onequity

OnEquity (MU) Ltd Information Security Policy

AUGUST 2025

ONEQUITY (MU) LTD
FSC License
No.GB23201814

1.0 Introduction

ONEQUITY (MU) LTD (the "Company", "We" "OnEquity") is regulated by the Financial Services Commission Mauritius ("FSC") under license number GB23201814 as an Investment Dealer (Full Service Dealer, Excluding Underwriting).

2.0 Policy

In line with the foregoing, it is the policy of the Company that information, as defined hereinafter, in all its forms -- written, spoken, recorded electronically or printed – will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All documentation, which may be in electronic form, must be retained for at least 7 (seven) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity and/or department within Company.

At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

3.0 Scope

The scope of information security includes the protection of confidentiality, integrity and availability of information.
The framework for managing information security in this policy applies the Company entities and workers, and other Involved Persons and all Involved Systems throughout the Company, as defined below under the heading "Information Security Definitions".
This policy and all standards apply to all protected personal information and other classes of protected information in any form as defined below under the heading 'Information Classification'.

4.0 Risk Management

A thorough analysis of all the Company's information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats- internal or external, natural or manmade, electronic and non-electronic – that affect the ability to manage the information resource. The analysis will also

document the existing vulnerabilities within each entity which potentially expose the information resource to the threat. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency ofthe risk analysis will be determined at the entity level.

Based on the periodic assessment, measures will be implemented that reduce the impact of the potential threats by reducing the amount and scope of the vulnerabilities.

5.0 Information Security Definitions

5.1 Affiliated Covered Entities: Legally separate, but affiliated, entities, which are covered by this Information Security Policy.

5.2 Availability: Data or information is accessible and usable upon demand by an authorized person.

5.3 Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

5.4 Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

5.5 Involved Persons: Every worker at the Company – no matter what their status. This includes employees, contractors, consultants, temporaries, volunteers, interns, etc.

5.6 Involved Systems: All computer equipment and network systems that are within that Company environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

5.7 Personal Information: Information related to a living who can be identified from such information or such information and other information in the possession of, or likely to come into the possession of, the Company (such information may include, but is not limited to, personal details such as name, address, date of birth, contact details, employment details, assets and liabilities, identification number, passports, driver's license etc, as well as other financial information related to a living individual who can be identified from such information or from such information and other information in the possession of, or likely to come into the possession of, the Company;

5.8 Proprietary Information: All information relating to the business, plans, intellectual property and/or technology of the Company including, but not limited to technical information including inventions, methods, plans, processes, specifications, characteristics, assays, raw data, scientific preclinical or clinical data, records, databases, formulations, clinical protocols, equipment design, know-how, experience, and trade secrets; developmental, marketing, sales, customer, supplier, consulting relationship information, operating, performance, and cost information; computer programming techniques whether in tangible or intangible form, and all record bearing media containing or disclosing the foregoing information and techniques including, written business plans, patents and patent applications, grant applications, notes and memoranda, whether in writing or presented, stored or maintained in or by electronic, magnetic, or other means, as well as all other materials containing information about the Company, as well as any other information specifically identified, either verbally or in writing, as proprietary

to the Company;

5.9 Protected Information: Comprises all information created or received by the Company, including, without limitation, the Company's Proprietary Information, as well as all Personal Information and/or Sensitive Information in the possession of, likely to come into the possession of the Company;

5.10 Sensitive Information: Personal Information related to a living individual who can be identified from such information or from such information in the possession of, or likely to come into the possession of the Company, including, without limitation, information or data pertaining to:

5.10.1 race or ethnic origin
5.10.2 religious beliefs or other beliefs of a similar nature,
5.10.3 political opinions,
5.10.4 physical or mental health or condition,
5.10.5 sexual history or orientation,
5.10.6 trade union membership and/or
5.10.7 commission or alleged commission of any offense and any related court proceedings.

5.11 Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

6.0 Information Security Responsibilities

Chief Technology Officer: The Chief Technology Officer (CTO') is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of the Company.
Specific responsibilities include:

6.1 Ensuring security policies, procedures, and standards are in place and adhered to by each entity;

6.2 Providing basic security support for all systems and users;

6.3 Advising owners in the identification and classification of computer resources;

6.4 Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, though testing and production implementation;

6.5 Educating custodian and user management with comprehensive information about security controls affecting system users and application systems;

6.6 Providing on-going employee security education;

6.7 Performing security audits;

6.8 Reporting regularly to the Company Oversight Committee on entity's status with regard to information security.

Information Owner: The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the Company Information Owner Form.

