SM8RTHEALTH
Sm8rtHealth LLP, Campus261, 261 Morrin Road, St John, Auckland, 1072, New Zealand

SM8RTHEALTH ACCESS CONTROL POLICY

Last updated: 2025-06-23

Contents

Purpose

This policy outlines the responsibilities and mechanisms required to ensure secure and controlled access to Sm8rtHealth's information systems. It must be read in conjunction with the Sm8rtHealth Privacy Policy. The intent is to include guidelines for integrating and managing OpenAI services, within the organization's access control framework.

Scope

This policy applies to all users of information assets including Sm8rtHealth employees, employees of temporary employment agencies, vendors, business partners, and contractor personnel and functional units regardless of geographic locations. This policy also applies to third-party services integrated with Sm8rtHealth systems, including AI tools such as OpenAI.

This Policy covers all Information Systems environments operated by Sm8rtHealth or contracted with a third party by Sm8rtHealth. The term "IS environment" defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, wireless devices), software, and information.

Although this Policy explicitly covers the responsibilities of vendors and developers, it does not cover the matter exclusively. Other Sm8rtHealth Information Security policies, standards, and procedures define additional responsibilities.
Vendors may be required to read, understand, and comply with.

- Sm8rtHealth Access Control Policy (Staff and Client Users)
- Sm8rtHealth Business Continuity Plan (Developers and Staff)
- Sm8rtHealth Incident Response Plan (Staff and Clients)
- Sm8rtHealth Privacy and Security Statement (Staff and Clients)

All policies and procedures are available on request or from link from the knowledgebase in from the Sm8rtHealth Application Workbench..

Responsibilities

Sm8rtHealth follows the AWS guideline on Best Practice for security and access control. Sm8rtHealth management is responsible for maintenance and accuracy of the policy. Any questions regarding this policy should be addressed to Compliance Officer at support@sm8rthealth.com

Definitions

Authentication means the identification requirements associated with an individual using a computer system. Identification information must be securely maintained by the computer system and can be associated with an individual's authorization and system activities.

Availability means ensuring that authorized users have access to information and associated assets when required.

Confidentiality means ensuring that information is accessible only to those authorized to have access.

Critical means the degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

Integrity means safeguarding the accuracy and completeness of information and processing methods.

Sensitive relates to the use of highly classified information or involving discretionary authority over important official matters.

Policy Statement

Access controls are necessary for Sm8rtHealth systems, to ensure the protection of intellectual property, and to contain sensitive or limited access to data. This policy describes the mechanisms to implement access controls and responsibilities to ensure a high level of information security.

Authorization of access to information

Access to information is authorized as follows.

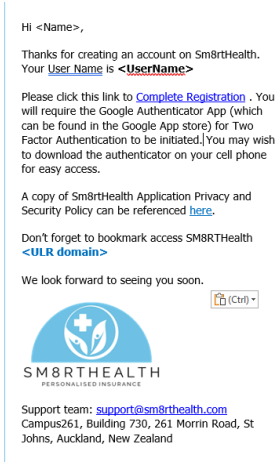
- Access to information is controlled based on business and security requirements and access control rules defined for each information system.
- All Sm8rtHealth vendors will be permitted to access only those critical business information assets and processes which are required for performing their duties.
- Access to critical business information assets and activation of accounts for contractors, consultants, temporary workers, or vendor personnel will only be granted when the individual is actively performing service for Sm8rtHealth (as employee or contractor).
- Access for contractors, consultants or vendor personnel to Sm8rtHealth critical business information assets is subject to signing the Sm8rtHealth Confidentiality Agreement (NDA).

User registration and system access

The registration and termination of user access to systems shall be managed as follows.

- All requests for access are logged in MantisHub for processing
- Users will be emailed the Sm8rtHealth ***Request for Access*** **Form**
- SM8 will ensure security check and personal credentials as may be required.
- Where the Client has already provided security clearance screening of the employee, SM8 will take no further vetting action and rely on the Clients due diligence in candidate security vetting.

- A voice call or SMS will be used to validate the new User and ensure contact details are accurate.
- User ID and access instructions are auto generated once the user is created and emailed to the User. (**Sample below**)
-



Hi <Name>,

Thanks for creating an account on Sm8rtHealth.
Your User Name is **<UserName>**

Please click this link to Complete Registration . You will require the Google Authenticator App (which can be found in the Google App store) for Two Factor Authentication to be initiated. You may wish to download the authenticator on your cell phone for easy access.

