Trackon Canada Private Limited
Vulnerability Management
Policy and Procedures

Version Number: 1.1

Last Updated: July 2022

Next Update: January 2023

Approved By:

Senior Officer Approval for Program:

Table of Contents

1 Policy Statement

1.1 Our Commitment

Reading this policy and our all-staff procedure is currently required for all new hires. An attestation confirming that the policy and procedure are read and understood is kept as a training record. There are also separate training materials for staff, which include quizzes designed to test the effectiveness of training.

2 Vulnerability Identification

Vulnerability is defined as a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. The input to this stage will come from the Security Incident report, Performance Evaluation Procedure, and vulnerability assessment. The vulnerability value is expressed on a scale of 1-3 which is directly proportional to the existing controls in place and defined.

Rating	Meaning
1 (Low)	A vulnerability that has minimal impact and holds lower chances of being exploited.
2 (Medium)	A vulnerability that if exploited will affect the organization's operations and will have financial/ regulatory consequences. These vulnerabilities can be exploited with some effort.
3 (High)	A vulnerability, which, if exploited would significantly compromise asset security (confidentiality, integrity, and availability), potentially allowing access to confidential/ restricted information assets, or could compromise the asset completely.

2.1 Threat Identification

A threat is the potential cause of an unwanted event that may result in harm to the organization and its assets. The threat can take many forms and to assess a threat, it is important to consider all potential threat sources that could cause harm to an IT system and its processing environment. Threat identification depends on the physical location of the facility, the dependency on technology, and other external factors. Once identified, the likelihood of each threat is documented. The approach to performing threat assessment is as follows:

2.2 Threat likelihood

It defines the probability of occurrence or past known precedence of identified threats. The threat likelihood is expressed on a scale of 1-3 as defined in the Risk Assessment methodology.

Probability Value	Rating	Meaning
1	Low	The threat is highly unlikely to occur. i.e. once in 2 yrs
2	Medium	The threat is likely to occur once per year.
3	High	The threat is likely to occur at least once per 3 months.

2.3 Threat Impact

The impact is the measure of the adversity of a security event that can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: confidentiality, integrity, and availability. The impact value is also expressed on a scale of 1-3 using the matrix mentioned below:

Impact Value	Rating	Meaning
1	Low	The impact is minor, major business operations are not affected.

2	Medium	Significant loss to business operations or customer confidence or market share. Customers may be lost.
3	High	The effect is disastrous, but the organization can survive, at a significant loss.

2.4 Threat Value

The threat value (T) shall be calculated as a summation of Threat Probability and Threat Impact.