Information Systems and Technology Security

Access Control Standard

Original author's name:	Pkkirisankar Jagannath
Most recent date:	November 22, 2022
Most recent version number:	v1.0
Process owner:	Program Director

Document History

Version	Date	Revised by	Description
v1.0	November 22, 2022	Pkkirisankar Jagannath	Original Draft
v1.0	November 22, 2022	Kulpreet Singh	Ratified Version

Designated document recertification cycle in days:	[Cycle 30 90 180 **365**]
Next document recertification date:	November 22, 2023

Access Control Standard

The **22nd Century Technologies** (the "Company") **Asset Protection Standard** defines objectives for establishing specific standards for protecting the confidentiality, integrity, and availability of Company information assets.

This Access Control Standard builds on the objectives established in the **Asset Protection Standard**, and provides specific instructions and requirements for the proper identification, authentication, and authorization controls necessary to access Company information assets.

1. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company premises or who have been granted access to Company information or systems, are covered by this standard and must comply with associated guidelines and procedures.

- **Authentication** refers to the controls for providing Users the means to verify or validate a claimed identity through the presentation of something they know (e.g., passwords), something they own (e.g., hardware token), or something they are (e.g. fingerprint, biometrics, etc.).
- **Authorization** refers to the controls for determining the resources that Users are permitted to access based upon the permissions and privileges for which they have been authorized.
- **Confidentiality classifications** are defined in the Information Classification Standard.
- **Encryption** refers to a method of scrambling information to render it unreadable to anyone except the intended recipient, who must decrypt it to read it.
- **Identification** refers to the controls for providing Users the means to convey their identities through the use of pre-determined identifiers.
- **Information assets** are defined in the Asset Identification and Classification Standard.
- **Integrity** refers to the protection of information and systems from malicious, unauthorized, or accidental changes.
- **Sensitive information** refers to information that is classified as Restricted or Confidential. Refer to the Information Classification Standard for confidentiality classification categories.

2. Requirements

a. Identification

i. Each User must have a unique account identifier or user ID.

ii. User communities and working groups must not share a single user ID for system access to ensure accurate accounting of user access and actions.

iii. User IDs should not be shared or used by anyone other than the User to whom they are assigned. Users shall be accountable for all activity associated with their assigned user IDs.

iv. User IDs should be added, modified, and deleted in accordance with Company-approved account management processes.

v. User IDs must be disabled within twenty-four (24) hours of notification of a status change (for example, resignation or change in job).

- User IDs must be disabled as soon as possible (Immediately) when user has been terminated under adversarial conditions to prevent retaliatory risks to company assets, resources, reputation, and employees. Any requests must come from Support PAL system to satisfy historical tracking, compliance requirements and audit requirements.

vi. User IDs that are unused, dormant, or inactive for 90 days days must be disabled.

vii. User IDs that are disabled for Inactive accounts are not deleted automatically, they are disabled and moved days must be deleted.

viii. Temporary User IDs (for testing, contractors and temporary employees) should have an account expiration date that coincides

with the anticipated end of employment, testing, or contract.

ix. Password resets must only occur through the usage of self-service portals utilizing challenge questions or predefined call-back numbers.

x. Disable, delete or deactivate any provided default access accounts to eliminate the potential of unauthorized access.

b. Authentication

i. Each user ID or account must be assigned a password.

ii. Passwords on new accounts must expire upon first log-in and require an immediate password change.

iii. All default system and application passwords must be changed prior to placing in the production environment or connecting to a live network.

iv. Authentication credentials such as passwords and tokens should not be used by anyone other than the User to whom they are assigned.

v. Passwords must conform to the following criteria, with native system enforcement when possible:

- Password length must be Twelve (12) characters or longer. If the system does not support Twelve (12) characters, the password must contain the maximum number of characters allowed by the system.

- Passwords must not be equal to, or a derivative of, the user ID.

- Passwords must contain at least one (1) alphabetic and one (1) non-alphabetic character.

vi. When password criteria cannot be enforced by the native system, an automated password system or tool should be used, whenever possible, to verify and enforce the password criteria.

vii. Password changes are required every 60 Days unless multifactor (two factor) authentication is used. Using MFA negates the need to change the base password as MFA generates a unique password every access instance.

viii. Password changes are required every three hundred and sixty-five (365) days for service and system IDs accounts, or within twenty-four (24) hours upon the termination of any employee with knowledge of the password to service and system IDs accounts.

- The account name and password must be transcribed onto a physical document containing the following information:
    - Custodians name and position
    - Date of creation
    - Date of recertification
    - Asset account belongs to
    - Password of the account
- There must be two identical copies of this document provided to the Program Manager and the CEO for physical safe storage or password vault application.
    - The document must be placed into a sealed envelope and placed into safe storage or password vault application.
    - The sealed envelope must be destroyed when it is replaced by a newly certified document.

- Under no circumstances should the document reside electronically in any email system, file system, or storage media without the highest level of encryption applied according to the 22nd Century Technologies Encryption Standard.

ix. Password changes are required every one hundred and eighty (180) days for user IDs with administrative or equivalent privileges or within twenty-four (24) hours upon the termination of any employee with knowledge of the password to administrative accounts.

x. Users should be notified a minimum of 14 Days before a current password expires.

xi. Grace log-ins after a required password change must be limited to one (1) log-in(s).

xii. Passwords must not be allowed in rapid succession, in order to prevent a user from "cycling" through passwords.

xiii. All systems, in accordance with the Auditing Standard, must log the date and time for all failed and successful user attempts to access the system.

xiv. All systems, in accordance with the Auditing Standard, must limit the number of failed log-on attempts to three (3) before disabling the user ID.

xv. Authentication credential, as user IDs and passwords, must not be written down or stored in readable form in automatic log-in scripts, software macros, terminal function keys, in computers without access control, shortcuts, or in other locations where unauthorized persons might discover them.

xvi. All passwords must be immediately changed if known or suspected of being disclosed.

xvii. All systems must require and authenticate a valid user ID and password or token prior to granting access to network or system resources. Appropriate access will be granted based on the Company defined role the employee or third-party requires and approved by management.

xviii. Authentication data (e.g. password files) must be protected with encryption controls to prevent unauthorized individuals from obtaining the data.

xix. Authentication data transmitted over a public or shared network must be encrypted in accordance with the Encryption Standard and Information Handling Standard.

c. Authorization

i. User access to information will be based on the confidentiality classification of the information asset.

- As it pertains specifically to access, the Company is required to maintain certifications and or regulatory requirements which are: FedRAMP -, ISO 27001 -, CMMC -, IRS 4812, CMMI

ii. Users should be only authorized the level of access to information assets that is required to meet an approved business need or perform prescribed job responsibilities.

- Specific IP ports and protocol restrictions must be implemented to properly control user and group access to infrastructure, applications, and network segments. Insecure service protocols are not permitted.

iii. Access to sensitive information must be provided on a need-to-know basis.

iv. User access rights to files, directories, and other objects should be assigned on a group basis and not assigned individually, unless doing so cannot be avoided.

v. Log-in time restrictions, whenever practical, should be set to limit the time of day when users can be logged into the system or network.

vi. The number of concurrent log-ins allowed per user ID should be restricted to the minimum number required to perform a given job function.

vii. Administrative access must be limited to only those users that explicitly require such privileged access. This access shall not be granted until a properly documented request has been approved by three designated managers to include the Program Manager.

viii. User with administrative responsibilities must not use a privileged account unless specifically performing actions that required an elevated privilege level.

3. Responsibilities

The Program Manager approves the Access Control Standard. The Program Manager also is responsible for ensuring the development, implementation, and maintenance of the Access Control Standard.

Company management, including senior management and department managers, is accountable for ensuring that the Access Control Standard is properly communicated and understood within their respective organizational units. Company management also is responsible for defining, approving and implementing procedures in its organizational units and ensuring their consistency with the Access Control Standard.

Asset Owners (Owners) are the managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the CEO will make the designation. The Owner is responsible for defining processes and procedures that are consistent with the Access Control Standard; defining the access control requirements for information assets associated with their

functional authority; processing requests associated with Company-approved access request procedure; determining the level of access and authorizing access based on Company-approved criteria; ensuring the revocation of access for those who no longer have a business need to access information assets; and ensuring the access controls and privileges are reviewed at least annually.

Asset Custodians (Custodians) are the managers, administrators and those designated by the Owner to manage process or store information assets. Custodians are responsible for providing a secure processing environment that protects the confidentiality, integrity, and availability of information; administering access to information assets as authorized by the Owner; and implementing procedural safeguards and cost-effective controls that are consistent with the Access Control Standard.

Users are the individuals, groups, or organizations authorized by the Owner to access to information assets. Users are responsible for familiarizing and complying with the Access Control Standard and associated guidelines; following Company-approved processes and procedures to request and obtain access to information assets; ensuring authorization credential such as password and tokens are not written down or stored in a place where unauthorized persons might discover them; reporting immediately to the **Information Security Helpline at 703-879-7996** when authorization credentials have been or may have been compromised; and maintaining the confidentiality, integrity and availability of information accessed consistent with the Owner's approved safeguards while under the User's control.

4. Enforcement and Exception Handling

Failure to comply with the Access Control Standard and associated guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the Access Control Standard should be submitted to the Company Program Manager. Exceptions shall be permitted only on receipt of written approval from the Program Manager. The Program Manager will periodically report current status to the Company CEO or its designee.

5. Review and Revision

The Access Control Standard will be reviewed and revised in accordance with the **Information Security Program Charter**.

Recommended: _____

Signature

Pakkirisankar Jagannath

Program Manager

Approved: _____

Signature

Anil Sharma

CEO