL, ISDN, cable, wireless and other connection methods.

Remote Access: Any access to CLIENT_NAME's corporate network through a non-CLIENT_NAME controlled network or device.

Restricted Area: those areas of the building(s) where PHI and/or sensitive organizational information are stored accessed or utilized at any time. These areas include, but are not limited to the following examples:

1. HIM departments;

CONFIDENTIAL

2. HIM control desks;
3. Data Centers or server locations;
4. Check-in desks/stations;
5. Nursing/Patient Care stations/desks;
6. Patient Care hallways;
7. Patient Care rooms or other designated area;
8. Employee meeting rooms/kitchens located in patient care areas;
9. Mailrooms;
10. Offices;
11. Cubicles;
12. Storage closets and cabinets (including medication storage areas);
13. Information Services equipment rooms;
14. Business Office windows and offices;
15. Human Resources window and offices; and
16. Administration offices.

Role: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.

Service Code: Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction.

System Owner: The individual(s) who has been designated to carry accountability for CLIENT_NAME information system.

Unrestricted Area: Those areas of the building(s) where PHI and/or sensitive organizational information is not stored or is not utilized there on a regular basis. These areas include but are not limited to the following:

1. Lunch rooms
2. Conference rooms
3. Building parking lots
4. Building entry ways
5. Main hallways
6. Restrooms

User: shall mean and include the authorized individuals that routinely utilize CLIENT_NAME's information assets (i.e., applications, systems, networks and/or electronic data).

Vendors: persons from other organizations marketing or selling products or services, or providing services to CLIENT_NAME. Examples include, but are not limited to the following:

1. Pharmaceutical Representatives
2. Equipment and Application Repair Service Personnel
3. Food Services
4. Independent Contractor for CLIENT_NAME

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Workstation: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, personal digital assistants (PDAs), tablet PCs, and other handheld devices. For the purposes of this policy, “workstation” also includes the

CONFIDENTIAL

combination of hardware (i.e. Ethernet ports, hard drive, etc.), operating system, application software, and network connection (including remote and wireless).

11.0.5 PROCEDURES

Refer to the Procedures document for procedures specific to this policy.

11.0.6 RESPONSIBILITIES

Compliance and review are the responsibility of the designated Information Security Officer.

11.0.7 COMPLIANCE

Failure to comply with this or any other security policy will result in corrective actions as per the Sanctions Policy. Legal actions also may be taken for violations of applicable regulations and standards such as ISO 27001, PCI DSS, HIPAA, HITECH, HITRUST, and others.

11.0.8 REFERENCES

HITRUST CSF v9.1 –Access Control – Related Standards	
Standard	**Description**
HIPAA Security Rule	HIPAA § 164.308(a)(3)(i) HIPAA § 164.308(a)(3)(ii)(A) HIPAA § 164.308(a)(3)(ii)(B) HIPAA § 164.308(a)(3)(ii)(C) HIPAA § 164.308(a)(4)(i) HIPAA § 164.308(a)(4)(ii)(A) HIPAA § 164.308(a)(4)(ii)(B) HIPAA § 164.308(a)(4)(ii)(C) HIPAA § 164.308(a)(5)(ii)(C) HIPAA § 164.308(a)(5)(ii)(D) HIPAA § 164.310(a)(1) HIPAA § 164.310(a)(2)(i) HIPAA § 164.310(a)(2)(iii) HIPAA § 164.310(b) HIPAA § 164.310(c) HIPAA § 164.310(d)(1) HIPAA § 164.312(a)(1) HIPAA § 164.312(a)(2)(i) HIPAA § 164.312(a)(2)(ii) HIPAA § 164.312(a)(2)(iii) HIPAA § 164.312(a)(2)(iv) HIPAA § 164.312(b) HIPAA § 164.312(d) HIPAA § 164.312(c)(2)(e)(1)
HITRUST De-Identification Framework v1	De-ID Framework v1 Access Control: General De-ID Framework v1 Access Control: Access Policies De-ID Framework v1 Identification and Authentication (Application-level): Authentication Policy De-ID Framework v1 Identification and Authentication (System-level): Authentication Policy De-ID Framework v1 Physical Security: General De-ID Framework v1 Transmission Encryption: Policies De-ID Framework v1 Identification and Authentication: Authentication Policy

