Trackon Canada Private Limited

Policy for Remediation of Vulnerabilities

Version Number: 1.1

Last Updated: July 2022

Next Update: January 2023

Approved By: Jaspreet Singh, Director.

Senior Officer Approval for Program: Jaspreet Singh, Director.

TABLE OF CONTENT

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 Terms and definitions

For this document, the following terms and definitions apply:

- **Asset -** anything that holds value to [Organization] IT system, its business operations, and their continuity.
- **Impact** – adverse change(s) to the level of business objectives achieved.
- **Information** – processed data.
- **Information security risk** - potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and its consequence (impact).
- **Risk management** – coordinated activities to direct and control the organization about risk.
- **Risk identification** – the activity of finding, listing, and characterizing the elements of risk.
- **Risk estimation** – the activity of assigning values to the likelihood and consequences of a risk.

- **Risk assessment** – the overall process of risk analysis (systematic use of information to identify sources and to estimate the risk) and risk evaluation (the process of comparing the estimated risk against given risk criteria to determine the significance of risk).
- **Risk treatment** – the process of selection and implementation of controls to modify risk, or take decisions to mitigate, avoid, accept, or transfer risks.
- **Risk avoidance** – decision not to become involved in, or action to withdraw from, a risk situation.
- **Risk communication** – exchange or sharing of information about risk between the decision-maker and other stakeholders.
- **Risk mitigation** – actions taken to lessen the likelihood, negative consequences, or both, associated with risk.
- **Risk acceptance** – acceptance of the negative consequences (losses) from a particular risk.
- **Risk transfer** – sharing with / transferring to, another party the negative consequences of risk; and
- **Residual risk** – the risk remaining after risk treatment.

3 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.

3.1 Determining Risk Score for Vulnerabilities Identified

The risk value of an asset is based on the Asset value, Vulnerability value, and threat value of an asset. The risk score will be calculated based on the following formula:

Risk Score = Threat Value * Vulnerability Value * Asset Value

All risks which have a risk value of 40 and above have to be considered for protective measures in Risk Treatment Plan **(Refer to the Risk Assessment and Risk Treatment Plan).** ISWC representative and department champion of respective function(s) shall perform a risk assessment for their respective functions.

Risk owners shall be identified for all the risks in the risk register.

RISK VALUE MATRIX

Risk Value = Asset Value*Vulnerability Value*Threat Value

		2			**3**			**4**			**5**			**6**		
Vulnerability		**1**	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**
Asset Value	3	6	12	18	9	18	27	12	24	36	15	30	45	18	36	54
	4	8	16	24	12	24	36	16	32	48	20	40	60	24	48	72

	5	10	20	30	15	30	45	20	40	60	25	50	75	30	60	90
	6	12	24	36	18	36	54	24	48	72	30	60	90	36	72	108
	7	14	28	42	21	42	63	28	56	84	35	70	105	42	84	126
	8	16	32	48	24	48	72	32	64	96	40	80	120	48	96	144
	9	18	36	54	27	54	81	36	72	108	45	90	135	54	108	162

Col our	Risk Value	Risk Rating
🟦	6-57	Low
🟨	58-109	Medium
🟥	110-162	High

3.2 Risk Acceptance Level for Vulnerabilities Identified

Following guidelines have been defined for a risk to be treated with appropriate controls in the risk treatment plan:

- Any risk having a value of '110' and above should be considered as “High Risks” and must be considered for adequate control implementation in RTP (Risk Treatment Plan).

- Any risk having the value between '58' to '109' should be considered as “Medium Risks” and must be treated with adequate control implementation in RTP; and
- All risks having a value equal to or less than ‘57’ is considered acceptable risk and does not require the formation of an RTP.

3.3 Remediation Plan of Vulnerabilities

The observed risks that are beyond the acceptable level of risk defined by the management will be documented and appropriate controls will be recommended to mitigate them. A comprehensive risk treatment plan will be developed along with the responsibility assigned, a tentative schedule for work with an expected deadline to complete the activity, and the estimated cost associated with it.

Residual Risk after Remediation Plan is implemented: Efforts will be made to treat the high-risk score to an acceptable risk value by implementing any of the risk treatment plans. The residual risk shall be accepted as per the risk’s acceptance criteria defined. The risk score which cannot be reduced to an acceptable level due to technical constraints or budgetary constraints shall have management’s acceptance

The management shall consider the following four options to treat the risks highlighted in the risk treatment plan:

- Accept the decision to accept the risk and not to implement any control.
- Transfer: transfer the risk to other bodies (e.g., insurance).
- Mitigate/ Control: implement control to mitigate the risk; and
- Avoid/ Terminate: forgo the system which has risk.

ISWC members are responsible to approve the responsibility and expected closure date for implementation of control defined and documented by the

Management Representative. For the risks accepted by the management, the ISWC will document the business justification for risk acceptance and residual risk faced by [Organization].

3.4 Risk Acceptance Criteria for Vulnerabilities Identified

4

Risk acceptance refers to the decision of the management in which the highlighted risk is accepted. Management decisions shall be taken after considering the existing residual risk and the mitigation plan. In cases, where management decides to accept the existing residual risk i.e., authorization is not granted for the implementation of controls, the reasons for acceptance shall be documented along with appropriate justifications.

Risk shall be accepted for several reasons including, but not limited to:

- The potential impact is low, and the cost of further protection against risk is not worthwhile in business terms.
- The likelihood of an incident is low, and the cost of further protection against the risk is not worthwhile in business terms; and
- The risk cannot be avoided, transferred, or mitigated. Any further within acceptable costs to the businesses.

4.1 Risk Mitigation Criteria for Vulnerabilities

Risk mitigation is the process of reducing a specific risk (or a set of risks) to an acceptable level by changing the operational environment and/ or applying technical or non-technical countermeasures such as.

- Physical: A perimeter fence.
- Procedural: an authorization form is signed by an appropriate person before a new user account is set up; and

- Technical: Use of approved certified services/ products.

4.2 Risk Transfer Criteria for Vulnerabilities Identified

Risk transfer involves a decision to share certain risks with external parties. Risk transfer can create new risks or modify existing, identified risks. Therefore, additional risk assessment followed by risk treatment may be necessary. Transfer can be done by insurance that shall support the consequences, or by sub-contracting a third party whose role shall be to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage.

4.3 Risk Avoidance/ Terminate Criteria for Vulnerabilities Identified

Risk can be terminated/ avoided by taking into consideration various means listed below:

- Choosing not to undertake the aspect of the business activity that attracts the particular risk, such as not providing direct customer access to the internet.
- Using alternative assets or methods to undertake the business activity, such as selecting different hardware or software; or
- Relocating assets away from known areas of physical risks, such as flood zones.