Human Resources Security Policy

Purpose

Prior to employment, to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. During employment, to ensure that employees and contractors are aware of and fulfill their information security responsibilities. At termination or change in employment, to protect Hirexa's interests as part of the process of changing or terminating employment.

Scope

This policy applies to all with access to Hirexa's information and assets

Policy Statements

Screening to be performed prior to entering a working relationship with Hirexa or its Clients.

All new employees and contractors are to be screened. The screening must be conducted in accordance with the Human Resource Policies of Hirexa or its Clients. The screening must include verification of:

- *Academic*
- *Address,*
- *Previous employment,*
- *and Criminal Check.*
- *Additional Checks or specific check requests if any by the Clients will be done accordingly.*

All Employees and Contractors are to be made aware of Hirexa's Information Security Policy.

The terms and conditions for employees and Contractors of Hirexa in accordance with the Employee and Contractor Agreement accordingly to be signed which include:

- *NDA*
- *Privacy*
- *Confidentiality*
- *Code of Conduct/Ethics & Acceptable Usage*

HRD/Onboarding Team to ensure that the terms and conditions of employment or contract Agreement are agreed to by the Employees and Contractors.

HRD Team to ensure that Employees and Contractors apply security in accordance with standards, policies and procedures.

HRD Team to support Hirexa's information security objectives by:

- *Briefing all Employees and Contractors on their security roles and responsibilities prior to granting access to sensitive data and systems;*
- *Ensuring all Employees and Contractors have access to these Information Security Standards; and*
- *Ensuring all Employees and Contractors conform to the terms and conditions of employment or contract agreement.*
- *Employees and Contractors to be made aware of reporting of wrongdoings.*

Employees and Contractors are to be given appropriate information security training and be informed of changes to standards, policies and procedures.

HRD Team to include an information security awareness component during orientation for new Employees and Contractors. Ongoing awareness training to be conducted. Among the topics that must be discussed are:

- *Safeguarding information;*
- *Legal responsibilities;*
- *Information security standards, policies, directives and guidelines;*
- *How to report information security events;*
- *Appropriate use of information and assets;*
- *Related disciplinary processes;*

A disciplinary process to be in place to take action against employees who have committed an information security breach.

When it is determined that an employees and contractors was responsible for a security breach or a violation of standards or policies, the Information Security Branch must notify the appropriate Information Security Officer in charge or Head of HR

Appropriate Officer to review details of the incident, consider disciplinary action if warranted and arrange for permanent or temporary removal of access privileges when appropriate.

HRD Team in association with IT Team to advise Employees and Contractors of their information security responsibilities when employment changes or is terminated.

Terminated employees and contractors must be made aware of:

- *Security requirements including the need to not disclose sensitive information;*
- *Legal responsibilities;*
- *Responsibilities described in confidentiality or non-disclosure agreements; and any other applicable policy, standards, or contract.*