©(ORGANISATION NAME)

INFORMATION SECURITY POLICY

Subject: Information Security Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 16	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	**Signature**	**Date**
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

Summary

This Information Security Policy explains why Information Security is important to CcHUB. It provides a single point of reference for the Organisation information security related policies, guidelines, and procedures.

CONTENTS

1.0 INTRODUCTION

Information security aims to protect information, information assets and ensure business continuity by preventing and minimising the impact of information security incidents. Information security provides the trusted environment that the Organisation needs to be confident in adopting efficient new ways of doing business. Information security deals with all aspects of information (spoken, written, printed, electronic or any other medium) and information handling (created, viewed, transported, stored, or destroyed).

Information will be classified and protected in a manner commensurate with its sensitivity, value, and criticality. Protection of information will apply regardless of the media where the information is stored, the systems that process it, or the transport mechanisms by which it is moved. Organisation will seek to enhance productivity of the business by reducing the probability of loss through the design and implementation of policies, standards, procedures, and guidelines that enhance the protection of business assets.

There are three basic elements to information security that must be maintained always to protect against loss, damage, and unauthorised disclosure of information:

- Confidentiality: Protecting sensitive information from unauthorised disclosure or interception.
- Integrity: Safeguarding the accuracy and completeness of information and computer software.
- Availability: Process of ensuring that authorised users have access to information and associated assets when required.

1.1 PURPOSE

The purpose of this policy is to define the requirements for information security within the Organisation, define roles and responsibilities, to provide direction for the board and senior management and establish high-level guiding principles for information security in accordance with business requirements, relevant laws and regulations, and contractual requirements.

1.2 SCOPE

This document applies and is of importance to all employees of the Organisation, including temporary Staff, external partners/vendors, and contractor personnel and other third parties. Conformance to the Information Security Policy is therefore required from the moment an employee or third parties joins or works for the Organisation until the moment he/she leaves.

The scope of this Information Security Policy includes, but is not limited to:

- All information processed by the Organisation in pursuit of all its operational activities, regardless of whether it is processed electronically or in paper form, including but not limited to:

    - Customer information
    - Operational plans, documents, and records
    - Employee records.

- All information processing facilities used in support of the Organisation's operational activities to store, process and transmit Information.
- All external Organisations that provide services to the Organisation in respect of information processing facilities.

All users must understand and adopt the use of this policy and are responsible for ensuring the safety and security of the Organisation's Information and Information assets. Violations of this policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

1.3 DEFINITIONS

- **The Organisation**: This refers to the Organisation's Name.
- **Third parties**: include contractors, vendors, external auditors, consultants, and any other person who is not an employee of the Organisation.
- **Users**: is a term inclusive of all employees of the Organisation, including temporary Staff, external partners/vendors, and contractor personnel and other third parties.
- **Information Asset** – Any information and information processing assets of value to the Organisation.
- **Information Owner** – individual accountable for the Information Asset
- **R = Responsible** = The user who does the work to achieve the task
- **A = Accountable** = The user ultimately accountable for the task or decision being made
- **C = Consulted** = The user who must be consulted prior to a decision being made and/or the task being completed
- **I = Informed** = The user who must be told when a decision is made, or work is completed

1.4 POLICY OBJECTIVES

The objective of the Information Security Policy is to protect the Organisation's information assets from accidental or intentional loss, disclosure, attack, or misuse. All reasonable measures shall be taken to ensure that:

- The Organisation's information remains confidential.
- The integrity of information is maintained.
- The Organisation's requirements for the availability of information and the systems used to process information are met.
- Accountability for information is maintained.
- All appropriate regulatory and legislative requirements are met in full.
- The Information Security Policy objectives are outlined below.

1.4.1 Ensure the confidentiality, integrity, and availability of Organisation's information assets.

1.4.2 Protect Organisation's information assets from internal and external threats.

1.4.3 Comply with applicable laws, regulations, and industry standards related to information security.

1.4.4 Manage the risk of security exposure or compromise.

1.4.5 Assure a secure and stable information technology (IT) environment.

1.4.6 Identify and respond to events involving information asset misuse, loss, or unauthorised disclosure.

1.4.7 Monitor systems for anomalies that might indicate compromise.

1.4.8 Promote and increase the awareness of information security.

2.0 INFORMATION SECURITY PRINCIPLES

2.1 Confidentiality: Information shall be accessible only to those authorised to have access. The privacy of sensitive information shall be protected.