The Information Owner has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on advice from the Legal Department.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information user or created within the unit.
4. Authorizing access and assigning custodianship.
5. Specifying controls and communicating the control requirements to the custodian and users of the information.
6. Reporting promptly to the CTO about the loss or misuse of the Company information.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the CTO, where appropriate.
9. Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

Custodian: The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the Information Owner.

Responsibilities include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the Information Privacy/Security Officer for use and disclosure using that protect the privacy of the information.
5. Evaluating the cost effectiveness of controls.
6. Maintaining information security policies, procedures and standards as appropriate and in consultation with the CTO.
7. Promoting employee education and awareness by utilizing programs approved by the CTO, where appropriate.
8. Reporting promptly to the CTO about the loss or misuse of the Company information.
9. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.
10. User Management: The Company management who supervise users as defines below. User management is responsible for overseeing their employees' use of information, including:
11. Reviewing and approving all requests for their employees' access authorizations.
12. Initiating security change requests to keep employees' security record current with their
13. positions and job functions.
14. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.

15. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
16. Providing employees with the opportunity for training needed to properly use the computer systems.
17. Reporting promptly to the CTO the loss or misuse of the Company information.

18. Initiating corrective actions when problems are identified.
19. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer systems/software to manage information.

User: The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

- Access information only in support of their authorized responsibilities.
- Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.
- Refer all disclosures of protected Information (a) outside of the Company, and (b) within the Company to the CTO. In certain circumstances, the Company's policies and procedures may specifically delegate the disclosure process to other departments. (For additional information, see the Company's Privacy Policy and the Company's International Personal Data Protection Policy).
- Keep promptly to the CTO the loss or misuse of the Company information.
- Initiate corrective actions when problems are identified.

7.0 Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information.
Regardless of classification, the integrity and accuracy of all classifications of information must be protected The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format.

The following levels are to be used when classifying information:

7.1. Protected Information

Protected Information comprises all information created or received by the Company, including, without limitation, the Company.
Unauthorized or improper disclosure, modification, or destruction of this information could violate applicable laws and regulations, result in civil and criminal penalties, and cause serious damage to the Company and its clients and/or their respective business interests.

7.2. Confidential Information

Confidential Information is very important and highly sensitive material that is not classified as Protected Information. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.
Examples of Confidential Information may include: personnel information, key financial

information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.
Unauthorized disclosure of this information to people without a business need for access may violate applicable laws and regulations, or may cause significant problems for the Company, its clients, or its business partners. Decisions about the provision of access to this information must always be cleared though the Information Owner.

7.3. Internal Information

Internal Information is intended for unrestricted use within the Company, and in some cases within affiliated organizations such as the Company business partners. This type of information is already widely- distributed within the Company, or it could be so distributed within the organization without advance permission from the information owner.
Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.
Any information not explicitly classified as Protected Information, Confidential Information or Public Information will, by default, be classified as Internal Information.
Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

7.4. Public Information

Public Information has been specifically approved for public release by a designated authority within each entity of the Company. Examples of Public Information may include marketing brochures and material posted to the Company entity internet web pages.
This information may be disclosed outside of the Company.

8.0 Computer and Information Control

All Involved Systems and related information are assets of the Company and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

8.1. Ownership of Software

All computer software developed by the Company employees or contract personnel on behalf of the Company or licensed for Company use is the property of the Company and must not be copied for use at home or any other location, unless otherwise by the license agreement.

8.2. Installed Software

All software packages that reside on computers and networks within the Company must comply with applicable licensing agreements and restrictions and must comply with the Company acquisition of software policies.

8.3. Virus Protection

Virus checking systems approved by the Chief Technology Officer and Information Services must

be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

8.4. Access Controls

Physical and electronic access to Protected Information, Confidential Information and Internal Information and computing resources must be controlled. To ensure appropriate levels to access by internal workers, a variety of security measures will be instituted as recommended by the Chief Technology Officer and approved by the Company. Mechanisms to control access to

Protected Information, Confidential Information and Internal Information include (but are not limited to) the following methods:

8.4.1 Authorizations: Access will be granted on a ‘’need to know’’ basis and must be authorized by the immediate supervisor and application owner with the assistance of the CTO. Any of the following methods are acceptable for proving access under this policy:

8.4.2 Context-based access: Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The ‘’external’’ factors might include time of day, location of the user, strength of user authentication, etc.;

8.4.3 Role-based access: An alternative to traditional access control models (e.g. discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to as organization’s structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role;

8.4.4 User-based access: Security mechanisms need to grant users of a system access based upon the identity of the user.

8.4.5 Identification/Authentication: Unique user identification (user id) and authentication is required for all systems are maintain or access Protected Information, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id;

8.4.6 At least one of the following authentication methods must be implemented:

8.4.7 Strictly controlled passwords (see Exhibit A- Password Control Standards);

8.4.8 Biometric identification; and/or

8.4.9 Tokens in conjunction with a PIN.

- The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager;
- An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes);

- The user must log off or secure the system when leaving it.

o

8.5 Data Integrity

8.5.1 The Company must be able to provide corroboration that Protected Information; Confidential and Internal Information has not been altered or destroyed in an unauthorized manner.
8.5.2 Listed below are some methods that support data integrity:

1. transaction audit;
2. disk redundancy (RAID);
3. ECC (Error Correcting Memory);
4. checksums (file integrity);
5. encryption of data storage;
6. digital signatures;

8.6. Transmission Security

Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

1. integrity controls and
2. encryption, where deemed appropriate

8.7. Remote access

Access into the Company network from outside will be granted using the Company approved devices and pathways on an individual user and application basis.
All other network access options are strictly prohibited. Further, Protected Information, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the Company network.

8.8. Physical Access

Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.
The following physical controls must be in place:

8.8.1 Mainframe computer system must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage and other environmental hazards such as power outages and extreme temperature situations.

8.8.2 File servers containing Protected Information, Confidential Information and/or Internal Information must be installed in a secure area to prevent theft, destruction or access by unauthorized individuals.

8.8.3 Workstations or personal computers (PC) must be secured against use of unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which include procedures that will:

1. Position workstations to minimalize unauthorized viewing of Protected Information.
2. Grant workstation access only those who need it in order to perform their job function.
3. Establish workstation location criteria to eliminate or minimalize the possibility of unauthorized

access to Protected Information.

4. Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passer-by access to Protected Information,
5. Use automatic screen savers with passwords to protect unattended machines.

Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

1. Contingency operations – Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
2. Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
3. Access Control and Validation – Documented procedures to control and validate a person's access to software programs for testing and revision.
4. Maintenance records – documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, ad locks).

8.9. Emergency Access

Each Department is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency. Procedures must be documented to address:

1. Authorization;
2. Implementation; and
3. Revocation.

9.0 Equipment and Media Controls

The disposal of information must ensure the continued protection of Protected Information, Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain Protected Information into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

9.1 Information Disposal/ Media Re-Use of:

i. Hard copy (paper and microfilm/ fiche);
ii. Magnetic media (floppy disks, hard drives, zip disks, etc.); and
iii. CD ROM Disks

9.2 Accountability: Each entity must maintain a record of the movements of hardware and electronic media and any person responsible for those;

9.3 Data backup and Storage: When needed, create a retrievable, exact copy of electronic Protected Information before movement of equipment.

10.0 Other Media Controls

10.1 Protected Information and Confidential Information stored on external media (diskettes, CD- ROMs, portable storage, memory sticks, etc.) must be protected from theft and authorized access. Such media must be appropriately labelled so as to identify it as Protected Information or Confidential Information. Further, external media containing Protected Information and Confidential Information must never be left unattended in unsecured areas.

10.2 Protected Information and Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum-security requirements implemented:

i. Power-on passwords;

ii. Auto logoff or screen saver with password;

iii. Encryption of stored data or other acceptable safeguards approved by Chief Technology Officer.

10.3 Furthermore, mobile computing devices must never be left unattended in unsecured areas.

If Protected Information or Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of the Company's Information Security Polices and Confidentiality Statement(s) signed as a condition of employment or affiliation with the Company.