A copy of Sm8rtHealth Application Privacy and Security Policy can be referenced here.

Don't forget to bookmark access SM8RTHealth
<ULR domain>

We look forward to seeing you soon.

(Ctrl)

SM8RTHEALTH
PERSONALISED INSURANCE

Support team: support@sm8rthealth.com
Campus261, Building 730, 261 Morrin Road, St Johns, Auckland, New Zealand

- As part of the onboarding process, once created, Users will be required to complete registration and create a password.
- All Users are provided with documentation of their access rights and terms of use.
- No users shall be granted access to any system prior to completing all authorisation steps.
- Where AI systems (e.g., OpenAI tools) are used, user access requests must also include the intended use case and required data access scope
- User accounts will automatically expire after 60 days due to inactivity

Redundant User ID's

- Will not be re-issued to new users.
- New accounts that have been unused for 60 days will by default be disabled.
- The User accounts of personnel leaving the employment of Sm8rtHealth or its service providers will be disabled immediately upon exit.
- Third-party personnel requiring access to Sm8rtHealth's systems must follow Third Party Access Authorisation procedures for user registration.

Review of user access rights

User access rights will be default.

- Will be auto disabled after 60 days if the account is not accessed
- Will be manually disabled immediately on departure from the Clients employment upon notification.
- Reviewed due to any breach of Sm8 security and privacy policy

Management of user privileges

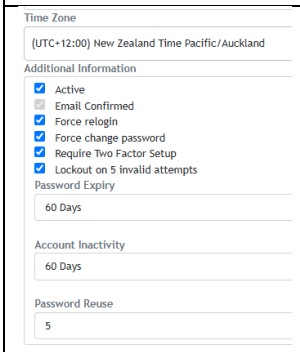
User privileges will be managed as follows.

- All user privileges are assigned through a formal authorisation procedure in the **Access Control Request Form.**
- Sm8rtHealth will ensure that no privileges are assigned before the completion of the **Access Control Request Form.**

- All privileges will be allocated or modified on an 'as required' basis, with the authority of the designated Client Product Manager.

User password management

User passwords controls and management.

User Account Extract	
	Active: Make account inactive on demand
	Force relog in: Set account inactivity default
	Force change password: Set Password expiry (default 60 days)
	Option to switch-on or off TFA setup by domain URL
	Maximum 5 failed attempts permitted before account will lock-out and require Admin. Reset.

User responsibilities regarding passwords and unattended equipment

User responsibilities for managing passwords and unattended equipment are as follows; .

- Users must enable password-protected screen savers on desktops, portable computers/laptops, and servers.
- Users should set their device timer to enable the screen saver after no more than 5 minutes of inactivity.
- Users must terminate (log-off) active sessions when activities are finished.
- For AWS connection, users must log off after completion of their tasks.

Access control – Hosting Network

Policy regarding use of network services.

- Access to hosting network services will be specifically authorised in accordance with Sm8rtHealth's User Access Control procedures and the NDA terms and conditions entered into with the Client or Supplier.
- Access to hosting network services will be controlled in accordance with SM8 business and security requirements, with access control rules defined as per AWS IAM secure network least privileges guidelines.

Access Control to AWS Hosting Services

Access to Sm8rtHealth's AWS cloud infrastructure is:

- Restricted to named DevOps personnel and security administrators.
- Provisioned through role-based AWS IAM with least privilege.
- Enforced with TFA, session timeout, and CloudTrail logging.
- Periodically reviewed (quarterly) and automatically revoked after 60 days of inactivity.
- Audited using AWS Config, GuardDuty, and Access Analyzer.

No AWS root account access is permitted for daily operations. Production (PROD) access requires documented change request approval.

User identification and authentication

- Sm8rtHealth will identify and authenticate all users before granting the appropriate system access.
- User ID naming conventions must be consistent and documented.
- User ID's must not be shared between users.
- Use of system programs
- Access to and use of system programs will be restricted and controlled.
- Use of system programs will be limited to authorised individuals.
- All actions undertaken by an individual on system programs will be logged
- All unnecessary system utilities and software, including compiler programs, will be removed.
- Terminal time-out
- All systems will be locked after a defined time of inactivity.

Access Control Information Resources

Information access will be restricted as follows.