2.2 Integrity: The accuracy, completeness, and consistency of information and processing methods shall be safeguarded over the entire life cycle.

2.3 Availability: Authorised users shall have reliable and timely access to information and associated assets when required.

2.4 Risk Management: Information security risks shall be identified, assessed, and prioritised, and appropriate controls shall be implemented to mitigate or transfer those risks.

2.5 Least Privilege: Access and permissions shall be granted at the minimum level necessary for users to perform their assigned duties.

2.6 Separation of Duties: Roles and responsibilities for critical functions shall be divided among multiple individuals to prevent any single person from compromising a critical process.

2.7 Defence in Depth: Multiple layers of security controls shall be implemented to protect information assets, ensuring that if one control fails, there are other controls in place to prevent a breach.

2.8 Continuous Monitoring and Improvement: The effectiveness of security controls shall be continuously monitored and evaluated, and improvements shall be made as necessary to address evolving threats and vulnerabilities.

2.9 Security Awareness and Training: Security awareness shall be promoted, and regular training shall be provided to all employees, contractors, and third-party users to ensure they understand their roles and responsibilities in protecting information assets.

2.10 Incident Management: Processes for detecting, reporting, and responding to security incidents shall be established to ensure timely and effective response.

2.11 Compliance: Compliance with applicable laws, regulations, and industry standards related to information security shall be ensured.

2.12 Accountability: Individuals shall be held accountable for their actions, and they shall understand their responsibilities for protecting information assets.

2.13 Data Classification and Protection: Information assets shall be classified based on their sensitivity and criticality, and appropriate protection measures shall be implemented for each classification level.

- These principles provide a foundation for an effective information security program and help ensure that appropriate controls and measures are in place to protect an Organisation's information assets.
- The Information Security Policy sets out supporting policies and standards intended to help the Organisation achieve these objectives.
- Compliance with this Information Security Policy is necessary to ensure business continuity, and minimise business damage by preventing the occurrence, and minimising the impact, of information security incidents.
- Breaches of the Information Security Policy and any supporting policies, or who knowingly or negligently allows employees or contractors under their supervision to do so will be subject to disciplinary action and up to termination of employment.

2.1 RISKS

Lack of, or failures in, information security can lead to incidents such as breach of the confidentiality of information, damage to its integrity, or issues surrounding its availability, which could lead to direct financial loss, damage to the Organisation's reputation and/or breach of regulatory standards or the law.

3.0 ROLES AND RESPONSIBILITIES

3.1 EXECUTIVE MANAGEMENT

Executive Management shall:

3.1.1 Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of the Organisation.

3.1.2 Ensure that information security processes are integrated with the Organisation's strategic and operational planning processes to secure its mission.

3.1.3 Ensure that adequate financial and personnel resources for information security are included in the budgeting and financial planning processes.

3.1.4 Ensure that the Security Team is given the necessary authority to secure the Information Resources under their control within the scope of the Organisation's Information Security Program.

3.1.5 Designate an Information Security Officer and delegate authority to that individual to ensure compliance with applicable information security requirements.

3.1.6 Evaluate and accept risk on behalf of the Organisation.

3.1.7 Identify information security responsibilities and objectives and integrate them into relevant Organisational processes.

3.1.8 Support the consistent implementation of information security policies, standards, and procedures.

3.1.9 Demonstrate leadership and commitment to information security by providing clear direction and allocating appropriate resources.

3.1.10 Promote awareness of information security best practices through the regular dissemination of materials provided by the Information Security Officer (ISO) or designated security representative.

3.1.11 Implement the process for determining the classification and categorization of information assets, based on industry-recommended practices, Organisational directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information.

3.1.12 Implement the process for the identification, handling, use, transmission, and disposal of information assets based on their classification and categorization.

3.1.13 Designate information owners and hold them accountable for maintaining the confidentiality, integrity, and availability of the data under their purview.

3.1.14 Participate in the response to security incidents.

3.1.15 Ensure compliance with notification requirements in the event of a breach of private or sensitive information.

3.1.16 Adhere to specific legal and regulatory requirements related to information security.

3.1.17 Communicate legal and regulatory requirements to the Information Security Officer (ISO) or designated security representative.

