IT Threat & Risk Assessment

Version 3.0

12th February 2020

Document History

Created by:	Eddy Lareine
Approved by:	Areff Salauroo

Release date	Version	Change Details	Reviewed by
22.10.19	1.0	Submitted for review	Legal Advisor
12.11.19	2.0	Apply changes submitted by legal advisor	Eddy Lareine
12.02.20	3.0	Submitted for review	Areff Salauroo

Table of Contents

IT THREAT & RISK ASSESSMENT

1.0 Objective

The objective of this policy is to evaluate the Information Technology systems and network for threats and vulnerabilities in order to protect the company Information Technology assets and reduce the Company’s risk.

2.0 Scope

To describe a procedure for identifying potential threats to the Company’s information technology assets (Information Technology assets) and assessing threats on the basis of probability and risk.

This policy applies to all Company Information Technology assets, including the Information Technology network.

3.0 Policy Description

3.1 IT Threat & Risk Assessment - Introduction

In order to prepare for threats to its Information Technology assets and infrastructure, the Company must be aware of the types of threats that exist, the likelihood that they will occur, their potential impact, and the risk these threats may pose to the Company.

Threats may be natural or manmade. Natural threats include floods, storms, and earthquakes. Manmade threats may be accidental or intentional. Examples of manmade threats include use of unauthorized hardware or software and having unauthorized access to Company systems.

Intentional threats exist both outside the Company and within.

The risk posed by any given threat is a function of the combined likelihood of the threat occurring and the impact it would have on the Company’s assets (hardware, software, data, network/infrastructure, and personnel) if it were to occur. While risk to Company Information Technology assets cannot be completely eliminated, the Company must make all reasonable efforts to minimize risk. Those efforts should begin with assessing threats and risks.

3.2 IT Threat Assessment Preparation

In advance of conducting a threat assessment of any of the Company's Information Technology systems, the IT Manager shall establish a baseline for assessment, identifying systems to be assessed (accounting, HR, sales, etc.) and determining their interconnectivity with other systems.

The IT Manager should identify and describe threats that may target the Information Technology assets and systems under consideration by one or more of the following means:

- Periodically (at least once a month) reviewing access control log for threat occurrences, such as unauthorized system access;
- Reviewing Information Technology incidents for trends and/or patterns, in accordance with procedure IT INCIDENT HANDLING;
- Reviewing any system test (test script, test procedures, expected results, etc.) for vulnerabilities testing;
- Conducting penetration testing at irregular intervals, to verify the Information Technology network's ability to withstand intentional attempts at circumventing Information Technology security

The IT Manager may acquire additional information for developing the assessment baseline by routinely reviewing threat alerts and bulletins from vendors, standards organizations, etc.

To determine if the Company needs to act on any given threat and to what extent it should act, the IT Manager shall classify threats/ vulnerabilities in the following manner:

- Threat likelihood may be categorized as:
  a. Low – the threat is unlikely to occur.
  b. Medium – the threat may occur.
  c. High – the threat is likely to occur.
- The impact of threats, in the absence of protection, and the possible or likely consequences of each. Threat impact may be classified as:
  a. Low – the threat may result in minimal loss of Company assets/resources;
  b. Medium – the threat may result in a significant loss of Company assets/ resources, harm the Company's mission or interests, or result in injury to an employee; and
  c. High – the threat may result in a very costly loss of Company assets/ resources, significantly harm the Company's mission, interests, or standing, or result in serious or fatal injury to an employee.
- An exposure rating or risk assessment shall be based on likelihood and impact ratings. A risk matrix is prescribed (Figure 1), with likelihood running from low to high along one axis and impact running from low to high on the other axis. The resulting exposure rating/risk assessment shall be used to prioritize threats (Figure 2).
  a. High-risk threats require the highest security levels and present the greatest need for immediate action, if existing security tools and techniques are inadequate.

b. Low-risk threats may require little or no response on the part of the Information Technology Manager.

	Impact	Low	Medium	High
Likelihood	High	Low	Medium	High
	Medium	Low	Medium	Medium
	Low	Low	Low	Low

Figure 1 – Risk Matrix

Risk Level	Description and Actions
High	Preventive actions are required and a preventive action plan shall be developed and implemented as soon as possible.
Medium	Preventive actions are required and a plan to incorporate those actions within a reasonable time frame shall be developed.
Low	IT Management should confer with managers of affected systems to determine if preventive action is required or if risk is acceptable.

Figure 2 - Threat Priority

3.3 IT Threat & Risk Assessment

At regular intervals (once a year, at least), the IT Manager shall conduct a threat/vulnerability scan of the Information Technology network. This scan should be performed using commercially available software designed expressly for the purpose.

The IT Manager shall;

- review scan results and analyze the findings in order to determine if the Company needs to act on them and to what extent.
- create a THREAT ASSESSMENT REPORT, summarizing assessment findings and containing the following information, at a minimum:
  - Systems reviewed;
  - Number of threats found this period and last; and
  - A summary of identified threats.
- submit the TREAT ASSESSMENT REPORT to the Management

In case there is a breach, the IT Manager and/or the Systems & Network Administrator will inform

- the management about the impact and the remediation.
- the employees, and hence, what are the procedures to follow depending of the cause and the impact.

- the third party, if the cause is from the latter, and hence, remove all his access temporarily until the breach has been tackled. Afterwards, will discuss on new protocols with the third party before access is granted again (if need be).

3.4 IT Threat Management Review

The Information Technology Security Manager shall periodically review the risk assessment process to ensure its continued timeliness and applicability.

Any time a significant implementation, revision, etc., takes place, the Information Technology Manager shall review the risk assessment process, to ensure existing controls are applicable to such changes or if improved controls are required.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Employee Declaration

I have read and I understand the IT Threat Management Policy and its related contents. I understand that I must comply with the instructions and guidelines given therein and if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

Name : ____

Signature : ____

Date : ____

IT THREAT/RISK ASSESSMENT REPORT

Date: ______________________

Systems Reviewed: ____

____

Threats found this period: _____________________________

Description: ____

____

____

Threats found last period: _____________________________

Description: ____

____

____

Threat Summary:

Risk Level	Number	Description
LOW		
MEDIUM		
HIGH		

IT Manager: ……………………………………………………………..