CONFIDENTIAL

HITRUST CSF v9.1 –Access Control – Related Standards	
Standard	**Description**
IRS Publications	IRS Pub 1075 v2014 3.2 IRS Pub 1075 v2014 4.3. IRS Pub 1075 v2014 4.5 IRS Pub 1075 v2014 4.7 RS Pub 1075 v2014 4.7.2 IRS Pub 1075 v2014 9.3.1.1 IRS Pub 1075 v2014 9.3.1.2 IRS Pub 1075 v2014 9.3.1.3 IRS Pub 1075 v2014 9.3.1.4
IRS Publications	IRS Pub 1075 v2014 9.3.1.6 IRS Pub 1075 v2014 9.3.1.7 IRS Pub 1075 v2014 9.3.1.8 IRS Pub 1075 v2014 9.3.1.9 IRS Pub 1075 v2014 9.3.1.10 IRS Pub 1075 v2014 9.3.1.11 IRS Pub 1075 v2014 9.3.1.12 IRS Pub 1075 v2014 9.3.1.13 IRS Pub 1075 v2014 9.3.1.14 IRS Pub 1075 v2014 9.3.1.15 IRS Pub 1075 v2014 9.3.3.3 IRS Pub 1075 v2014 9.3.5.7 IRS Pub 1075 v2014 9.3.7.2 IRS Pub 1075 v2014 9.3.7.3 IRS Pub 1075 v2014 9.3.7.4 IRS Pub 1075 v2014 9.3.7.5 IRS Pub 1075 v2014 9.3.7.6 IRS Pub 1075 v2014 9.3.7.8 IRS Pub 1075 v2014 9.3.9.4 IRS Pub 1075 v2014 9.3.10.3 IRS Pub 1075 v2014 9.3.10.6 IRS Pub 1075 v2014 9.3.11.5 IRS Pub 1075 v2014 9.3.11.9 IRS Pub 1075 v2014 9.3.16.3 IRS Pub 1075 v2014 9.3.16.5 IRS Pub 1075 v2014 9.3.16.7 IRS Pub 1075 v2014 9.3.16.10 IRS Pub 1075 v2014 9.4.1 IRS Pub 1075 v2014 9.4.2 IRS Pub 1075 v2014 9.4.5 IRS Pub 1075 v2014 9.4.8 IRS Pub 1075 v2014 9.4.9 IRS Pub 1075 v2014 9.4.10 IRS Pub 1075 v2014 9.4.11 IRS Pub 1075 v2014 9.4.13 IRS Pub 1075 v2014 9.4.14 IRS Pub 1075 v2014 9.4.15 IRS Pub 1075 v2014 9.4.16 IRS Pub 1075 v2014 9.4.17 IRS Pub 1075 v2014 9.4.18 IRS Pub 1075 v2014 Exhibit 10