3.1.18 Communicate the requirements of information security policies and associated standards, including the consequences of non-compliance, to the workforce and third parties, and address adherence in third-party agreements.

3.2 THE INFORMATION SECURITY OFFICER (ISO)/DESIGNATED SECURITY REPRESENTATIVES

ISO/designated security representative shall:

3.2.1 Chair the Information Security Committee and provide updates on the status of the Information Security Program to Executive Management.

3.2.2 Manage compliance with all relevant statutory, regulatory, and contractual requirements pertaining to information security.

3.2.3 Participate in security-related forums, associations, and special interest groups to stay abreast of industry best practices and emerging threats.

3.2.4 Assess risks to the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of the Organisation.

3.2.5 Facilitate the development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.

3.2.6 Ensure that the Organisation has trained all personnel to support compliance with information security policies, processes, standards, and guidelines. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities.

3.2.7 Ensure that appropriate information security awareness training is provided to Organisation personnel, including contractors.

3.2.8 Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the Organisation’s information security policies, procedures, and practices.

3.2.9 Develop and implement procedures for testing and evaluating the effectiveness of the Organisation 's Information Security Program in accordance with stated objectives.

3.2.10 Develop and implement a process for evaluating risks related to vendors and managing vendor relationships pertaining to information security.

3.2.11 Report annually, in coordination with the Information Security Committee, to Executive Management on the effectiveness of the Organisation’s Information Security Program, including progress on remedial actions.

3.2.12 Maintain familiarity with the Organisation’s business functions and requirements as they relate to information security.

3.2.13 Maintain an adequate level of current knowledge and proficiency in information security through the acquisition of annual Continuing Professional Education (CPE) credits directly related to the field.

3.2.14 Advise on security issues related to the procurement of products and services to ensure alignment with the Organisation’s security requirements.

3.2.15 Escalate security concerns that are not being adequately addressed in accordance with the established reporting and escalation procedures.

3.2.16 Disseminate relevant threat information to appropriate parties within the Organisation.

3.2.17 Participate in the response to potential security incidents.

3.2.18 Promote information security awareness through the development and delivery of awareness programs and training initiatives.

3.3 IT MANAGEMENT

IT Management shall:

3.3.1 Support information security by providing clear direction and ensuring the consideration of security controls in the data processing infrastructure and computing networks which support the information owners.

3.3.2 Provide the resources needed to maintain a level of information security control consistent with the Organisation's information security policies and standards.

3.3.3 Identify and implement all processes, policies, and controls relative to the security requirements defined by the business and the Organisation's information security policies.

3.3.4 Implement the proper controls for information assets based on their defined classification and categorization.

3.3.5 Provide training to appropriate technical staff on secure operations, including but not limited to secure coding and secure system configuration.

3.3.6 Foster the participation of information security and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures.

3.3.7 Implement and maintain business continuity and disaster recovery plans to ensure the resilience and availability of critical information systems and assets.

3.4 HUMAN RESOURCES

Human Resources shall:

3.4.1 Conduct thorough background checks and screening processes for potential new hires to mitigate insider threats.

3.4.2 Verify employment history, credentials, and references to ensure the trustworthiness of new employees.

3.4.3 Ensure that the Organisation's HR practices and procedures comply with relevant security regulations and industry standards.

3.4.4 Promote a security-conscious culture within the Organisation.

3.4.5 Ensure that security policies are clearly communicated to all employees and enforced consistently across the Organisation.

3.5 ALL EMPLOYEES, CONTRACTORS, AND OTHER THIRD-PARTY PERSONNEL

All Employee, Contractors, and Other Third-Party shall:

3.5.1 Understand their responsibilities for complying with the Organisation's Information Security Program.

3.5.2 Formally acknowledge and agree to abide by all applicable information security policies, standards, and guidelines that have been established.

3.5.3 Use the Organisation's Information resources in compliance with all Information Security Policies.

3.5.4 Seek guidance from the Information Security Team for any questions or issues related to information security.

3.5.5 Develop an understanding of the baseline information security controls necessary to protect the confidentiality, integrity, and availability of the information entrusted to them.

