## AMENDMENTS LOG

**Revision History**

| Version | Revision Author | Reviewer / Approver | Date | Summary of Changes |
|---|---|---|---|---|
| 1.0 | Nor Asfiah Binte Jamalludin<br>(ISMS MR) | James Chia<br>(CEO) | 1 Aug 2025 | Initial Release |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## TABLE OF CONTENTS

## PURPOSE

This document sets out a procedure to be used when applying the appropriate level of screening to the recruitment process, and controls for employee onboarding and exit management with the intention to minimise the risk to the organization arising from accidental or deliberate malpractice in the role and/or after employment.

## SCOPE

This screening procedure should be used for any candidate that has been selected and prior to being onboarded.

The exit management section of this procedure should be used prior to and/or on the last day of employment.

This procedure may also apply to contract staff and interns or trainees or freelancers, where appropriate.

## REFERENCE

| | |
|---|---|
| ISO/IEC 27001 Standard | Annex A 6.1 Screening |
| | Annex A 6.2 Terms and conditions of employment |
| | Annex A 6.5 Responsibilities after termination or change of employment |
| | Annex A 6.6 Confidentiality or non-disclosure agreements |
| | Annex A 5.10 Acceptable use of information and other associated assets |

## RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this procedure.

The HR function is responsible to ensure that all prospective employees of the organization have gone through appropriate screening process prior to employment, and that those who are exiting are managed accordingly.

The Management Representative (MR) is responsible for ensuring information security awareness, education and training within the organisation.

## PROCEDURE

### A. SCREENING

The recruitment process will have relevant job descriptions provided for the role, and advertising and interviewing of applicants will take place in a manner appropriate to the role. The preferred candidate will provide information in support of his or her application.

The purpose of screening is to ensure that necessary information provided by the candidate can be verified before employment. The specific screening activities that should be applied in any particular case will depend on a number of factors including the following:

- The classification of information they will have access to
- If the role will have access to financial assets
- If the role will have access to personal data
- The level of potential to cause harm to the organization
- Level of involvement in technology

A judgement must be made in each case about the levels of screening to be applied. This should reach a balance between being rigorous enough to protect the organization without being overly time-consuming.

Consensus from the candidate must be obtained prior to conducting the required verification check. Screening checks carried out and their results shall be recorded.

The table below provides initial guidance regarding the screening checks available and the criteria that may be used in deciding whether to apply them. The following screening checks should be used in the circumstances stated.

| **Screening check** | **Criteria for selection** | **Task to be completed** |
|---|---|---|
| Proof of Identity & Proof of Right to Work | In all cases | Verification of original passport (for foreigners) / NRIC / WP / EP / S Pass |
| Education Check and Relevant Professional Qualifications (necessary for the role) | In all cases | All qualifications that have a bearing on the ability to perform the role or are pre-requisites should be checked for accuracy and completeness<br>Where verification proof requirements for Employment Pass / S Pass application is required for foreigners, a background screening company as declared in the MOM website has to be engaged for educational qualification verification. |
| Work History Verification | Except for those with no past employment history | Previous employment payslip or referral letter/testimonial or certificate of employment from previous employment (preferably the most recent |

| Screening check | Criteria for selection | Task to be completed |
|---|---|---|
| | | employment or within the last 3 years)<br>Where verification proof requirements for Employment Pass / S Pass application is required for foreigners, a background screening company as declared in the MOM website has to be engaged for employment record verification. |

Where a candidate is hired via a third party or staffing agency, evidence may be obtained from the agency that the above screenings / reference verifications had been carried out.

Department head shall advise if the candidate is selected for the position subject to favourable results of screening checks and pre-employment medical examination as may be required. The *ISMS-PPL-01-F1 New Hire Checklist* will be completed to document the screening done and relevant information / documentation obtained or completed for the new hire.

## B. TERMS & CONDITIONS OF EMPLOYMENT

Employment agreements shall state applicable information security responsibilities. This will be through:

- A confidentiality clause added into the contract and requiring the personnel to sign a separate non-disclosure agreement (NDA) prior to being given access to information and other associated assets;
- Acknowledgment of the applicable information security policies and acceptable use including legal responsibilities and rights such as regarding copyright laws, intellectual property rights or data protection *(refer to ISMS-PPL-01-F2 Acknowledgment of Information Security Policies and Rules)*

The management shall ensure that personnel agree to the terms and conditions concerning information security and must continue to keep in strict confidence and not divulged to any third parties without proper authorization any confidential information accessed by the personnel in the course of their employment and even after their employment has ended.

It shall be explained to the personnel during their onboarding that they are required to comply with all applicable information security policies and procedures in force during the period of their employment, and failure to comply may result in disciplinary action being taken in accordance with the organisation's *ISMS-PPL-03 Information Security Disciplinary Process.*

The employment agreements and policy acknowledgment shall be retained inside the employee file.

## C. ONBOARDING

HR shall ensure that policies for information security have been read and understood, and have been acknowledged by the new hire.

HR shall notify IT via email for laptop issuance and account setup for the new joiner prior to start date. Request for access to other company systems and applications, if necessary for the role, shall be submitted by the department head to the respective System Administrator.

Issuance of company assets and access shall be recorded through *ISMS-PPL-01-F3 Company Assets & Access Issuance.*

Induction and competency planning for the new hire shall be carried out in line with *ISMS-PPL-02 Awareness & Competence Development.*

## D. EXIT MANAGEMENT

On the employee's last day, HR shall ensure that Exit Checklist is completed to confirm that the employee has returned all assets issued to him/her, and acknowledged applicable information security obligations even after their employment has ended.

HR shall notify IT via email about the existing employee prior to last day unless it is an unfriendly termination and therefore must be prioritised by IT for asset return and access removal. For such exceptions, HR must notify IT as soon as the termination date has been confirmed. Removal of access to other company systems and applications, if any has been provided previously to the exiting employee, shall be submitted by the department head to the respective System Administrator so it can be removed on the employee's last day as well.

Completion of the recovery of assets and access removal shall be documented in the *ISMS-PPL-01-F4 Exit Checklist.*

## FORMS

| | |
|---|---|
| ISMS-PPL-01-F1 | New Hire Checklist |
| ISMS-PPL-01-F2 | Acknowledgment of Information Security Policies and Rules |
| ISMS-PPL-01-F3 | Company Assets and Access Issuance Form |
| ISMS-PPL-01-F4 | Exit Checklist |