Access Management Policy

Version No: 1.0

**Document Information:**

|  |  |
| --- | --- |
| Date of Release | 18-Jan-2024 |
| Document Author | Raghava V |
| Document Owner | DevSecOps |
| Document Reviewer |  |
| Document Approver |  |

**Version History:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Number | Authored By | Approved By | Approved On | Description of Change |
| 1.0 | Raghava V |  | 18-Jan-2024 | Full policy revamp.  -Privileged Access  -Access Revocation  -Access Review |

Table of Contents

[1. Introduction 3](#_Toc156473273)

[1.1 Scope 3](#_Toc156473274)

[1.2 Responsibility 3](#_Toc156473275)

[2. Policy 3](#_Toc156473276)

[2.1 Business requirements of Access Control 3](#_Toc156473277)

[2.2 User Access Management 4](#_Toc156473278)

[2.3 Users Responsibilities 7](#_Toc156473279)

[2.4 System and Application Access Control 8](#_Toc156473280)

[2.5 Management of Removable Media 11](#_Toc156473281)

[2.6 Data Protection Compliance 12](#_Toc156473282)

[3. Process 13](#_Toc156473283)

[3.1 User Access Management Process 13](#_Toc156473284)

[3.2 Secure Log-on Process 15](#_Toc156473285)

[3.3 Operating Systems and Applications Access Management Process 15](#_Toc156473286)

[3.4 Monitoring Access & Usage 16](#_Toc156473287)

[3.5 Privilege Access Management 16](#_Toc156473288)

# Introduction

This Policy defines the controls that need to be implemented and maintained to protect information assets against unauthorized access/usage that poses substantial risk to the organization. Access to information, information assets, and information-processing facility, systems, applications, equipment, and network devices shall be restricted as per the valid business requirements, user’s job responsibility, and information security & privacy requirements.

## Scope

This policy applies to all employees and interested parties who have access to CrossIdentity’s facilities, fixed assets, and books of record and information systems.

## Responsibility

This ownership of defining and effective implementation of this policy and process lies with IT Steering Committee and Project Leads.

## References

**ISO 27001:2022 (ISMS)**: A.5.15 (Access Control Policy), A.5.16 (Identity Management), A.5.17 (Authentication Information), A.5.18 (Access Rights), A.8.2 (Privileged Access Rights), A.8.3 (Information Access Restriction), A.8.4 (Access to Source Code), A.8.5 (Secure Authentication).

# Policy

## Access Control Policy

* Except for the publicly available information, access to all other information, information assets, systems, applications, equipment, and network devices shall be granted based on the legitimate business needs and after requisite approval.
* All information systems, applications, equipment, and network devices shall use an authentication mechanism to validate the users based on unique user ID and password. In the absence of the authentication mechanism, respective application-level authentication system shall be used to authenticate users.
* User IDs shall be linked to a specific individual and shall not be associated with computer terminals, departments, or job titles unless duly authorized.
* All employees shall be responsible for the activities carried out using their user ids and access cards.

### Access to Networks and Network Services

* All users shall have direct access only to the services that they have been specifically authorized to use.
* Users shall not establish any external network connections which include applications, client networks, servers from non-Crossidentity devices that could permit third-party users to gain access to Crossidentity systems and information.
* When using Crossidentity’s IT systems, or any Crossidentity’s information asset, users shall not deliberately conceal or misrepresent their network identity.

## Identity Management

### User Enrollment and De-Enrollment

* Allocation of access rights to non-public information / information assets shall be done in accordance with the ‘*Access Management Process’* (Refer Section 3 in this document).
* Every user shall be provided with unique login credential to access Crossidentity’s information / information assets, information systems, applications, equipment, and network devices based on the business and legitimate needs.
* Crossidentity does not encourage shared IDs but however based on necessity of business or operational reasons; approval shall be obtained for exception from Function Head.
* Every system where a user ID is created / modified and deleted shall have the capability to generate an audit trail of these events.
* Adequate approval shall be obtained before granting administrator rights to users. It is responsibility of the Project Lead or Function Head to ensure only employee with the appropriate role have privilege access for the system. This access shall be used for legitimate business purposes and shall be removed when no longer necessary.

