Your Organization Logo Here

Organization XYZ Personnel Security Policy

1.0 Purpose

All corporate assets must be adequately protected. Personnel security is a necessary building block for safeguarding assets.

This policy defines requirements for protection of Organization XYZ's corporate assets from intentional abuse, misuse, or destruction by employees, contractors, or consultants.

2.0 Scope

This policy applies to all employees, contractors, and consultants who handle Organization XYZ's assets including sensitive information or sensitive information entrusted to Organization XYZ.

3.0 Policy Statement

Asset protection is addressed at the recruitment stage, included in the employee handbook and contracts, and monitored during an individual's employment. To ensure compliance with policy objectives, these statements must be followed:

3.1 Requirement to Protect Corporate Assets

3.1.1 All employees, contractors, and consultants must protect both tangible and intangible corporate assets.

3.1.2 All employees, contractors, and consultants are responsible for reporting to the appropriate manager any real or suspected threats to corporate assets.

3.2 Information Security Responsibilities in Employee Handbook & Contracts

Include information security responsibilities in company rules and worker's contracts.

3.2.1 Information security responsibilities to be followed by all employees must be incorporated into Organization XYZ's Employee Handbook.

3.2.2 All employees must acknowledge in writing (electronic acknowledgement is acceptable) that they have read and understood Organization XYZ's Employee Handbook.

3.2.3 Specific information security responsibilities must be incorporated into all contracts with contractors (including consultants or any non-employee who performs work-for-hire) who have access to restricted, customer or otherwise sensitive information.

3.3 Information Security Training

Ensure all employees, contractors, and consultants are aware of information security policies and processes.

mmenninger@runbox.com

3.3.1 All employees, contractors, and consultants must be trained in the security requirements and processes associated with their jobs, appropriate business controls, and the correct use of IT systems and facilities before they are granted access to IT systems and facilities.

3.3.2 All employees, contractors, and consultants must acknowledge in writing (electronic acknowledgement is acceptable) that they have read and understood Organization XYZ's Information Security Policy.

3.3.3 All employees, contractors, and consultants must receive refresher training on Organization XYZ's Information Security Policy at least once per year.

3.4 Background Checks

Screen all potential employees and contractors to minimize the risk of attacks from internal sources.

3.4.1 All employees, contractors, and consultants must pass a background check that includes examination of criminal conviction records, credit bureau records, and verification of previous employment.

3.5 Bonding

Insure the organization against acts of disloyalty such as fraud, embezzlement, and industrial espionage.

3.5.1 All employees, contractors, and consultants must be surety bonded for a minimum of $1,000,000.

3.6 Conflict of Interest

Require employees to identify any conflicts of interest to minimize acts that may harm the organization’s assets or reputation.

3.6.1 All employees must be trained to recognize conflicts of interest and the appearance of conflicts of interest during their first week of employment and at least once per year thereafter.

3.6.2 All employees must identify in writing any conflicts of interest and the appearance of conflicts of interest during their first week of employment and at least once per year thereafter.

3.6.3 All conflict of interest statements must be reviewed by the Security Compliance Officer and subsequently filed in the employee’s HR files.

3.6.4 If the Corporate Compliance Officer identifies any significant conflicts of interest, the conflict(s) must be discussed with the employee’s supervisor or other management to determine the appropriate course of action.

3.7 Non-Disclosure Agreements

Prevent the disclosure of sensitive information to anybody who has not signed a non-disclosure agreement.

3.7.1 All employees, contractors, and consultants must personally sign an Organization XYZ non-disclosure agreement. The provision of a signature must take place before work begins, or if a worker has been working without a non-disclosure agreement, a signature must be provided as a condition of continued employment.

3.8 Security Incidents

Ensure security incidents and policy violations are escalated appropriately.

3.8.1 The Chief Security Officer will implement a system for security incident reporting, response, tracking, and resolution.

3.8.2 All employees and contractors are responsible for reporting to the appropriate manager any violations of policy or other directives promptly.

4.0 Responsibilities

4.1 Human Resources is responsible for ensuring background checks and employee bonding are conducted.

4.2 Corporate Security and Corporate Training are responsible for implementing the educational requirements of this policy.

5.0 Compliance

5.1 Company officers and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

5.2 Company line managers have the responsibility to enforce compliance with this policy.

5.3 Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

6.0 Definitions

{This section intentionally left blank}

7.0 Related Policies and Standards

- Corporate Security Policy
- Information Security Policy

8.0 Revision History

Version	Date	Revision
1.0	Month Day, Year	Policy Approved by Board

mmenninger@runbox.com