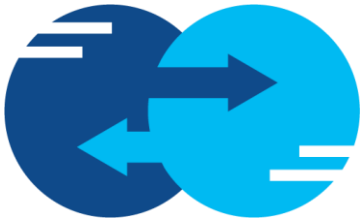

Trackon Canada Private Limited

Log Management or Network Monitoring 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

Information Security Incident is a single or a series of unwanted or unexpected Information Security Events that have a significant probability of compromising business operations and threatening information security. It is related to exceptional situations or a situation that warrants the intervention of Senior Management. The purpose of the Information Security Incident Management Policy is to provide directions to develop and implement a robust process for identifying, managing, resolving, and communicating information security incidents.

1.3 Scope and Definitions

The Information Security Incident Management Policy applies to all employees, sub-contractors, associated third parties, information systems, and assets (assets as defined and classified as IT Infrastructure and Hardware, Services, Digital, Tangible and Human Assets in the “Information Assets Inventory”) that are owned by Trackon.

Terms	Definitions
Information Security Management System	Information Security Management System (ISMS) refers to a set of policies and processes established by management to assess the security requirements, develop and implement controls, evaluate the effectiveness of controls and implement improvements following a continuous improvement process
Confidentiality	Confidentiality is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.

Integrity	To preserve the integrity of information means to protect the accuracy and completeness of the information and the methods that are used to process and manage it
Availability	Availability is a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. Assets include things like information, systems, facilities, networks, and computers. All these assets shall be available to authorized entities when they need to access or use them
Information Asset	Information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization
Information Security	Information Security is the protection of information from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities
Information Security Incident	An Information Security incident is made up of one or more unwanted or unexpected Information Security events that could very likely compromise the security of your information and weaken or impair your business operations
Information Security Event	An Information Security event indicates that the security of an information system, service, or network may have been breached or compromised. An Information Security event indicates that an Information Security Policy may have been violated or a safeguard may have failed
Information Security Forums	Forums/groups that supply opinions and guidance on different aspects of Information Security
Information Security Management Committee (ISMC)	ISMC is responsible for the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS for the defined scope and boundaries
Information Security Working Committee (ISWC)	ISWC is responsible for ensuring smooth execution of audit activities, participation in pre-audit meetings, etc.

IT Security Head	IT Security Head is the owner of the ISMS. The IT Security Head shall co-ordinate all Information Security activities across the organization
IT Security Manager	IT Security Manager to assist IT Security Head in implementing and coordinating the Information Security activities across the organization
Information Security Management System (ISMS) Auditor	The Information Security Management System Auditor (ISMSA) performs periodic audits of Trackon Canada Pvt Ltd ISMS and related processes
Information Processing Facility	An Information Processing Facility can be a system, service, or infrastructure, or any physical location that houses information. It can be either a system or a place; it can be either tangible or intangible
Malicious Code	Malicious code includes all and any programs (including macros and scripts) which are deliberately coded to cause an unexpected (and usually, unwanted) event on an IT system
Risk	Combination of the probability of an unwanted event and its consequence
Sensitive System	A critical system that contains sensitive/confidential information
Threat	A threat is a potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organization or system
Vulnerability	Vulnerability is a weakness in an information asset or group of information assets. An information asset's weakness could allow it to be exploited and harmed by one or more threats

2 Policy

2.1 Logging and monitoring *(ISO 27001 Control: 12.4)*

1) Event logs shall be enabled for all critical systems. It shall be ensured that the event logs recording the critical user activities, exceptions, and security events are enabled and stored for reasonable periods to assist in future investigations and access control monitoring. Logs shall be monitored and analyzed for any possible unauthorized use of information systems.

2) Security controls shall be built to ensure the integrity of logs. It shall be ensured that the Administrators do not have permission to erase or de-activate logs of their activities. Access to event logs and audit trails shall be provided to authorized users only.

3) Logging facilities and log information shall be protected against tampering and unauthorized access; and

4) The clocks of all relevant information processing systems or security domains shall be synchronized with an agreed and accurate time source. Users shall not have the access to change the system date and time settings. The rights shall be restricted to authorized Administrators only.

3 Responsibilities

The owner of the Policy Manual shall be the IT Security Head who shall be assisted by the IT Security Manager. The IT Security Head, IT Security Manager, and their designates shall be responsible for the maintenance and accuracy of these policies.