### User Access Provisioning

* A formal user access provisioning shall be implemented to assign access rights for accessing Crossidentity’s information / information systems and information processing facilities.
* The access to Crossidentity’s information / information systems and information processing facilities must be in accordance with the principles of “least privilege” and "need to have" basis.
* Access shall be provisioned based on the authorization from respective Project Lead(s) or Function Head.
* The Project Lead or Function Head shall maintain a record of access rights granted or revoked for a user ID.

### Management of Privileged Access Rights

* Privileged access granted shall remain in effect for the requested duration and upon approval from respective Project Lead or Function Head.
* Quarterly review of all administrative privileges shall be performed by the respective Project Lead or Function Head.
* The respective Project Lead or Function Head shall maintain record of all the privileged access allocated. (Refer Section 3.5 in this document).

### Management of Secret Authentication Information of Users

* All information, information assets, information systems, applications, equipment, and network devices shall be configured with parameters for password management, as specified in the ‘Password Management Policy’.
* The password management system shall be based on the Authentication, Authorization and Accountability principle and shall be capable of enforcing the ‘Password Management Policy’.
* Recovery and change of encryption keys shall be ensured whenever there is termination of employment /change of role for the key(s) owner. Crossidentity’s ‘*Cryptography & Key Management Policy’* shall be followed as required.

### Review of User Access Rights

* End users access rights to information / information assets, information systems, applications, equipment, and network devices shall be reviewed at least annually and upon any change and shall be approved by the respective Project Lead / Function Head(s).
* For the internal transferred employee (changes in job responsibilities, across projects, departments), the existing user access rights shall be revoked within 24 hours of the date of transfer. Project Lead/ Function Head shall be responsible for access revocation.

### Removal or Adjustment of Access Rights

* Modification to access rights shall be tracked and logged. At a minimum, such tracking and logging shall provide the following information:
* Who modified the access
* Date and time of modification
* Identification of person whose access is being modified
* Brief description of modified access right(s)
* Approving authority
* Upon request for removal from HR Team via email, user ID shall be blocked/deleted/deactivated within 24 hrs.
* The review of user access rights shall include, but not limited to the following:
* Access for the existing / active users
* Access rights configured for users is in accordance with the approved job responsibilities.
* User IDs of the terminated employees are deactivated on the last working day.
* Access right modification due to transfer or changes in the job responsibilities.

## Users Responsibilities

### Use of secret authentication information

* For all information systems, applications, equipment and network devices, initial / default password shall be changed by the user after the first login.
* Passwords shall never be shared or revealed to anyone.
* Users shall not store passwords in any computer files, such as logon scripts or computer programs, unless the passwords have been encrypted with authorized encryption software/or password protected.
* Passwords shall not be written down.
* Login credentials and passwords are not encouraged to be shared in emails but however if necessary, login and password shall be shared in separate encrypted emails.
* All Crossidentity information systems, applications, equipment, and network devices shall be configured to ensure that passwords are masked, suppressed, or otherwise obscured such that unauthorized parties may not be able to observe and / or subsequently recover them.
* Users shall be accountable for safe and secure usage of their credentials.

## System and Application Access Control

### Information Access Restriction

* Access to information systems, applications, equipment, and network devices shall be provided and Crossidentity’s business sensitive information shall be hosted on a dedicated cloud-based access-controlled systems which at a minimum shall support following access restriction requirements:
* Controlling which data can be accessed by a particular user
* Controlling the access rights of user, e.g., read, write, delete, execute
* Provide physical and logical access controls for the isolation of sensitive application, application data or systems
* Any type of video or audio recording (For e.g., Zoom recording, StartMeeting Recording, Teams Meeting Recording, CCTV Recording) access shall be limited to authorized personnel and shall be deleted after it has served its purpose or as per the contractual requirement.
* Audio and Video Recording which are subject to any Incident, Event or Disciplinary action shall be retained and disposed as per ‘*Incident Management Policy*’.

### Secure Log-on Process

* The access to the information systems, equipment and network devices shall be restricted through a defined log-on process and access controls.
* The log-on process shall ensure that:
* The system shall not disclose any system related information unless the user is authenticated.
* The system shall log successful and unsuccessful attempts.
* Potential attempted or successful breach of log-on if detected, shall be raised as an incident for further proceedings.
* The system shall not display a password being entered.
* The user ID and password (or authentication key) are mandatorily required when accessing a system, a combination of both shall be provided to access the system.
* Administrator login shall be disabled or restricted to be used on certain occasions which shall be authorized by the respective project lead / Function Head.
* The number of unsuccessful login-attempts to critical systems shall be limited to less than or equal to five within 45 minutes after which account shall be locked out. All unsuccessful login attempts shall be recorded.
* Infra Team/Function Head and Project Lead while reviewing the access control matrix shall verify if the user ID is not used for more than 3 days, then the user ID access shall be revoked.
* All end point devices shall lock automatically when not in use for more than 5 minutes and can be accessed only with authentication.

### Password Management System

* Crossidentity shall use strong passwords / pin / keys as per the Password Security Standard to protect access to Crossidentity information systems and network / network services to minimize the risk of unauthorized access.
* All Passwords/ Credentials shall be created in accordance with the ‘*Password Management Policy*’ but otherwise in accordance with Client’s Password Management Policy.
* Credentials for the Administrator access (Administrator login) shall be changed on need basis.
* The password management system shall:
* Enforce the use of individual user IDs and passwords to maintain accountability
* Allow users to select and change their own passwords
* Enforce a choice of quality passwords
* Force users to change their passwords at the first log-on
* Enforce regular password changes as needed
* Store and transmit passwords in protected form

### Use of Privileged Utility Programs

* Access to various system utility programs that can override system and control applications shall be restricted to ensure that users do not obtain information or privileges other than what they require to perform their responsibilities.
* Privileged access is enabled only to competent & experienced professionals.
* All information systems shall have capability to log the use of utility programs.
* All utility programs that are not necessary for operations shall be removed or disabled.

### Access Control to Program Source Code

* All production program source code shall be stored in an approved version control management system.
* Function Head/ Project Lead shall be responsible to monitor access to all the environments of the defined scope of work. This shall consider the following: -
* Ensure that approval is only given to authorized personnel directly involved in delivering the services.
* Ensure that access is restricted based upon specific roles such that only authorized personnel are given access to production data, production programs, staging environment, live environment, Distribution List, Developed Application, and any other materials that are relevant to the scope of work.
* Perform quarterly reviews to ensure source code and object code remains restricted to authorized personnel only in accordance with *Access Control Matrix*.
* Environment/ Repositories must retain version history of source code changes. Such records must associate code changes with the individual who committed the change and date and time of change.
* Ensure that individual user accounts must be associated with a single individual.
* Ensure that individual account having access to production data, production programs, staging environment, live environment, and Developed Application, Distribution List must be promptly disabled if:
* Relieved from the organization.
* No longer required access.
* Ensure that activity records/ event logs are retained for as long as specified in the agreement but otherwise not less than 180 days.
* Code commits to the production environment shall be approved by the Technical Lead.
* Ensure backups of source code repositories have been performed as specified in the agreement but otherwise in accordance with ‘*Backup Management Policy*’.
* Source Code repository shall be deleted/archived as per the contractual obligation when it is no longer required.

## Use of Privileged Utility Programs

* Access to various system utility programs that can override system and control applications shall be restricted to ensure that users do not obtain information or privileges other than what they require to perform their responsibilities.
* Privileged access is enabled only to competent & experienced professionals.
* All information systems shall have capability to log the use of utility programs.
* All utility programs that are not necessary for operations shall be removed or disabled.

## Management of Removable Media

* All USB ports shall be disabled by group policy and an exception group who are permitted to access the ports shall be recorded and approved by management.
* Refer ‘*Asset Management Policy’* for more information.

## Data Protection Compliance

### Protection of Records

* CrossIdentity shall define Data retention and destruction policies to ensure the ability to access data (both media and format readability) throughout the retention period to safeguard against loss due to future technology change.
* CrossIdentity shall incorporate appropriate controls that restricts the transmission of client’s personal data or sensitive information outside CrossIdentity’s network.

### Privacy of Personally Identifiable Information

* Only authorized personnel shall have access to sensitive information. The controls shall address following, at a minimum:
* Ensuring that information is obtained and processed fairly and lawfully.
* Ensuring that there is a clear purpose for use/access to such information.
* Ensuring that the information is accurate, complete, up-to-date, adequate, and relevant.
* Ensuring to get explicit consent from an individual to collect and process their data.
* Ensuring that the data at rest and in transit shall have appropriate encryption in accordance with ‘*Cryptography and Key Management Policy’*.
* The modification, deletion and retention of the sensitive information are as per the applicable laws and regulations.
* CrossIdentity shall monitor usage of its information as per applicable laws. This may include, but not be limited to, logging, and reviewing of user activity such as web sites visited from CrossIdentity owned assets and electronic communications exchanged through CrossIdentity’s information processing facilities and networks.

# Process

## User Access Management Process

The User Access Management process shall include the following key activities.

### New Employee Onboarding – User Accounts

* For all types of employees requiring access, HR Team shall send email to Infra Team for providing necessary access.

### Resource Access Management

* User shall raise request via email along with required approval for any access requisition.
* New user accounts shall be provided with read only access by default for “CrossIdentity ISMS” folder in GDrive.
* For third party users (Client, Auditors, Vendors etc.), respective Function Head/ Project Lead shall authorize the request. The approval and authorization shall be given after analyzing whether the access rights requested by the user are the minimum required to perform his duties.
* Infra Team shall verify that proper, authorization and approvals are given before creating the user accounts.
* Project Lead and Function Head shall monitor access is given in accordance with *Access Control Matrix*.

### Requisition to Modify User Accounts Access

* Employee shall raise a request via Email to Application Owner (Function Head/ Project Lead) for any change in access along with required access.
* The change could be an additional access to perform his/her responsibilities or removing access for any application, software, or tools etc., where it is no more required for executing the job.
* If the change in access is because of internal transfer, then the existing project lead or Function Head shall revoke the access of the user as per the Access Control Matrix.

### Requisition to Remove User Accounts Access

* Access removal shall be initiated by respective Project Lead or Function Head for reasons like exit of an employee, internal transfers of the resource or access is no longer required etc.
* Infra team shall take back up of laptop or endpoint devices submitted by an employee upon exits if requested by the reporting manager.
* For user who resigns/relieves, HR Team shall send email to Infra Team post obtaining no-due clearance form from respective Project Lead or Business Head to revoke the access or account.
* If the removal of access is initiated by the Project Lead/ Function head for reasons beyond exit, then access shall be revoked accordingly. However, ticket shall be raised in CrossIdentity Helpdesk for accountability purpose.

### Emergency Change Request

Emergency change request shall be implemented for business continuity purposes. It shall have a fallback procedure to return to the previous state. Function Head(s) are responsible for the implementation of the changes. The status shall be updated by Function Head(s) to the necessary stakeholders.

### Review of Accesses

* Project Lead and Function Head shall own the responsibility to review the list of users associated with them to verify whether the privileges granted to the user is as per need to know and need to have basis. *Access Control Matrix* shall be reviewed and updated at least annually and upon any change.
* *Access Control Matrix* shall be reviewed by Function Head/Project Lead upon any change or minimum once a year.

## Secure Log-on Process

This process shall enable users including Infra Team to secure passwords and prevent from unauthorized access. Password parameters across CrossIdentity including Operating Systems, Applications and Network equipment’s shall be configured as per process below.

### Multi-factor Authentication (MFA)

Infra Team shall ensure the users are granted access only after successfully presenting more than one piece of evidence to an authentication mechanism for AWS and Gmail.

## Operating Systems and Applications Access Management Process

* Infra Team shall develop and maintain Hardening Guidelines for Operating Systems, devices and Applications and shall consider the following:
* Restriction on use of various type of user accounts.
* Restriction on access advanced programs and utilities.
* Restriction on access to Administrative Operating Systems Commands.
* Infra Team shall also ensure that all the installations of Operating Systems, devices and Applications are configured as per Hardening Guidelines.
* Infra Team shall review and update the Hardening Guidelines on an annual basis or on need basis to include latest security configuration issues.
* Infra Team shall perform periodic audit on the installations of Operating Systems, devices, and Applications to ensure that all of them are configured as per Hardening Guideline*.* The findings of the review shall be reported to Infra Head.

## Monitoring Access & Usage

All user activities must be logged by the Operating Systems, Applications and Network devices. If logging degrades the performance of the system, only critical commands or actions shall be logged and monitored. For further information refer “Logging and Monitoring Policy”

## Privilege Access Management

The privilege management is the practice of controlling and administering identities and the rights of those identities to perform actions on specified resources.

* Project Team/Function Head shall identify all the privileges associated with all Operating Systems, Business Applications, and Network Elements used in the.
* These privileges shall then be mapped with the job functions of the personnel involved in *Access Control Matrix*.
* *Access Control Matrix* shall be modified by Function Head/Project Lead when an Operating System, Application, or Network equipment undergoes a major change or new module, or a functionality is added.