Third-Party Supplier Information Security Requirements

VicTrack Standard

Document Information

Document ID	IS-ST 005
Reference No.	D/15/43301
Version	1.0
Dated	02 December 2024

Contents

1 Definitions

In this Standard, the following defined terms apply:

Term	Definition
CSA STAR	means the Cloud Security Alliance Security, Trust and Assurance Registry published by Cloud Security Alliance.
ICT Systems	means all information and communication technology systems, assets, applications, hardware, Software-as-a-Service (SaaS) applications or software that collect, store, process, transmit and display information, including telecommunication systems.
Information Assets	means any data, information, or knowledge that is of value to VicTrack and requires protection.
Information Asset Owner	means a nominated role or business group in VicTrack accountable for the secure management of all information generated by, or on behalf of them, and/ or under their control.
IRAP	means the Information Security Registered Assessors Program by the Australian Signals Directorate.
ISO	means an accreditation by the International Organisation for Standardisation.
Manager Enterprise Architecture and Security	means the person employed by VicTrack as the Manager Enterprise Architecture and Security in the Corporate Services Group.
Significant Impact	means an impact that may directly impact VicTrack and hinder its ability to deliver services including (without limitation) any impact to transport infrastructure classified as critical under the *Security of Critical Infrastructure Act 2018* (Cth).
SOC 2	means Service Organisation Control 2 as developed by the American Institute of Certified Public Accountants.
Standard	means this VicTrack standard titled “Third-Party Supplier Security Requirements”.
Supplier	means a supplier of goods and/or services requiring access to VicTrack’s ICT Systems and/or Information Assets.
VicTrack	means Victorian Rail Track.
VPDSS	means the Victorian Protective Data Security Standards issued by the Office of the Victorian Information Commissioner under sections 86 and 87 of the *Privacy and Data Protection Act 2014* (Vic).

2 Purpose

The purpose of this Standard is to set out the information security requirements for any supplier requiring access to VicTrack's ICT Systems and/or Information Assets.

3 Scope and coverage

The scope and coverage of this Standard includes:

Suppliers	Organisational Locations	Technology
This Standard applies to all of VicTrack's Suppliers who have or gain any access to VicTrack's ICT Systems and/or Information Assets.	This Standard applies to all of VicTrack's ICT Systems and Information Assets owned, acquired, developed or managed by VicTrack regardless of their location.	This Standard applies to all ICT Systems owned, managed, acquired, or developed by VicTrack that store, process, or transmit information, including but not limited to applications, networks, hardware, software, Software-as-a-Service (SaaS) applications and telecommunications systems.

4 Compliance statement

The compliance language used in this Standard is defined below. The variable use of the terms indicates the differing degrees of risk and the applicable exemption process for the requirement.

Term	Risk	Description
Must	High	The requirement is mandatory unless a risk assessment is performed, and an exemption is approved by the Executive General Manager of Corporate Services.
Should	Medium	The requirement is mandatory unless a risk assessment is performed, and the risk is accepted by the Information Asset Owner.

5 General security requirements

5.1 The Supplier's systems that store or host VicTrack's Information Assets ***must*** be located within Australia.

5.2 The Supplier ***must*** notify VicTrack immediately and comply with all directions from VicTrack if the Supplier becomes aware of any notable changes or contravention of security requirements set out in this standard.

5.3 Designated personnel from the Supplier ***must*** attend and successfully complete security and cyber awareness training provided by VicTrack:

(a) prior to providing any goods or services to VicTrack; and

(b) if the provision of goods or services continues for more than 24 months, every 24 months after the Supplier commences the provision of goods or services to VicTrack; and

(c) as otherwise requested by VicTrack in writing.

5.4 The Supplier ***must*** have an information security policy in place that complies with applicable industry standards including the VPDSS and is subject to review by VicTrack.

5.5 The Supplier ***must*** not store any passwords used to access VicTrack's ICT Systems or Information Assets in unsecured formats, such as Word, Excel, or OneNote.

5.6 The Supplier ***must*** not access VicTrack's ICT Systems or Information Assets while connected to public Wi-Fi, such as in coffee shops or shopping centres.

5.7 The Supplier ***must*** not use VicTrack provided credentials to create social media accounts such as Facebook or Apple ID.

5.8 The Supplier ***must*** implement appropriate security controls aligned to industry best practices, to safeguard any VicTrack Information Assets in their possession.