CONFIDENTIAL

HITRUST CSF v9.1 –Access Control – Related Standards	
Standard	**Description**
ISO 27799:2008	ISO 27799-2008 7.3.3.1 ISO 27799-2008 7.8.1.2 ISO 27799-2008 7.8.2.1 ISO 27799-2008 7.8.2.2 ISO 27799-2008 7.8.2.3 ISO 27799-2008 7.8.2.4 ISO 27799-2008 7.8.3 ISO 27799-2008 7.8.5.1 ISO 27799:2008 7.8.6.1 ISO 27799-2008 7.8.6.2
ISO 27001:2005	ISO/IEC 27001:2005 A.11.4.1
ISO 27002:2005	ISO/IEC 27002:2005 7.2.2 ISO/IEC 27002:2005 8.1.3 ISO/IEC 27002:2005 9.2 ISO/IEC 27002:2005 10.1.3 ISO/IEC 27002:2005 11.1.1 ISO/IEC 27002:2005 11.2.1 ISO/IEC 27002:2005 11.2.2 ISO/IEC 27002:2005 11.2.2(b) ISO/IEC 27002:2005 11.2.2(d) ISO/IEC 27002:2005 11.2.2(e) ISO/IEC 27002:2005 11.2.2(f) ISO/IEC 27002:2005 11.2.3 ISO/IEC 27002:2005 11.2.4 ISO/IEC 27002:2005 11.3.1 ISO/IEC 27002:2005 11.3.2 ISO/IEC 27002:2005 11.3.3 ISO/IEC 27002:2005 11.4.1 ISO/IEC 27002:2005 11.4.2 ISO/IEC 27002:2005 11.4.3 ISO/IEC 27002:2005 11.4.4 ISO/IEC 27002:2005 11.4.5 ISO/IEC 27002:2005 11.4.6 ISO/IEC 27002:2005 11.4.7 ISO/IEC 27002:2005 11.5.1 ISO/IEC 27002:2005 11.5.2 ISO/IEC 27002:2005 11.5.3 ISO/IEC 27002:2005 11.5.4 ISO/IEC 27002:2005 11.5.5 ISO/IEC 27002:2005 11.5.6 ISO/IEC 27002:2005 11.6.1 ISO/IEC 27002:2005 11.6.2 ISO/IEC 27002:2005 11.7.1 ISO/IEC 27002:2005 11.7.2 ISO/IEC 27002:2005 12.5.4 ISO/IEC 27002:2005 13.1.1

CONFIDENTIAL

HITRUST CSF v9.1 –Access Control – Related Standards	
Standard	**Description**
ISO 27001:2013	ISO/IEC 27002:2013 6.2.1 ISO/IEC 27002:2013 6.2.2 ISO/IEC 27002:2013 7.2.2 ISO/IEC 27002:2013 8.2.3 ISO/IEC 27002:2013 9.1.1 ISO/IEC 27002:2013 9.1.2 ISO/IEC 27002:2013 9.2.1 ISO/IEC 27002:2013 9.2.2 ISO/IEC 27002:2013 9.2.3(b) ISO/IEC 27002:2013 9.2.3 ISO/IEC 27002:2013 9.2.4 ISO/IEC 27002:2013 9.2.5 ISO/IEC 27002:2013 9.3.1 ISO/IEC 27002-2013 9.4.1 ISO/IEC 27002:2013 9.4.2 ISO/IEC 27002:2013 9.4.3 ISO/IEC 27002:2013 9.4.4 ISO/IEC 27001:2013 A.9.2.6 ISO/IEC 27002:2013 11.2.8 ISO/IEC 27002:2013 11.2.9 ISO/IEC 27002:2013 11.5.2 ISO/IEC 27002:2013 13.1.3

CONFIDENTIAL

HITRUST CSF v9.1 –Access Control – Related Standards	
Standard	**Description**
PCI/DSS v3.2	PCI DSS v3.2 A.1.1 PCI DSS v3.2 1.1 PCI DSS v3.2 1.1.4 PCI DSS v3.2 1.2 PCI DSS v3.2 1.2.1 PCI DSS v3.2 1.4 PCI DSS v3.2 2.1 PCI DSS v3.2 2.2.1 PCI DSS v3.2 2.2.5 PCI DSS v3.2 7.1 PCI DSS v3.2 7.1.1 PCI DSS v3.2 7.1.2 PCI DSS v3.2 7.1.3 PCI DSS v3.2 7.1.4 PCI DSS v3.2 7.2 PCI DSS v3.2 7.2.1 PCI DSS v3.2 7.2.2 PCI DSS v3.2 7.2.3 PCI DSS v3.2 7.3 PCI DSS v3.2 8.1 PCI DSS v3.2 8.1.1 PCI DSS v3.2 8.1.2 PCI DSS v3.2 8.1.3 PCI DSS v3.2 8.1.4 PCI DSS v3.2 8.1.5 PCI DSS v3.2 8.1.6 PCI DSS v3.2 8.1.7 PCI DSS v3.2 8.1.8 PCI DSS v3.2 8.2 PCI DSS v3.2 8.2.1 PCI DSS v3.2 8.2.2 PCI DSS v3.2 8.2.3 PCI DSS v3.2 8.2.4 PCI DSS v3.2 8.2.5 PCI DSS v3.2 8.2.6 PCI DSS v3.2 8.3.1 PCI DSS v3.2 8.3.2 PCI DSS v3.2 8.4 PCI DSS v3.2 8.5 PCI DSS v3.2 8.5.1 PCI DSS v3.2 8.6 PCI DSS v3.2 8.7 PCI DSS v3.2 9.5 PCI DSS v3.2 12.3.2 PCI DSS v3.2 12.3.8 PCI DSS v3.2 12.3.9 PCI DSS v3.2 12.3.10
Joint Commission	Joint Commission IM.02.01.03 EP 1 Joint Commission IM.02.01.03 EP 5

CONFIDENTIAL

MARS-E v2	MARS-E v2 AC-1 MARS-E v2 AC-2 MARS-E v2 AC-2(1) MARS-E v2 AC-2(2) MARS-E v2 AC-2(3) MARS-E v2 AC-2(7) MARS-E v2 AC-3 MARS-E v2 AC-3(9) MARS-E v2 AC-4 MARS-E v2 AC-6 MARS-E v2 AC-6(1) MARS-E v2 AC-6(2) MARS-E v2 AC-6(5) MARS-E v2 AC-6(9) MARS-E v2 AC-6(10) MARS-E v2 AC-7 MARS-E v2 AC-9 MARS-E v2 AC-10 MARS-E v2 AC-11 MARS-E v2 AC-11(1) MARS-E v2 AC-12 MARS-E v2 AC-14 MARS-E v2 AC-17 MARS-E v2 AC-17(1) MARS-E v2 AC-17(2) MARS-E v2 AC-17(3) MARS-E v2 AC-17(4) MARS-E v2 AC-18 MARS-E v2 AC-18(1) MARS-E v2 AC-19 MARS-E v2 AC-19(5) MARS-E v2 AC-20 MARS-E v2 AT-2 MARS-E v2 AU-2 MARS-E v2 AU-5(1) MARS-E v2 AU-12 MARS-E v2 CM-2 MARS-E v2 CM-7 MARS-E v2 CM-7(1) MARS-E v2 DM-1 MARS-E v2 IA-1 MARS-E v2 IA-2 MARS-E v2 IA-2(1) MARS-E v2 IA-2(2) MARS-E v2 IA-2(3) MARS-E v2 IA-2(8) MARS-E v3 IA-2(11) MARS-E v2 IA-3 MARS-E v2 IA-4 MARS-E v2 IA-5 MARS-E v2 IA-5(1) MARS-E v2 IA-5(2) MARS-E v2 IA-5(3) MARS-E v2 IA-5(7) MARS-E v2 IA-5(11) MARS-E v2 IA-6 MARS-E v2 IA-8 MARS-E v2 MA-4

CONFIDENTIAL

HITRUST CSF v9.1 –Access Control – Related Standards

Standard	Description
	MARS-E v2 MA-4(2) MARS-E v2 MA-4(3) MARS-E v2 MP-3 MARS-E v2 PE-5 MARS-E v2 PE-17 MARS-E v2 PS-5 MARS-E v2 RA-2 MARS-E v2 SC-4 MARS-E v2 SC-7 MARS-E v2 SC-7(3) MARS-E v2 SC-7(4) MARS-E v2 SC-7(5) MARS-E v2 SC-7(7) MARS-E v2 SC-7(8) MARS-E v2 SC-7(12) MARS-E v2 SC-7(13) MARS-E v2 SC-8 MARS-E v2 SC-10 MARS-E v2 SC-13 MARS-E v2 SC-15 MARS-E v2 SC-32 MARS-E v2 SC-39

- FIPS PUB 140-2
- 42 C.F.R Section 160.103.
- Fair and Accurate Credit Transactions (FACT) Act of 2003

CONFIDENTIAL