Information Security Policy Statement
OMS630

It is Ontrack's policy to develop, implement and maintain an Information Security Management system (ISMS) that:

1. Provides confidence within the company and to our clients, partners and interested parties that the availability, integrity and confidentiality of their information will be maintained appropriately.

2. Manages information security risks to all Ontrack and customer assets.

3. Protects Ontrack's ongoing ability to meet contracted commitments through appropriate continuity.

4. Bases information security decisions and investments on risks assessment of relevant assets considering Availability, Integrity, and Confidentiality.

5. Takes into account business and regulatory/legal requirements and contractual security obligations.

6. Maintains awareness of all employees so they can identify and fulfil contractual, legislative and Ontrack specific security management responsibilities.

7. Reduce the business impact and deals effectively with security incidents.

Ontrack's policy is supported by the following high-level internal objectives:

1. Implementation of a company wide information security management system that is compliant and independently certified to the ISO27001:2022 standard for information security management systems.

2. Implementation of a sensitive information control policy including compliance with regulations under the GDPR to protect client, partner, our own and personal employee information which is not in the public domain.

3. Implementation of an information security risk assessment process that assesses the business harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of current threats and vulnerabilities, and controls currently being implemented.

4. Development and deployment of a business continuity plan to counteract set backs to business activity and to protect processes from the effects of major failure and disaster.

5. Information security awareness guidance for all employees.

6. Management that supports the continuous review and improvement of Ontrack's ISMS and objectives.

7. Implementation of incident management procedures for identifying and reporting/ investigating security incidents for review and action.

Ontrack's ISMS policy is reviewed by management every 12 months as part of the management review who will recommend amendments and updates to the existing policy as part of our continuous service improvement process.

The policy will remain available for interested parties upon request and via the Ontrack web site.

Signed

Date….05/01/2026……

Katrina O'Connor
Chief Executive Officer

Document Control

Document title	OMS630 Information Security Policy Statement
Author (name)	Tim Lawson
Owner (role)	Programme Manager
Date published	05/01/2026
Version	4.0
Classification	External Use
Audience	All Interested Parties
Approved by (name, role)	Katrina O'Connor, CEO