innov8@comtrac.com.au | 1300 292 939

Master Terms & Agreements

Information & Cybersecurity Standards

INTRODUCTION AND GENERAL TERMS

Relationship with Comtrac's Master Services Agreement

This document forms part of the Comtrac Master Services Agreement (MSA) and its referenced or related material, together the "Agreement". This document should be read in concert with Comtrac's MSA and other referenced or related material found at the Comtrac Trust Portal (https://trust.comtrac.com.au).

Comtrac and Comtrac Services

Comtrac is the operating entity of Investigation Management Australia Pty Ltd (IMA), an Australian Private Company limited by Shares registered to Level 6 of 300 Ann Street, Brisbane Queensland Australia 3000, under ACN 159 058 241. Comtrac provides software, information security and cloud infrastructure services for government and regulated industries (Comtrac Services).

Comtrac Trust Portal

Comtrac hosts and maintains the Comtrac Trust Portal as a centralised location for its customer facing legal, compliance and security documents. Material found on the Comtrac Trust Portal will always be the most current version, so it is important material as it relates to legal, compliance and security at Comtrac should always be sourced there, as it is required as printed or saved versions may be out-dated.

Definitions

In this document, unless the contrary intention appears, Terms or other Definitions are per the Comtrac Definition Schedule. Terms capitalised that are not defined in this document, or the Comtrac Definition Schedule may be mistakenly represented

as Terms. If words are mistakenly capitalised and treated as Terms or if certain words are intentionally left undefined but are believed by a party to have the potential of being Terms; their meaning should be understood based on the context in which they appear. This determination should be made by considering what a reasonable person, who is deemed capable of responsibly reviewing commercial agreements, would interpret those words to mean. Definitions can be inferred from the subject matter discussed in each section, and when suitable, terms can be defined within the text or introduced by their acronyms.

Disputes & Contact

Any disputes are to be raised in accordance with the dispute resolution process outlined in Comtrac's MSA. Other inquiries relating to this document should be directed to trust@comtrac.com.au.

Information Security Standards

The Customer must maintain security in the acquisition and use of the Comtrac Services in accordance with applicable standards, frameworks, and best practice.

Customers in Australia

For an Australian Customer, these include:

- Australian Government Information Security Manual (ISM)
- Australian Government Protective Security Policy Framework (PSPF)
- Australian Government Essential Eight
- Information Security Registered Assessors Program (IRAP)
- and/or any later versions of these.

Customers not in Australia

For a Customer in a jurisdiction outside of Australia, these include the relevant jurisdiction equivalents, aligned to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, and/or any later version of this.

All Customers

All Customers must identify applicable requirements from:

- ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 9001:2015. Quality management systems - Requirements;
- ISO/IEC 31000:2018. Risk Management – Guidelines; and
- OWASP Application Security Verification Standard,
- and/or any later versions of these, and implement requirements appropriate to the Customer and the Comtrac Services to which the Customer subscribes.

Certification against standards is not a requirement, but alignment with and adoption of applicable requirements is, and Comtrac reserves the right to request sight of any related Statement of Applicability.

Security Governance

In order to support the acquisition and use of the Comtrac Services, the Customer must develop and maintain information security policies, procedures, and guidelines in accordance with the requirements above that are reviewed at regular intervals (and no less than annually); Facilitate appropriate responses to changing threats and risks; and Cater for technology advances.

Roles Responsibilities and Personnel security

Security Executive

The Customer must Appoint a member of its senior executive (Security Executive) to be responsible for the Comtrac Services and the Customer's protective security policy and security oversight obligations under this Agreement. The Security Executive (or his/her Nominee) shall be the person responsible for the operational aspects of the acquisition and use of the Comtrac Services and Shall be the single point of contact with Comtrac.

The Security Executive shall nominate a suitably qualified person(s) as the System Owner (as it relates to the Comtrac Service) with authority to Notify Comtrac of possible and/or actual security (including personal data) incidents and breaches; Assign new Users to the Comtrac Services; Evoke the authority of Users of the Comtrac Services; Advise Comtrac of resulting changes to the acquisition and use of the Comtrac Services; and Advise and authorise Comtrac on matters relating to database rollback.