11.0 Data Transfer/Printing

Electronic Mass Transfers

11.1 Downloading and uploading Protected Information, Confidential Information and between systems must be strictly controlled.

11.2 Request for mass downloads of, or individual requests for, research purposes that include protected information must be approved by company's CTO.

11.3 All other mass downloads of information must be approved by the Information Owner and include only the minimum amount of information necessary to fulfil the request.

11.4 Appropriate Confidentiality Agreements must be in place when transferring Protected Information to external entities.

11.1. Other Electronic Data Transfers and Printing

a) Protected Information, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals.

b) Protected Information and Confidential information must not be downloaded, copier or printed indiscriminately or left unattended and open to compromise.

c) Protected Information that is downloaded for educational purposes where possible should be de-identified before use.

11.2. Other Communications

a) The company staff should be aware of their surroundings when discussing Protected Information and Confidential Information. This includes use of cellular telephones in public areas.

b) The company's staff should not discuss Protected Information or Confidential

Information in public areas if the information can be overheard.

c) Caution should be used when conducting conversations in: semi-private rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

11.3. Audit Controls

a) Hardware, software, and /or procedural mechanisms that record and examine activity in information systems that contain or use Protected Information must be implement.

b) Furthermore, procedures mast be implemented to regularly review records of information system activity, such as audit logs, reports, and security incident tracking reports. These reviews must be documented and maintained for (6) years.

11.4. Evaluation

a) The company requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic Protected Information to ensure its continued protection.

11.5. Contingency Plan

a) Control must ensure that the company can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain Protected Information, Confidential Information, or Internal Information.

a) This will include developing policies and procedures to address the following:

i. Data Backup plan:

- A data plan must be documented and be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.
- Backup data must be stored in an off-site location and protected from physical damage.
- Backup data must be afforded the same level of protection as the original data.

ii. Disaster Recovery Plan:

A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

iii. Business Continuity Plan/Emergency Mode Operation Plan:

A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or, system failure.

iv. Testing and Revision Procedures:

Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weakness and the subsequent process of revising the documentation, if necessary.

v. Applications and Data Critically Analysis:

The critical of specific applications and data in support of other contingency plan components must be assessed and documented.

12.0 Compliance

This information security Policy applies to all users of the Company information including: employees and outside affiliates.

Failure to comply with this Information Security Policy by employees and/or outside affiliates may result in disciplinary action up to and including dismissal, termination of the affiliation.

Furthermore, penalties associated with applicable laws and regulations may apply.

Possible disciplinary corrective action may be instituted for, but is not limited to, the following:

a) Unauthorized disclosure of Protected Information or Confidential Information asspecified in Confidentiality Statement.

b) Unauthorized disclosure of sign-on code (user id) or password

c) Attempting to obtain a sign-on code or password that belongs to another person.

d) Using or attempting to use another person's sign-on code password.

e) Unauthorized use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review.

f) Installing or using unlicensed software on the company computers.

g) The international unauthorized destruction of the Company information.

h) Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

Exhibit A

Password Control Standards

1.1. The Company Information Security Policy requires the use of strictly controlled for accessing Protected Information (Protected Information), Confidential Information and Internal Information. (See the Company Information Security Policy for definition of these protected classes of information.)

1.2. Listed below are the minimum standards that be implemented in order to ensure the effective of password controls.

Standards for Accessing Protected Information, Confidential Information, Internal Information

1.3. Users are responsible for complying with the following password standards:

a) Passwords must never be shared with another person, unless the person is a designated security manager.

b) Every password must, where possible, be changed regularly – (between 45 and 90 days depending on the sensitivity on the information being accessed)

c) Password must, where possible, have a minimum length of six characters.

d) Password must never be saved when prompted by any application with the exception of central single sign-on (SSO) system as approved by the CTO.

e) Password must not be programmed into a PC or recorded anywhere that someone may find and use system.

f) When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pet's, names, birthdays, etc.) A combination of alpha and numeric characters more difficult to guess.

1.4. Where possible, system software must enforce that following password standards:

a) Passwords routed over a network must be encrypted.

b) Passwords must be entered in a non-display field.

c) System software must enforce the changing of passwords and the minimum length.

d) System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15-minute timeframe.

e) System software must maintain a history of previous passwords and prevent their reuse.