P2111 - HITRUST - Access Control Policy

Contents

Purpose:

The purpose of the Access Control policy is to provide and establish Executive level explicit direction for all individuals and entities to follow guidelines for managing and controlling access to Organization information systems and data. This policy aims to align with HITRUST CSF requirements by defining procedures for user authentication, authorization, and access management.

The Organization is responsible for overseeing the development, implementation, and maintenance of the Information Security Program and associated components.

Scope:

This policy applies to all implemented information systems and supporting infrastructure used to support and protect sensitive data (PHI). This applies to systems whether managed centrally or in a distributed fashion, and to all individuals and entities who intend to access information systems and data. Within this document, the phrase "information systems and data" includes all technology resources and systems, transactions, applications, platforms, networks, databases, and other information systems within Integrity's technological environment.

Statement:

Access Control Requirements

Access control rules and rights for each user or group of users are based on clearly defined requirements for information dissemination and authorization (e.g., need-to-know, need-to-share, least privilege, security levels, and information classification).

The policy further defines logical and physical access control rules and rights for each user or group of users are considered together and clearly defined in standard user access profiles (e.g., roles).

The access control program must take into account security requirements of individual business applications and business units and validate standard user access profiles for common jobs roles in the organization.

Reference: 1101.01a1Organizational.1245

Users are given a written statement of their access rights. Users are required to sign a written statement stating they understand the conditions of access.

Reference: 1110.01b2System.7

Access rights to other applications are controlled according to applicable access control policies.

Reference: 1130.01v2System.1

Data stored in information systems is protected with system access controls, including file system, network share, claims, application, and/or database specific access control lists, and is encrypted when residing in non-secure areas.

Periodic reviews of such output are performed to ensure that redundant information is removed.

Reference: 1132.01v2System.3

Default Accounts

Default and unnecessary accounts are removed, disabled, or otherwise secured.

Reference: 1107.01b1System.2

Shared/Generic Accounts

User account administration processes do not use group, shared, or generic accounts and passwords.

Reference: 1111.01b2System.1

The organization validates account types are identified (individual, shared/group, system, application, guest/anonymous, emergency, and temporary) and conditions for group and role membership are established.

If used, shared/group account credentials are modified when users are removed from the group.

Reference: 1139.01b2System.10

Guest/anonymous, shared/group, emergency, and temporary accounts are specifically authorized.

Use of guest/anonymous, shared/group, emergency, and temporary accounts is monitored.

Reference: 1110.01b2System.7

Shared user/group IDs are only used in exceptional circumstances, where there is a clear business benefit for the use of a shared user ID for a group of users or a specific job.

Approval by management is documented when shared user/group IDs are used.

Additional controls are required to maintain accountability when shared user/group IDs are used.

Generic IDs that are used by an individual are allowed only where the functions accessible or actions carried out by the ID do not need to be traced (e.g., read only access).

Reference: 1124.01q2System.12

Proper identification is required for requests to establish information system accounts and approval of requests to establish such accounts.

Reference: 1106.01b2System.4

Help desk support requires user identification for any transaction that has information security implications.

Reference: 1128.01q2System.5

User Maintenance

Account managers are notified when users are:

- terminated,
- transferred,
- their information system usage or need-to-know/need-to-share changes, or
- when accounts (including shared/group, emergency, and temporary accounts) are no longer required.

Account managers modify the user's account accordingly.

Reference: 1108.01b2System.5

The organization maintains a current listing of all workforce members (individuals, contractors, vendors, business partners, etc.) with access to sensitive information (e.g., PII).

Reference: 11219.01b2System.8

User registration and de-registration, at a minimum:

- communicates password procedures and policies to all users who have system access;
- grants access to the information systems based on minimum necessary for assigned official duties, intended system usage and personnel security criteria such that usage/access is granular enough to support an individual's consent that has been captured by the organization and limit access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function;
- checks that the user has authorization from the system owner for the use of the information system or service;
- separates approval for access rights from management;
- checks that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy (e.g., it is consistent with sensitivity and risks associated with the information and/or information system, and it does not compromise segregation of duties);
- gives users a written statement of their access rights ;
- requires users to sign statements indicating that they understand the conditions of access;
- ensures service providers do not provide access until authorization procedures have been completed;
- maintains a formal record of all persons registered to use the service;
- removes or blocks critical access rights of users who have changed roles or jobs or left the organization immediately;
- removes or blocks non-critical access within 24 hours; and
- automatically removes or disables accounts within 90 days that have been inactive for a period of 60 days or more.

Reference: 1109.01b2System.6

User registration and de-registration formally addresses establishing, activating, modifying, reviewing, disabling, and removing accounts.

Further, at a minimum, the organization addresses:

- how access requests to information systems are submitted,
- how access to the information systems is granted,
- how requests to access sensitive information are submitted,
- how access to covered and/or confidential information is granted,
- how authorization and/or supervisory approvals are verified, and
- how a workforce members level of access to covered and/or confidential information is verified.

Reference: 11220.01b2System.9

The organization has a documented termination checklist that identifies all the steps to be taken and assets to be collected.

Reference: 11149.02g1Organizational.2

The termination process includes the return of all:

- previously issued software in the termination process,
- corporate documents in the termination process,
- equipment in the termination process, and
- other organizational assets such as mobile computing devices, credit cards, access cards, manuals, and information stored on electronic media in the termination process.

Reference: 11152.02h1Organizational.1

The organization ensures logical and physical access authorizations to systems and equipment are reviewed, updated, or revoked when there is any change in responsibility, or employment.

Reference: 11143.02i1Organizational.3

Access Authorization Requirements

The allocation of privileges for all systems and system components is controlled through a formal authorization process.

The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified.

Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role–user or administrator, only when needed).

Reference: 1143.01c1System.123

The access control system for the system components storing, processing, or transmitting covered information is set with a default "deny-all" setting.

Reference: 1150.01c2System.10

When PKI-based authentication is used, the information system validates certificates by:

- constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information;
- enforcing access to the corresponding private key;
- mapping the identity to the corresponding account of the individual or group; and
- implementing a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network.

Reference: 11111.01q2System.4

The requirements for controlling access to applications and application functions are addressed, such as, but not exclusive to:

- providing menus to control access to application system functions; controlling which data can be accessed by a particular user;
- controlling the access rights of users, e.g., read, write, delete and execute;
- controlling the access rights of other applications;
- limiting the information contained in outputs;
- and providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

Reference: 1129.01v1System.12

The organization ensures that outputs from application systems handling covered information contain only the information relevant to the use of the output, and are sent only to authorized terminals and locations.

Reference: 1131.01v2System.2

Actions to be performed without identification and authentication are permitted only to the extent necessary to accomplish mission objectives.

Reference: 1133.01v2System.4

Role-Based Access

Role-based access controls are implemented and capable of mapping each user to one or more roles, and each role to one or more system functions.

Reference: 1145.01c2System.1

The development and use of system routines and programs which avoid the need to run elevated privileges is promoted.

Reference: 1146.01c2System.23

Privileged Account Management

The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users and tracks and monitors privileged role assignments.

Reference: 1151.01c1System.2

System administrators only use accounts with privileged access when performing administrative duties and use a separate user account with standard user access rights when performing non-privileged activities (e.g., Internet browsing, email, or similar activities).

Reference: 11183.01c1System.3

Elevated privileges are assigned to a different user ID, other than one used for normal business.

All users access privileged services in a single role (users registered with more than one role designate a single role during each system access session).

The use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is minimized.

Reference: 1147.01c2System.456

Access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware is restricted and access to security relevant information is restricted to explicitly authorized individuals.

Reference: 1148.01c2System.78

The information system uses replay-resistant authentication mechanisms such as one-time passwords, or time stamps (e.g., Kerberos, TLS, etc.), nonce (a value used in security protocols that is never repeated with the same key) for network access to privileged accounts.

Reference: 11112.01q2System.12

Information Sharing

The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to business partners match the access restrictions on information for specific circumstances in which user discretion is allowed and employing manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions.

Reference: 1149.01c2System.9

Periodic Access Reviews

The organization reviews all accounts (including user, privileged, system, shared, and seeded accounts), and privileges (e.g., user-to-role assignments, user-to-object assignments) periodically (annually at a minimum).

Reference: 11.01e1System.2

The organization ensures all types of accounts, user access, and changes to access authorizations are reviewed at least every 90 days.

The organization ensures critical system accounts and authorizations for special privileged access rights are reviewed at least every 60 days.

Reference: 1168.01e2System.2

User access rights are reviewed after promotions, demotions, and termination of employment or end of other arrangement with a workforce member.

User access rights are reviewed and re-allocated when moving from one employment or workforce member arrangement to another within the same organization (i.e., transfer).

Reference: 1166.01e2System.3

Clear Desk/Screen Requirements

Covered or critical business information is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.

Workstations are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism that conceals information previously visible on the display when unattended, and protected by key locks, passwords, or other controls when not in use.

Documents containing covered or critical information are removed from printers, copiers, and facsimile machines immediately.

When transporting documents with covered or confidential information within facilities and through inter-office mail, covered or critical information is concealed during transit (e.g., using opaque envelopes).

Reference: 1114.01h1Organizational.123

External/Remote Access Requirements

Remote access by vendors and business partners (e.g., for remote maintenance) is disabled unless specifically authorized by management.

Remote access to business partner accounts (e.g., remote maintenance) is immediately deactivated after use.

Reference: 1117.01j1Organizational.23

Appropriate authentication methods, including strong authentication methods in addition to passwords, are used for communicating through an external, non-organization-controlled network (e.g., the Internet).

Reference: 1125.01q2System.1

Non-organizational users, or processes acting on behalf of non-organizational users, determined to need access to information residing on the organization's information systems, are uniquely identified and authenticated.

Reference: 11110.01q2System.10

When individuals are accessing sensitive information (e.g., covered information, cardholder data) from a remote location, then the copying, moving, printing, using print screen to capture, and storage of this information onto local hard drives and removable electronic media is prohibited, unless explicitly authorized for a defined business need.

Reference: 1134.01v3System.1

Minimum Necessary Configuration

Ports, services, and applications installed on a computer or network systems, which are not specifically required for business functionality, are disabled or removed.

Reference: 1194.01l1Organizational.2

Account Lockout

A policy applicable to the organization's information systems addressing account lockout after consecutive unsuccessful login attempts is documented and enforced through technical controls.

Reference: 11.01p1System.5

Unique User ID's

Each user ID in the information system (including non-privileged, privileged, seeded, and service accounts) is assigned to a specific, named individual to maintain accountability.

Reference: 1123.01q1System.2

The organization ensures that redundant user IDs are not issued to other users.

Users are uniquely identified and authenticated for local access and remote access.

Reference: 11109.01q2System.9

Multi-Factor Authentication

The organization requires multi-factor authentication for network and local access to privileged accounts.

Reference: 11.01q1System.3

The organization requires multi-factor authentication for access to non-privileged accounts from remote networks (including accounts in Web applications and in remote access solutions such as VPNs).

Reference: 11.01q1System.4

System Utilities

The use of system utilities is controlled by implementing the following:

- implementing identification, authentication, and authorization procedures;
- segregating of system utilities from applications software; and
- limiting the of the use of system utilities to the minimum practical number of trusted, authorized users.

Reference: 11124.01s1System.2

Session Time-out

Both bring your own device (BYOD) and company-owned devices are configured to require an automatic session time-out screen as enforced through technical means.

Reference: 11190.01t1System.2

Connection Time Controls

Connection time controls are implemented for sensitive computer applications, especially from high-risk locations (e.g., public, or external areas that are outside the organization's security management).

Connection time controls include:

- using predetermined time slots (e.g., for batch file transmissions or regular interactive sessions of short duration),
- restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation, and
- re-authentication at timed intervals.

Reference: 11131.01u1System.2

Segregation of Duties

Access authorization (e.g., access requests, approvals, and provisioning) is segregated among multiple individuals or groups.

Reference: 1105.09c1Organizational.2

This Access Control Policy is supported by the following procedures:

- *11 – HITRUST – Access Control Procedure*

The Organization - Deft Research LLC, Integrity LLC

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

Compliance Measurement

The Integrity Security Governance Committee will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Integrity Security Governance Committee in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A contractor found to have violated this policy may be subject to an immediate termination of the right to access Integrity's systems and may also include the termination of Integrity's engagement with the contractor's employer.

Policy References:

Related Procedure References:

Related Regulatory Information:

P2111 - HITRUST - Access Control Policy		
Document Author	**Name:** **Title:** **Email:**	Sumit Dhawan Manager Cybersecurity Compliance Sumit.Dhawan@integrity.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matt Williams Senior Director Cybersecurity & Cloud Engineering CISO matthew.williams@integrity.com 2/24/2026
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan McQueen Assistant General Counsel Duncan.McQueen@integrity.com 3/16/2026
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Product and Technology Officer Harsh.Singla@integrity.com 3/30/2026

Last Published Date: 3/30/2026

Document Version Number 2.0