SM8RTHEALTH

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

ACCESS CONTROL POLICY

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 the;

- Sm8rtHealth Access Control Policy
- Sm8rtHealth Business Continuity Plan (developers and support vendors)
- Sm8rtHealth Incident Response Plan (network and support vendors)
- Sm8rtHealth Privacy and Security Statement

All policies and procedures available on request.

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. **Note**: Where the Client has already provided security clearance screening of the employee, SM8 will take no further screening action and rely on the Clients employee on-boarding security process and protocols.
- A voice call or SMS will be used to validate the User contact details.
- User ID and any access instructions will be emailed to the User
- 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
- A log of all registered Users is maintained and checked periodically for unused, redundant, or expired user accesses or accounts, or incorrect privileges.

Redundant User ID's

- Will not be re-issued to new users.
- New accounts that have been unused for 14 days will 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 reviewed every 6 months.

A review of all special privilege access rights will be carried out annually, or as required.

Management of user privileges

User privileges will be managed as follows;

- All user privileges must be assigned through a formal authorisation procedure
- Sm8rtHealth will ensure that no privileges are assigned before the completion of such procedure
- All privileges will be allocated on an 'as required' basis.

User password management

User passwords will be managed as follows;

- Users must apply Sm8rtHealth's password policy regarding password usage and management.
- Initial temporary passwords must be conveyed in a secure manner.
- When Sm8rtHealth's standard encryption algorithm option is available, initial temporary passwords shall be conveyed via e-mail.
- Users must change their temporary password upon first login.
- In the event of forgotten passwords, temporary passwords will only be issued following positive identification of the user.
- All passwords relating to a System Administrator that has left the employ of Sm8rtHealth or its service provider will be immediately changed.
- Users may not store passwords on a computer or in any place with public access.
- Passwords must be changed at least every 6 months.

User responsibilities regarding passwords and unattended equipment

User responsibilities for managing passwords and unattended equipment are as follows; • Users must abide by the password management policy set out above.

- 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 15 minutes of inactivity.
- Users must terminate active sessions when activities are finished.
- For AWS connection, users must log off after completion of their tasks.

Access control - Networks

Policy regarding use of network services;

- Access to networks and network services will be specifically authorised in accordance with Sm8rtHealth's User Access Control procedures and NDA terms and conditions.
- Access to networks and network services will be controlled in accordance with business and security requirements, and access control rules defined for each network.

Network connection control;

A Service Policy Table will be formulated for each service that is allowed through each firewall.

All external connections by business partners and customers will be documented and authorized in accordance with the defined "Security Change Request" procedure.

Network routing control;

Appropriate routing control methods will be deployed to restrict information flows to designated network paths within the control of Sm8rtHealth.

Network routing controls will be based on positive source and destination address checking methods.

Security of network services;

Sm8rtHealth will obtain detailed descriptions of the security attributes of any external services (if any) from external Network services providers

Security attributes descriptions will establish the confidentiality, integrity, and availability of business applications and the level of controls (if any) required to be applied by Sm8rtHealth.

Description of the security controls will be included in the agreement of services.

Access control - Operating Systems

- Automatic terminal identification
- Automatic terminal identification will be used when it is important that transactions are only initiated from a specific terminal or location.
- Terminal log-on procedures
- Terminal logon procedures will disclose a minimum amount of information about the system.
- System administrators will set the password management system to suspend the User ID after three consecutive unsuccessful attempts. A system administrator will require approval from the user's supervisor to reset the User ID.
- A legal banner will appear on all Sm8rtHealth systems prior to login.

- The logon procedure will not identify the system or application until the logon process has been successfully completed.
- Systems will validate logon information only on completion of all input data.
- After a rejected logon attempt, logon procedures will terminate. The procedure will not explain which item of information (the User ID or password) was the reason for the logon termination.
- If an error condition occurs, systems will not indicate which item of data is correct or incorrect. The logon procedures will set a maximum time allowed for the logon process. If the time is exceeded, the system will terminate the logon process.
- On successful completion of logon, the logon procedures will display the date/time of the previous successful logon, and the number and date/time of unsuccessful logon attempts since the last successful logon.

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.

Limitation of connection time

Wherever possible, all critical systems will have a defined time slots for access and connectivity.

Access control - Applications

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

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

- Access to shared folders will be authorised for specific persons only.
- Shared Folders will be used for work purpose only.

- Use of an approved document repository for remote and limited access to shared folders and files.

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 LLP

Request for access to Sm8rtHealth environments and information

All individuals seeking access to intellectual property or confidential information owned by Sm8rtHealth LLP 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 company	
Your title or position in company	
Name of person you report to	
ID (*Driver's license / Passport No. / HKID etc.)*	
Email address	
Mobile phone	

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

☐ Source code
☐ Sandbox Environments
☐ Development/Testing Environments
☐ Production environments
☐ URL's requested

☐ Hosting and network environment
☐ Document repositories
☐ Reporting and analytics data
☐ Backups and BC authority and data

☐ I agree to the terms set forth in the Sm8rtHealth Access Control Policy.

Applicant name		Organisation	
Applicant signature		Approved by	
Dated		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: