System Access Control Policy

Doorway

SOC 2 Criteria: CC6.2, CC6.3, CC6.4, CC6.5, P4.3

Keywords: Access, Least privilege principle, Least access principle, Role change, Access reviews

---

Background

Access to Doorway systems and applications is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, and consultants. Access by any other entity is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorised use or access of the organisation's information systems.

Purpose

The purpose of this procedure is to provide a policy and guideline for creating, modifying, or removing access to the company’s network and data by creating, changing or deleting the network account configuration for a User.

Scope

This policy and defined process is used to allow access to the company’s data and systems to individuals who meet the requirements defined in this policy. This policy governs individuals who are granted access that is necessary to support the business. This policy relates to all data used, processed, stored, maintained, or transmitted in and through the company’s systems.

Access Establishment and Modification

Requests for access to Doorway Platform systems and applications are made formally using the following process:

1. A Doorway workforce member initiates the access request by creating an Issue in the Doorway ticketing system.
    1. User identities must be verified prior to granting access to new accounts.
    2. Identity verification must be done in person where possible; for remote employees, identities must be verified over the phone.
    3. For new accounts, the method used to verify the user's identity must be recorded on the Issue.
2. The Security Officer will grant or reject access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request.
3. If the request is rejected, it goes back for further review and documentation.
4. If the review is approved, the request is marked as “Done”, and any pertinent notes are added.

Access Reviews

All access to Doorway systems and services is reviewed and updated on an annual basis to ensure proper authorisations are in place commensurate with job functions. The process for conducting reviews is outlined below:

1. The Security Officer initiates the review of user access by creating an Issue in the Doorway Ticketing System
2. The Security Officer is assigned to review levels of access for each Doorway workforce member.
3. If user access is found during review that is not in line with the least privilege principle, the Security Officer may modify user access and notify the user of access changes.
4. Once the review is complete, the Security Officer then marks the ticket as “Done”, adding any pertinent notes required.

Workforce Clearance

- The level of security assigned to a user to the organisation's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification.
- All access requests are treated on a **"least-access principle."**
- Doorway maintains a minimum necessary approach to access to Customer data.

Unique User Identification

- Access to the Doorway Platform systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user and developer.
- Passwords requirements mandate strong password controls.
- Passwords are not displayed at any time and are not transmitted or stored in plain text.
- Default accounts on all production systems, including root, are disabled.
- Shared accounts are not allowed within Doorway systems or networks.
- Automated log-on configurations other than the company’s approved Password Management provider that store user passwords or bypass password entry are not permitted for use with Doorway workstations or production systems.

Automatic Logoff

- Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).

Employee Workstation Use

All workstations at Doorway are company owned, and all are laptop products running Windows, Mac OSX or Linux.

- Workstations may not be used to engage in any activity that is illegal or is in violation of organisation's policies.
- Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through the organisation's system.
- Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organisation's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
- Solicitation of non-company business, or any use of organisation's information systems/applications for personal gain is prohibited.
- Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
- Workstation hard drives must be encrypted

- All workstations have firewalls enabled to prevent unauthorised access unless explicitly granted.

Employee Termination/Off-boarding Procedures

1. The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitate completion of the "Termination Checklist".
2. The Human Resources Department, users, and supervisors are required to notify the Security Officer to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):
    1. The user has been using their access rights inappropriately;
    2. A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
3. The Security Officer will terminate users' access rights within 1 business day of termination/separation, and will coordinate with the appropriate Doorway employees to terminate access to any non-production systems managed by those employees.
4. The Security Officer audits and may terminate access of users that have not logged into the organisation's information systems/applications for an extended period of time.

Revision History

Version	Date	Editor	Description of Changes
1.0	15.03.2022	Henry Sinclair	Initial Creation