Personnel

The Customer must ensure that Users who access and use the Comtrac Services:

- Are subject to confidentiality obligations.
- Are eligible to have access.
- Have had their identity established.
- Are suitable to have access at the access level authorised.
- Have undergone probity, where necessary.
- Have agreed to comply with the Customer policies, procedures, standards, and guidelines that safeguard the Customer Data and resources from harm;

- Are properly trained.
- Have procedures in place for reporting security incidents that may compromise the use of the Comtrac Services and/or the integrity of Customer Data.

The Customer shall monitor and update User security requirements at least on a monthly basis, and report to Comtrac any breaches in protocol.

Codes of Conduct

The Customer must comply with all relevant public and private sector codes of conduct and must ensure that all Users of the Comtrac Services comply with Customer policy and codes of conduct, including that they act lawfully, with care, diligence, honesty, empathy, respect, openness, fairness, and accountability.

Asset Management

Data Loss Prevention

The Customer must have in place Data Loss Prevention (DLP) capability in the form of software, systems and/or processes to ensure the protection of Customer Data and Comtrac Data from data leakage risks.

Portable Media Handling

The Customer must not store Comtrac Data on portable or removable media without the prior written consent of Comtrac. In the event that the portable or removal media is approved by Comtrac, the Customer must have in place best practise encryption technologies to ensure that the Comtrac Data is removed from portable removable media on Comtrac' request.

Comtrac and the Customer acknowledge and agree that Customer Data may be exported and/or transferred to portable media by the Customer as part of the Comtrac Services (which include for purposes of legal proceedings).

Access and Identity Management

Controlled Access to Systems and Logging

The Customer must ensure that administrative access to the Comtrac Services is delivered through secure communications infrastructure. Establish and maintain complete, accurate, and up to date records of Customer Data and Comtrac Data accessed; details of Customer Personnel who accessed, collected, or changed the Customer Data and Comtrac Data; and the date and purpose for which it was accessed, collected, or changed.

On Comtrac' request, provide copies of the records referred to above as soon as possible. At a minimum within 24 hours of the request, the Customer must ensure that where access to any portion of the Comtrac Systems used to deliver the Comtrac Services is provided to any third party in connection with this Agreement, that such access is only provided subject to best practise authentication and access control restrictions.

The Customer must ensure that it keeps development, test and production environments used to access the Comtrac Services separate and only use the Comtrac Cloud Multi-Tenancy Beta (Pre-Production) Environment as outlined in the Comtrac Cloud Environment document.

The Customer must ensure that all access to Comtrac Systems required to use the Comtrac Services comply with Comtrac' standard security procedures and

processes, as notified to the Customer from time to time, and are accessed only for the purposes of the Customer using the Comtrac Services as set out in the Agreement.

The Customer must restrict access to Comtrac Systems to personnel who have been approved and authorised by the Customer to have such access. Comtrac may on reasonable grounds revoke its approval in respect of any individual User at any time, and the Customer must ensure that Personal comply with any such notification immediately.

The Customer must enforce Multi-Factor Authentication (MFA) at all times, including for VPNs, RDP, SSH and other remote access, and for all Users when they perform privileged access actions, or access sensitive and high-availability data repositories.

The Customer must ensure that remote administration access is compliant with the Customer's mobility policy (remote access policy) and that it complies with Comtrac' standard security procedures and processes as notified to the Customer from time to time. (For example, when administering Tenancy subscriptions and providing support).

The Customer must ensure that remote access complies with the Comtrac Services' architecture defined mobility security model (For example, restrictions on search facilities from the Customer's remote Personnel accessing the Comtrac Services on web portals and mobile applications).

The Customer must document, communicate, and enforce its security policy, in accordance with Comtrac standard security procedures and processes as notified to the Customer from time to time.

Operations Security

Security Vulnerability Management

The Customer must ensure that all Customer Systems that store, transmit, or process Customer Data and Comtrac Data undergo vulnerability scans on a regular basis (at least once a month); and Immediately after any system change.

