Information Systems and Technology Security

Access Control Procedure

Original author's name:	Pkkirisankar Jagannath
Most recent date:	May 2, 2023
Most recent version number:	v1.0
Process owner:	Program Director

Document History

Version	Date	Revised by	Description
v1.0	April 13, 2023	Pkkirisankar Jagannath	Original Draft
v1.0	May 2, 2023	Kulpreet Singh	Ratified Version

Designated document recertification cycle in days:	[Cycle 30 90 180 **365**]
Next document recertification date:	May 2, 2024

Access Control Procedure

The **22nd Century Technologies.** (the "Company") **Access Control Standard** provides specific instructions and requirements for the proper identification, authentication, and authorization controls necessary to access Company information assets.

This Access Control Procedure implements the requirements established in the **Access Control Standard** and provides detailed steps to perform tasks in support of the 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 procedure and must comply with associated standards and procedures.

2. Requirements

a. New User Access Request

All 22nd Century Technologies New User Access Requests are initiated by Human Resources Representatives:

- Human Resources Representatives should only submit an **Access Control Request Form** for a new user after completing the **Screening Checklist** as defined in the **22nd Century Technologies Onboarding Procedure**

- Human Resources Representative is responsible for ensuring the contains the following User Details at a minimum prior to submission:

    - First Name
    - Last Name

- Status: Exempt, Temporary, Contractor
- Position Title
- Contact Number
- Date for Initial Access
- Planned Date of Removal for Contractors or Temporary Workers
- Manager
- Position Title of Manager
- Location of the User

b. Upon receipt of the the 22nd Century Technologies Operations Team is responsible for ensuring the Human Resources Representative has completed all of the **User Details Section** of the Access Control Request Form. The Operations Team will place the Access Control Request on **HOLD status** and request the Human Resources Representative to resubmit the **if:**

- **User Details** are incomplete
- **Position Title** is not categorized as a Role in the Access Control Matrix.
- **Date of Access to be Removed** has not been completed for Temporary workers or Contractors

If a **Position Title** is not defined as a Role in the **Access Control Matrix** the Operations Team must request the Human Resources Representative to complete an **Access Control Exception Request** with authorization from the Program Manager.

c. s with complete User Details must be sent to the Manager of the new user for approval to initiate provisioning tasks for required access to resources.

The Manager is responsible for identifying the required resources for the new user and including descriptions for each resource category.

- Electronic Messaging
- Network Access
- Production Environment

- Development Environment
- Remote Access
- Multi-Factor Authentication
- Database Access
- Physical Access

d. Once the Manager of the New User has returned the the Operations Team can begin the **Provisioning Task Checklist**:

e. The Operations Team will update the status of the New User Access Request to Complete once the Provisioning Task Checklist has been completed.

Provisioning Task Checklist	Responsible
f. Review each resource requested and the associated description in the for completeness. **g.** The Operations Team is responsible for requesting the Manager to provide further detail for any descriptions that are incomplete, ambiguous, or unclear.	○ Operations Team ○ Manager
h. Review the Access Control Matrix and the resources requested by category: • Any resource access requested that is in compliance with the Role criteria defined in the Access Control Matrix can proceed to the next task in this checklist. • **For any resource category requested that is not an assigned membership or privilege for the applicable Role in the Access Control Matrix will require an exception request to completed with authorization from the Program Manager**. The Operations Team must	○ Operations Team ○ Manager ○ Program Manager

notify the Manager that the resources access requested is not assigned for the position title in the Access Control Matrix. The Operations Team must request the manager to complete an access control exception request. • Resource access that is requested and in compliance with the Access Control Matrix or that has been approved as an exception by the Program Manager will require the Operations Team to initiate Provisioning requests to the designated administrators in the Access Control Matrix.	
i. The Operations Team will initiate provisioning requests with the designated administrators for each resource category in the Access Control Matrix. The Operations Team is responsible for: • Including the and any associated Access Control Exception Authorization in the provisioning request • Updating the once the provisioning request has been initiated • Tracking the status of the provisioning request. • The Operations Team will initiate a follow up request to the Designated Resource Administrator if provisioning has not been completed within 3 business days. If the provisioning request has not been completed	○ Operations Team

within 5 business days, the Operations Team will notify the Manager and the Designated Resource Administrator that the provisioning request is still outstanding.	
j. The Designated Administrator for each resource category defined in the Access Control Matrix will provision the access requested and update the provisioning request immediately upon completion. **k.** The Designated Administrator is responsible for validating that the provisioning request includes the Manager's authorization and any applicable Access Control Exception authorizations. **l.** The Operations Team will initiate a follow up request to the designated administrator if provisioning has not been completed within 3 business days. If the provisioning request has not been completed within 5 business days, the Operations Team will notify the Manager and the designated administrator that the provisioning request is still outstanding.	o Designated Resource Administrators o Operations Team o Manager

m. Removing User Access

Human Resources Representatives, Assets Owners, and Asset Custodians can initiate a request to remove user access.