6 Right to audit and security assessment

6.1 The Supplier ***must*** be aware that VicTrack reserves the right to audit the Supplier for compliance with the requirements of this Standard and any other contractual obligations related to information security.

6.2 The Supplier ***must*** permit VicTrack to conduct periodic security assessments on a Supplier, including the completion of a security questionnaire, which the Supplier ***must*** fill out upon request.

6.3 The Supplier ***must*** implement the security controls recommended by VicTrack, if any, following the outcome of the Supplier's security assessment.

7 Access security requirements

7.1 The Supplier will be provided with, and ***must*** use, unique named credentials for each individual requiring access to VicTrack's ICT Systems and/or Information Assets.

7.2 The Supplier ***must*** acknowledge that they are responsible for all activities performed using the issued credentials.

7.3 The Supplier ***must*** notify VicTrack of any staff changes affecting the nominated individuals who have access to VicTrack's ICT Systems and/or Information Assets.

7.4 The Supplier ***must*** designate a technical contact to act as the primary liaison for all information security matters, ensuring prompt communication, issue resolution and compliance with information security requirements. The Supplier ***must*** inform VicTrack if that technical contact changes.

7.5 The Supplier ***must*** ensure that any individual accessing VicTrack's ICT Systems and/or Information Assets:

(a) have verified reference checks prior to employment; and

(b) successfully passed a criminal background check.

8 Standard industry certification requirements

8.1 The Supplier ***should*** provide at least one of the following standard industry certifications, upon request by VicTrack, to demonstrate that effective security controls are in place to protect VicTrack's Information Assets:

(a) SOC 2;

(b) ISO 27001;

(c) IRAP assessment; and

(d) any other independent audit that VicTrack deems appropriate and fit for purpose as confirmed to the Supplier in writing.

8.2 If the Supplier supplies SaaS (Software-as-a-Service) cloud based applications, the Supplier ***should*** provide at least one of the following standard industry certifications, upon request by VicTrack, to demonstrate that effective security controls are in place to protect VicTrack's Information Assets:

(a) CSA STAR certification Level 1, Level 2 and Level 3 (Link); and

(b) ISO/IEC 27034 certification for application security (Link).

9 Cyber incidents notification and handling requirements

9.1 The Supplier ***must*** notify VicTrack within 12 hours of any actual or suspected cyber incidents that may have a Significant Impact.

9.2 The Supplier ***must*** notify VicTrack of any actual or suspected cyber incidents that are not classed as Significant Impacts within 72 hours.

9.3 The Supplier ***must*** assist VicTrack in cyber incident response activities if VicTrack issued credentials are involved in any incident, or if there is any suspicion of the Supplier's ICT Systems or networks being involved in the incident.

9.4 The notification of incidents in accordance with this Standard or any notifications concerning information security generally ***should*** be sent to the following VicTrack contacts:

(a) Network Management Centre

Email: nmc@victrack.com.au

Phone: 1800 887 662

(b) Service Desk

Email: servicedesk@victrack.com.au

Phone: +61 3 9619 1101

10 Information sharing security requirements

10.1 The Supplier ***must*** not share any information with VicTrack outside of VicTrack provided and approved data sharing channels being Microsoft Outlook, Microsoft Teams, OneDrive, SharePoint and any other data sharing channels approved by VicTrack in writing.

10.2 The Supplier ***must*** not upload, copy or share VicTrack's Information Asset to any other data sharing channels, public clouds or personal emails including (without limitation) Dropbox, Google Drive, WeTransfer, personal Outlook accounts and Gmail.

11 Subcontracting

11.1 The Supplier ***must*** ensure that any subcontractors it engages during the provision of goods or services to VicTrack comply with the requirements of this Standard.

11.2 The Supplier ***must*** ensure that the requirements of this Standard are incorporated into the subcontract of any subcontractors it engages during the provision of goods or services to VicTrack.

12 Reference documents

Document ID	Title
VPDSS Framework	Victoria Protective Data Security Standard Framework (Link)

13 Document history

Version	Description	Author	Date
Version 1.0	First version	Manager Enterprise Architecture and Security	02 December 2024

This Standard is going to replace the Supplier Security Requirements (IS-ST-005).

14 Review period

This Standard will be reviewed at least every two (2) years by the Manager Enterprise Architecture & Security or amended as appropriate. The content of this document is uncontrolled when printed.