Trackon Canada Private Ltd

Disaster Recovery and Business Continuity Management Policy

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 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.

1.2 Purpose

The purpose of the Information Security – Business Continuity Management Policy is to define the requirements of information security continuity and appropriate redundancy measures which shall be defined and implemented to ensure continuity of operations in case of business disruptions.

1.3 Scope

The Information security – Business Continuity Management Policy applies to all the individuals and groups who will be involved in performing Business Continuity activities at the time of a disaster situation.

2 Information Security – Disaster Recovery and Business Continuity Management Policy *(ISO 27001 Control: A.17)*

2.1 Information security continuity *(ISO 27001 Control: 17.1)*

2.1.1 Planning information security continuity *(ISO 27001 Control: 17.1.1)*

1) Information security requirements shall be integrated into IT Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

2) Trackon Canada Pvt Ltd shall identify and document business process interdependencies and relationships with other processes, services, and underlying information systems.

3) Trackon Canada Pvt Ltd shall identify and document events that can cause possible interruptions to business processes along with the probability and impact of such interruptions and their consequences for business operations.

4) Based on the identified impact of such interruptions and their consequences for business operations, Trackon Canada Pvt Ltd shall identify acceptable service outage limits and data losses; and

5) Trackon Canada Pvt Ltd shall define and document recovery guidelines that can be taken as a baseline reference to classify mission-critical systems and develop recovery and restoration procedures.

2.1.2 Implementing information security continuity *(ISO 27001 Control: 17.1.2)*

1) IT BCP and DRP shall ensure availability and continuity of critical activities and associated systems to ensure minimum impact to the organization.

2) Appropriate risk assessment shall be conducted to identify risks that can disrupt Trackon Canada Pvt Ltd's information systems.

3) Business Impact Analysis shall be conducted to ascertain critical activities which would cause the maximum impact in the least possible time.

4) Appropriate Management structure shall be identified and trained adequately to ensure an effective response to business disruptions; and

5) IT BCP and IT DRP shall be updated at least annually or whenever there is a major change to ensure that they are relevant to the current requirements of Trackon Canada Pvt Ltd.

2.1.3 Verify, review, and evaluate information security continuity *(ISO 27001 Control: 17.1.3)*

1) IT BCP and IT DRP tests shall be conducted at least annually to ensure that the arrangements made for continuity of operations are effective and efficient.

2) The designated business process owners and team members shall be engaged in performing the IT BCP and IT DRP tests.

3) The records and results of IT BCP and IT DRP shall be maintained; and

4) The results shall be used to enhance the IT BCP and IT DRP plans.

2.2 Redundancies *(ISO 27001 Control: 17.2)*

1) Trackon Canada Pvt Ltd shall identify business requirements for the availability of information systems.

2) Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures shall be considered.

3) Where applicable, redundant information systems shall be tested to ensure the failover from one component to another component works as intended: and

4) Additionally, redundancies developed shall be tested on an annual basis to ensure the mechanisms are working appropriately.