Requests to remove User Access can be initiated by submitting a User Termination Request via the , automated or manual email notification, or telephone call to:

- Human Resources Representatives

- Operations Team
- Designated Resource Administrator in the Access Control Matrix

The requestor is responsible for providing a specific **time for Access to be Removed** and indicating whether the request is for a **Friendly or Unfriendly Access Removal**. If the requestor has indicated the request is for an Unfriendly Access Removal, the Program Manager should be notified immediately via email and telephone.

Human Resources Representatives, Assets Owners, and Asset Custodians that have received a User Termination Request must complete an for termination of user access. Termination requests initiated via email notification or telephone also require a User Termination Request Form to completed.

Unfriendly Access Removals may be kept confidential if authorized by the user's Manager or the Program Manager. If confidentiality is requested the Manager or Program Manager must specify:

- The exact time when the access should be terminated
- The designated person to initiate an for the Termination Request

The Human Resources Representative, Asset Owner, or Asset Custodian that has received the User Termination Request is responsible for documenting the following at a minimum in the :

- User's First Name
- User's Last Name
- User's Position Title
- Planned Date/Time for Removal of Access
- Manager or Requestor
- Position Title of Manager or Requestor
- Location of the User

The must be submitted to the Operations Team.

Upon receipt of the the Operations team will start completing the Access Termination Task Checklist.

Access Termination Task Checklist	Responsible

n. has been submitted to Human Resources if Human Resources Representative has not already approved the Termination Request.	o Operations Team o Human Resources
o. has been submitted to the User's Manager for approval. **p.** The User's Manager is responsible for determining whether the Electronic Communications Resource Administrator should terminate, disable, or provision the User's accounts for forwarding for a specific period of time. **q.** The User's Manager is responsible for requesting access to any of the User's data or resources if this access has not already been provisioned. This will require authorization from the Program Manager.	o Operations Team o Manager o Electronic Communications Resource Administrator o Program Manager
r. The Operations Team will submit Termination requests to each Designated Resource Administrator. **s.** The Operations Team is responsible for providing all previous Provisioning Requests applicable to the user including the New User Access Request and all User Access Change Requests to the Designated Resource Administrators defined in the Access Control Matrix.	o Operations Team o Designated Resource Administrator
t. The Designated Resource Administrators will terminate or disable access in accordance with the applicable Resource Standard Operating Procedures. **u.** The Designated Resource Administrator is responsible for ensuring they have	o Designated Resource Administrators o Operations Team o Manager

reviewed all previous Provisioning Requests to ensure that all provisioned access has been terminated. **v.** The Designated Resource Administrator is responsible for reviewing all active accounts for association with the User's name. **w.** The Designated Resource Administrator will change any authenticators for shared or privileged accounts that were provisioned for the user. **x.** The Designated Resource Administrator will update the Termination Request immediately after access termination has been completed. **y.** The Operations Team will track and monitor all outstanding Termination Requests until completion. **z.** The Operations Team must issue follow up termination requests to Designated Resources Administrators if the termination request has not been completed within 1 business day. If the termination request has not been completed within 2 business days, the Operations Team will issue follow up termination requests to the Designated Resource Administrator and the Program Manager.	

3. Responsibilities

The Program Manager approves the Change Management Procedure. The Program Manager also is responsible for ensuring the development, implementation, and maintenance of the Change Management Procedure.

Company management, including senior management and department managers, is accountable for ensuring that the Change Management Procedure 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 Change Management Procedure.

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 Change Management Procedure; 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 Change Management Procedure.

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 Change Management Procedure 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 Change Management Procedure 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 Change Management Procedure 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 Procedures will be reviewed and revised in accordance with the **Information Security Program Charter**.

Recommended: _____

Signature

Pakkirisankar Jagannath

Program Manager

Approved: _____

Signature

Anil Sharma

CEO