Telecommunications Acceptable Use policy

Document information

HPRM ref	D/16/115993 [v3] VT-PO 158
Date	23 August 2017
Security class	UNCLASSIFIED

Introduction

1. Purpose

The objective of this Policy is to communicate to customers acceptable usage and access requirements of VicTrack's telecommunications services and resources.

2. Definitions

Telecommunications Services	Services and resources provided by VicTrack include, but are not limited to, Wide Area Networks, broadband access links, internet, video conferencing, unified, PABX and wireless communications, cloud computing and communications links.
Customer Services	Services and resources accessed or used by the customer, subject to a contract with VicTrack.

3. Scope

Inclusive of all individuals who access, use and / or maintain VicTrack's Telecommunications Services.

Individuals Covered

- Customers, who access or use the Telecommunications Services pursuant to a contract with VicTrack;
- All full-time, part-time and temporary staff employed by, or working for or on behalf of the customer;
- Contractors and consultants working for, or on behalf of, the customer;
- Customer approved third parties, customer's customers or end users working for, or on behalf of, the customer.

Location

- This Policy applies to all users of VicTrack's Telecommunications Services, systems and infrastructure regardless of location.

Systems

- This Policy includes, but is not limited to, systems, infrastructure, information and resources owned, provided, maintained, used by or for VicTrack's Telecommunications Services.

4. Policy statements

General - prohibited use and content

Individuals accessing and using VicTrack's Telecommunications Services may not use the Telecommunications Services or upload content onto VicTrack's Systems (including but not limited to user accounts, computer systems or networks connected to VicTrack's Telecommunications Services) in a manner that:

- Violates any federal, state or local, (in that order) statute, regulation, rule, order, treaty, or other law (each a "Law"), including, but not limited to, the Telecommunications Act 1997, the Telecommunications (Interception and Access) Act 1979, the Mutual Assistance in Criminal Matters Act 1987, the Victorian Protective Data Security Standards, the Criminal Code Act 1995, the Privacy Act 1998, the Privacy and Data Protection Act 2015, the Information Privacy Principles, Spam Act 2003, Freedom of Information Act 1982, the Archives Act 1983, the Evidence Act 2008, the Crimes Act 1958, or those Laws concerning child pornography and illegal gambling;
- Violates, discriminates, or otherwise encroaches on the rights of others, including, but not limited to, infringing or misappropriating any intellectual property rights (copyright, trademarks, trade secrets, patents, designs, confidential information or other intellectual property or other proprietary rights of another)
- May be or is defamatory or constitutes an illegal threat;
- Inappropriate usage, as determined in the sole and absolute discretion of VicTrack, or encumbers network or other system resources beyond those provided to your organisation as part of the Telecommunications Services purchased;
- Makes fraudulent offers to sell or buy products, items, or services, or to advance any financial scam;
- Advocates, indulges in, or induces illegal activity;
- Stalks, harasses, harms or intends to harm;
- Impersonates any person or entity or otherwise misrepresents customer's affiliation with a person or entity;
- Accesses or attempts to access or use the Telecommunications Services in a way intended to avoid incurring fees or exceeding usage limits or quotas;
- Is using Telecommunications Services not provided or intended for use by customer's organisation;
- Interferes with, tampers or disrupts the Telecommunications Services or servers or networks connected to the Services or any other party's use of the Services;
- Uses any high volume automated means (including robots, spiders, scripts or similar data gathering or extraction methods) to access the Telecommunications Services or VicTrack's systems;
- Is using or is attempting to use the Telecommunication Services to intrude or launch network-based attacks on local and/or foreign networks, hosts, servers, systems or applications including but not limited to overloading, denial of service attacks, crashing or mail-bombing;

- Violates the security or integrity of VicTrack's Systems by (including, but not limited to):
    - Accessing or attempting to access any portion of the Telecommunications Service or VicTrack's systems without permission, including attempting to probe, scan, or test its vulnerability or to breach any security or authentication controls used by a user, system or network;
    - Knowingly uploading content that contains viruses, worms, corrupt files, Trojan horses, or other forms of malicious code, or any other content that may compromise Telecommunications Services; or
    - Hacking, destabilising, or adapting the Telecommunications Services, or altering another website to falsely imply it is affiliated with the Telecommunications Services;
    - Physical tampering with VicTrack equipment located on customer's premises;
- Connects or attempts to connect to any users, systems, or networks where a customer does not have permission to communicate with such users, systems, or networks by (including, but not limited to):
    - Monitoring or crawling a system so that such system is impaired or disrupted;
    - Conducting denial of service attacks;
    - Conducting vulnerability scans without prior written authorisation;
    - Circumventing or attempting to circumvent security controls;
    - Exploiting or attempting to exploit known or unknown vulnerabilities;
    - Intentionally interfering with the proper functioning of any system, including any deliberate attempts to overload a system by any means;
    - Operating network services such as open proxies, open mail relays, or open recursive domain name servers; or
    - Using means (manual or electronic) to avoid any use limitations placed on a system, such as access and storage restrictions;
- Distributes, publishes, sends, or facilitates unsolicited mass e-mailings (spam), promotions, advertising, or solicitations, including commercial advertising and informational announcements;
- Forging or changing packets or email headers or any part of a message to hide the origin or route of the message or the identity of the sender; or
- Collects or stores replies to messages if those messages violate this Acceptable Use Policy.