3.5.6 Protect information and resources from unauthorised use or disclosure.

3.5.7 Safeguard personal, private, and sensitive information from unauthorised use or disclosure.

3.5.8 Report suspected information security incidents or weaknesses to the appropriate manager and the Information Security Officer (ISO) or designated security representative.

3.6 POLICY STATEMENT

The Organisation shall ensure that:

- Information assets and information processing facilities shall be protected against unauthorised access.
- Information shall be protected from unauthorised disclosure.
- Confidentiality of information assets shall be a high priority.
- Integrity of information shall be maintained.
- The Organisation's requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities shall be met.
- Statutory, and expressed and implied legal obligations shall be met.
- Unauthorised use of information assets and information processing facilities shall be prohibited.
- Obscene, offensive, or damaging statements shall be dealt with in accordance with other policies published by the Organisation.

- This Information Security Policy shall be communicated to all users for whom information security training shall be given.
- All breaches of information security, actual or suspected, shall be reported and investigated in line with the Organisation's published policies.
- Controls shall be commensurate with the risks faced by the Organisation. In support of this Information Security Policy, more detailed security policies, processes, and standards shall be developed.

4.0 TOPIC-SPECIFIC POLICIES

4.1 The Organisation shall develop and maintain topic-specific policies and procedures to address various aspects of information security, including but not limited to:

- Onboarding/Off-boarding policy
- Acceptable Use policy
- Access Control policy
- Anti-Malware/Anti-Virus guidelines
- Asset Inventory template
- Asset Management policy
- Backup policy
- Bring Your Own Device policy.
- Change Management policy.
- Data Protection policy
- Disaster Recovery policy
- Disposal (data and asset) policy
- Email policy
- Encryption policy
- Hardening/Baseline standards
- Incident Management policy
- Information Security policy
- Network Security policy
- Patch Management policy
- Record Retention policy
- Risk Assessment policy
- Risk Register Template
- Travel policy (Remote Access/VPN)

5.0 POLICY COMPLIANCE

5.1 Compliance with this policy and related topic-specific policies is mandatory for all parties outlined in Section 1.1 - Scope.

6.0 POLICY REVIEW AND UPDATES

6.1 This policy shall be reviewed and updated annually, or as needed, to ensure its continued effectiveness and alignment with industry best practices and regulatory requirements.

7.0 RECOMMENDATIONS/ADVISORY ON INFORMATION SECURITY

Organisations with 1 – 5 Employees	Organisations with 6 – 20 Employees	Organisations with more than 20 Employees
• Implement a reliable backup strategy, such as using cloud-based backup solutions or external storage devices, to ensure data can be recovered in case of a security incident or data loss. • Use strong passwords, multi-factor authentication (MFA), and least-privilege access controls to limit access to sensitive information and systems. • Implement SSL/TLS encryption, regularly update content management systems (CMS) and plugins and conduct vulnerability scans. https://letse.ncrypt.org/ • Educate all employees on cybersecurity best practices, such as	• Implement Role-Access Based Controls like https://www.manageengine.com/network-configuration-manager/role-based-access-control-RBAC.html SolarWinds. https://www.solarwinds.cam/access-rightsmanager/use-cases/role-based-access-control • Perform regular risk assessments to identify potential vulnerabilities and threats to your Organisation's information assets and develop mitigation strategies accordingly. • Implement advanced security solutions such as firewalls, intrusion detection/prevention systems (IDS/IPS), and security information and event management (SIEM) tools to protect your network and systems.	• Deploy security monitoring and logging tools to monitor and analyse security events, detect potential threats, and provide visibility into your Organisation's security posture. • Establish and regularly test business continuity and disaster recovery plans to ensure that your Organisation can maintain critical operations in the event of a security incident or other disruption. • Implement logging and monitoring mechanisms to track all remote access activities. Tools like Splunk https://www.splunk.com/ or ELK Stack https://www.elastic.co/elk-stack

recognizing phishing attempts, secure handling of sensitive data, and reporting suspicious activities.	https://www.solarwinds.com/security-event-manager	• Deploy DLP solutions to monitor and protect sensitive data from unauthorised access or disclosure, both within your Organisation and when data is shared with third parties. https://www.forcepoint.com/product/dlp-data-loss-prevention