- Access to Sm8rtHealth information resources and applications will be restricted to Users that require them and in accordance with information Access Control Policy.
- All users will have controlled access (Read, Write, Modify, Execute and Full control) to all information resources and business applications of Sm8rtHealth, in accordance to their requirements.
- The owner of the information resources and business application will review the access rights based on criticality of information or at every 6 months.
- AI-based tools used in system programs must be reviewed and approved by Sm8rtHealth's Information Security Team prior to use

Access control - Other devices and shared SaaS tools and repositories

Mobile computing and remote access

- All mobile computing facilities (e.g. laptop computers, palmtop computers, notebooks, mobile phones) will be used in a secured environment, using cryptographic controls for communication purposes.
- All mobile computing facilities (e.g. laptop computers, tablets, notebooks, mobile phones) will have boot or access password or pattern.

- All personnel using remote access will be provided with a secure connection (e.g. Secure Socket Layer, IPSec, Virtual Private Network, encryption) to information system networks.
- The maintenance and support, audit, monitoring, training on security controls and practices, management of access rights, and physical security for remote access, will be in accordance with the defined procedures.

Shared Folders

Clients are granted access to Sm8rtHealth-approved SaaS applications (e.g., Slack, MantisHub, Dropbox) for collaboration and project tracking. Access is:

- Provisioned only to named client contacts based on contractual role (e.g., product owner, QA lead).
- Time-bound and reviewed quarterly.
- Revoked immediately upon project completion or role change.
- Restricted to specific channels or folders as per role-based access control (RBAC).

All client-accessible repositories are logged and auditable. Client access requests must be processed through the Access Control Request Form and authorised by the designated Client Product Owner.

Monitoring of system access and usage

Access monitoring will be as follows.

- All event details on information system will be logged and stored for 6 months for ordinary systems and one year for critical systems.
- All information systems and business application will be monitored, and results of monitoring must be reviewed periodically.
- Use of third-party AI services (including OpenAI) must be logged and monitored, and logs must include prompts submitted and responses received for audit purposes.
- All system clocks will be synchronised and reviewed for inaccuracy and drift.
- All unsuccessful login attempts to critical servers will be recorded, investigated, and escalated to management.

Compliance management

Compliance with the Access Control Policy is mandatory, as follows.

- Managers will ensure continuous compliance monitoring.
- Compliance with Access Control Policy will be reviewed periodically.
- Violations of the policies, standards, and procedures will result in corrective action by management, with disciplinary action taken consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:
- Loss of access privileges to information assets
- Other actions as deemed appropriate by management, Human Resources, and the legal recourse.

SM8RTHEALTH
Sm8rtHealth LLP, Campus261, 261 Morrin Road, St John, Auckland, 1072, New Zealand

Request for access Sm8rtHealth environments.

All individuals seeking access to intellectual property or confidential information owned by Intelligent Life or its clients, including (without limitation) source code, specifications, documentation, designs, underwriting rules, audits, 3rd party information and other related materials, must complete this form.

First name	
Surname	
Your job title	
Client authority name	<client product owner responsible for platform)
Name of person you report to	
Email address	
Mobile phone	
Your LinkedIn profile Id	

I request access to (Mark with ☑ all that apply)

☐	Sm8rtHealt Dropbox Document	☐	AWS Hosting environment
☐	MantisHub Ticketing system	☐	Client Development environment (DEV)
☐	Sm8rtHealth Slack Channel	☐	Client Testing environment (UAT)
☐	Swagger (API) documentation	☐	Client Production environment (PROD)
☐	Reporting extracts	☐	SM8 demonstration environment

Comments or special requests:

☑ I agree to the terms as read in Sm8rtHealth Access Control Policy.

Applicant name		Organisation	
Applicant signature		Product owner	
Dated		Authoriser Signature	

Request for Removal of Access from Sm8rtHealth hosted environments and information.

All individuals seeking removal of access to intellectual property or confidential information owned by Sm8rtHealth or its clients, including (without limitation) source code, specifications, documentation, designs, underwriting rules, audits, 3rd party information and other materials, must complete this form.

First name	
Surname	
Your company	
Your title or position in company	
Name of person you report to	
ID (Driver's license or NRIC or Passport No.)	
Email address	
Mobile phone	

I request removal of user access from ALL Sm8rtHealth research and development environments and eco-systems for the following reasons: (Select most relevant reason with an 'X')

I am no longer employed by the service provider under which I was granted access	
I am no longer involved in supporting Sm8rtHealth solutions	

Signed:	Dated:
Removed by:	Removal date: