©(ORGANISATION NAME)

ONBOARDING/OFF-BOARDING POLICY

Subject: Onboarding/Off-boarding Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 8	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

CONTENTS

1.0 OVERVIEW

Information security is very important to help protect the interests and confidentiality of the Organisation and its customers. Information security cannot be achieved by technical means alone, it must also be enforced and applied by people, and this policy addresses security issues related to employees of the Organisation.

2.0 PURPOSE

The purpose of this policy is to set out the processes and responsibilities that are necessary to ensure that the employees of Organisation contribute to the security of its information and information assets from their entry to exit from the Organisation.

3.0 OBJECTIVES

The objective of this policy is:

- To ensure that all employees understand their responsibilities and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud, or misuse of the Organisation's information facilities.
- To maintain the security of the Organisation's information and information systems that are accessed, processed, communicated to, or managed by third parties.
- To ensure that all users are aware of information security threats and concerns, their responsibilities, and liabilities, and are equipped to support the Organisation's security policy in the course of their normal work, and to reduce the risk of human error.
- To ensure users exit the Organisation or change employment in a secure manner.

4.0 POLICY DETAILS

Human resources security responsibilities shall be addressed prior to employment, during employment, change of employment and termination and this will be included in contracts and monitored during an individual's employment. To fulfil this policy, the following statements shall be adhered to:

All employees must comply with the information security policies of the Organisation. Any information security incidents resulting from non-compliance will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

4.1 PRIOR TO EMPLOYMENT

- Background verification checks on all candidates for employment must be carried out in accordance with relevant local laws, regulations and ethics and are proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
- The terms and conditions of employment shall include requirements for compliance with information security policies.
- A written undertaking shall be obtained from agencies (outsourced parties) providing temporary employees that appropriate character and business references have been obtained for such employees.
- The employment contractual agreements with employees and contractors shall clearly state their responsibilities and the Organisation's responsibilities towards information security practices and must agree to follow the information security policies of the Organisation.
- Indemnity Clauses relating to restitution to the Organisation in instances of negligence by an employee from agencies (outsourced parties) shall be included in the contracts.
- Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important.
- Contractors shall not be allowed in sensitive areas (e.g., computer rooms), without supervision and authorisation.
- IT resources (Laptop/phone/email access/ access card, etc.) shall be set up for new employees. Communicating login credentials securely to the new joiner/employee directly to their personal email for account activation and change of password is very important.
- A workspace shall be set up ahead of prospective employee resumption.
- An Orientation session shall be organised for the prospective employee in line with the Human Resources Training plan for new hires.

4.2 DURING EMPLOYMENT

- All new employees shall attend the mandatory information security awareness training as part of induction before being granted access to the network or systems. When employees change jobs, their information security needs must be reassessed, and any new training provided a priority.
- Temporary employees shall not be granted access to the network or authorised to use any systems except office productivity tools without the approval of the CISO.
- All employees and contractors shall be required to apply information security in accordance with the established policies and procedures of the Organisation.

- All employees and contractors of the Organisation shall receive appropriate awareness, training and regular updates in Organisational policies and procedures, as relevant for their job function.
- The Organisation shall provide an overview of the company's history, culture, values, and mission to the employee.
- There shall be a formal and communicated disciplinary process in place to act against employees who have committed an information security breach.
- Employee's compliance with information security policies shall be monitored.
- Management shall ensure that policies are complied with, through regular review and monitoring.
- End-users shall be fully trained in the correct use of IT facilities including logon procedures, use of software packages, etc. before they are given access to the IT facilities, to reduce the likelihood of errors.
- Managers shall monitor the work performance of the employees and hold periodic appraisals to identify training needs and to discover any problem areas, particularly where employees deal with sensitive information or work on sensitive computer applications.
- Employees shall receive training in emergency procedures, first aid treatment and the use of fire fighting and other emergency equipment.
- All employees shall be educated on business continuity.
- The disciplinary process for employees shall include sanctions (which may include dismissal) for employees who violate the Organisation's information security policies and procedures. This will be developed by the CISO in collaboration with the Human Resources Department and approved by the board.

4.3 TERMINATION AND CHANGE OF EMPLOYMENT

- An employee resigning from the Organisation shall send a copy of his/her resignation to the Human Resource Department who shall notify Information Technology
- Departing employees must return all information assets and equipment belonging to the Organisation, unless agreed otherwise with the designated owner responsible for the information asset.
- Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced.
- The Organisation shall ensure proper notification and communication with the departing employee and relevant stakeholders.
- The Organisation will facilitate knowledge transfer from the departing employee to their successor or team members.

- All access to company systems, applications, and facilities (disable accounts, retrieve keys, etc.) must be revoked and company-issued assets (laptop, mobile devices, company credit cards, etc.) will be retrieved.
- An exit interview shall be conducted to gather feedback, address concerns, and understand the reasons for departure and use the feedback to identify areas for improvement in the Organisation's processes or culture.