5. Responsibility of customer

All content that is provided to VicTrack or actions that are performed via a customer's account, whether provided or performed by a customer's employees, customer's contractors, customer approved third parties, customer's customers or end users, knowingly or inadvertently, are the sole responsibility of the customer.

Customers are required to maintain detailed logging and audit trail for all security related activities, including but not limited to, failed authentication or as otherwise required by Law.

Customers are required to ensure that their user credentials (including, but not limited to the administration account to access VicTrack's hosted cloud computing service self-service portal) are

securely managed and that password management procedures aligned with industry best practice are followed.

It is recommended that customers implement preventive and detective controls to safeguard Customer Services against intrusions, malicious and mobile code like viruses, worms, spyware, adware, malware, trojans etc. Reasonable perimeter security measures must be applied on Customer Services and related networks by the customer as per industry best practice on all external connections to the Customer Services including but not limited to the internet and the customer's network.

Customers must not resell VicTrack provided services in whole or in part or otherwise redistribute them unless prior written consent is provided by VicTrack to the customer.

Customers must not act or engage in a practice that contravenes any Law.

Digital storage

In addition to the General Requirements set out above, customers are:

- required to comply with all license requirements for all software used by the customer on VicTrack hosted Cloud Service.
- responsible for ensuring their use of VicTrack hosted Cloud Services complies with all Laws; and
- required to ensure that their data stored on the VicTrack hosted Cloud Services does not violate any export control laws.

6. Monitoring and enforcement

While VicTrack does not ordinarily monitor customers' activity, it may be required to in accordance with the terms of a contract or by Law. In these circumstances, VicTrack may:

- Be required to preserve information pursuant to a notice issued under any Law;
- Preserve information in accordance with the Public Records Act 1973;
- Provide interception capabilities to duly authorised law enforcement officials, regulators, or other appropriate third parties to be able to monitor voice traffic on VicTrack's Telecommunications Services or infrastructure when required by the law;
- Report any activity that it suspects violates any law or regulation to duly authorised law enforcement officials, regulators, or other appropriate third parties;
- Cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Acceptable Use Policy.
- Investigate violations of this Acceptable Use Policy or misuse of the Telecommunications Services;
- Investigate and help prevent security threats, fraud, or other illegal, malicious or inappropriate activity;
- Remove or disable access to any content or resource that violates this Acceptable Use Policy or any other contract VicTrack has with customer for use of the Telecommunications Services; or

- Suspend, restrict or terminate provision of Telecommunications Services to the customer for uses that violate this Acceptable Use Policy or any other agreement VicTrack has with customer for use of the Telecommunications Services.

7. Notification

Customers are responsible to ensure that all users of the Telecommunications Services (including, but not limited to customer's employees, customer's contractors, customer approved third parties, customer's customers and end users) are made aware of and are required to adhere to this Policy prior to their use of the Telecommunications Services, including any updates to this Policy from time to time.

VicTrack may, in its sole and absolute discretion, make changes to this Policy from time to time. The revised policy will be made available on VicTrack's website. VicTrack will notify you of any material changes to this Policy.

Continued use of the Telecommunications Services following notice of any such changes shall indicate the customer's acknowledgement of such changes and agreement to be bound by the terms and conditions, as changed.

8. Applicability and enforcement

This Policy applies to all Individuals, work locations and systems covered in the Policy scope. Compliance with this Policy and all related documents is mandatory.

VicTrack reserves the right to undertake compliance audits on Customer Services from time to time.

9. Reporting policy abuse

Any party seeking to report any violations of this Policy may send an e-mail to: service.assurance@victrack.com.au. All communication will be treated in confidence.

10. Related policies and references

- Victorian Protective Data Security Standards
- Public Records Act 1973
- Telecommunications Act 1997
- Privacy and Data Protection Act 2015 & Information Privacy Principles
- Privacy Act 1998
- Mutual Assistance in Criminal Matters Act 1987
- Freedom of Information Act 1982
- Archives Act 1983
- Evidence Act 2008
- SPAM Act 2003
- Crimes Act 1958
- Criminal Code Act 1995
- Telecommunications (Interception and Access) Act 1979

- Telecommunications Act 1997
- Australian Security Intelligence Organisation Act 1979
- Intelligence Services Act 2001
- Electronic Transactions Act 1999

11. Protected Disclosure Act Amendments and review

This Policy will be reviewed once every three years at a minimum or when required by a technology, industry or business change. Customers will be provided with access to this Policy via VicTrack's website.