If a vulnerability scan performed by the Customer reveals any vulnerabilities, the Customer must immediately take all steps to remediate such vulnerabilities and report to Comtrac, detailing the vulnerabilities and their remediation action taken as soon as practicable.

Protection from Malware

In the event that the Customer uses Customer software to access the Comtrac Services, the Customer must ensure no backdoor, time bomb, trojan horse or other computer software enables access to a third person not authorised by Comtrac.

The Customer must use all reasonable endeavours to ensure that the Comtrac Services are not compromised by malware. The Customer must use anti-malware controls to help avoid malicious software gaining unauthorised access to Customer Data and Comtrac Data including malicious software originating from public networks.

Denial of Service Protection

The Customer must ensure that all Customer Systems and devices used to access and use the Comtrac Services are protected from Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks with appropriate technologies and solutions.

Penetration Testing

The Customer must engage an independent third party to perform (at its own expense) and as least once every 12 (twelve) months, penetration testing and ethical hacking activities on the Customer Systems (and solutions and software if applicable) used to access and use the Comtrac Services.

Where the results of the penetration testing negatively and materially impact the Comtrac Services, the Customer shall notify Comtrac as soon as reasonably possible, making the relevant results of the testing available to Comtrac. The Customer and Comtrac shall agree on a plan to rectify the vulnerabilities with immediate effect, prioritised by criticality.

Back-ups

The Customer must document and implement a backup policy which takes daily copies of Customer Data and Customer Systems used in the acquisition and use of the Comtrac Services, including for system administration; Patching; and Change management to ensure that the Customer is able to determine the Customer database restore point for database rollback purposes.

The following daily backups must be retained for at least three months: New and material changes; and Software and configuration settings.

The following daily backups must be retained for at least 12 months: Test restoration; and ICT infrastructure changes.

The backup process must be regularly tested against the Customer's backup policy and suspected or identified defects must be remedied as soon as possible.

System Monitoring

The Customer must develop and maintain a system for monitoring the detection of security events, including from inside the Customer environment, for example by building a Security Operation Centre (SOC) to reduce cybersecurity threats, detect and respond to incidents on its computers, servers, and networks; and Engaging a Security Information and Event Management (SIEM) approach to provide real-time analysis of security alerts generated by applications and network hardware.

Cryptography

The Customer must ensure that: Any digital device including mobile phones, laptops, and tablets used to access or use the Comtrac Services has end-point encryption capabilities installed; All API connections must be protected using TLS 1.2 or above; Encryption must conform with the Comtrac encryption policy; It maintains the confidentiality of all encryption techniques such as keys and secrets at all times; All Customer Data held on Customer Systems outside of the Comtrac Systems must be encrypted at rest and in transit at all times; and It has the ability to delete Customer Data on User devices when it is no longer needed, or on Comtrac reasonable request.

Physical and environmental security

The Customer must ensure that it has adequate policies, systems, practices, procedures and guidelines in place to secure, monitor and audit the physical security of its Personnel, premises, facilities and Systems, including but not limited to personnel probity and access /identity cards; Customer Owned Environments and/or Data Centres; Equipment Inventories and access; Locks, lights, sensors; HVAC systems; Back to base alarms; and Physical security monitoring (guards) as required; Any other requirements under legislation or frameworks.

Systems Software and Application Security

The Customer must ensure that any Customer device, server, system, or network element, (including APIs) that store, process or facilitate Customer access to and use of the Comtrac Services must have in place the following.

- Application control to prevent execution of unapproved or malicious programs including .exe, DLL, scripts (e.g., Windows Script Host, PowerShell and HTA) and installers.
- Application patching - (e.g., Flash, web browsers, Microsoft Office, Java, and PDF viewers).
- Operating system patching – to secure computers (including network devices) with ‘extreme risk’ vulnerabilities as soon as possible, but no later than within 48 hours. Use the latest operating system version. Do not use unsupported versions.
- User application hardening.
- Web browsers configured to block Flash (preferably, uninstall), advertisements and Java on the internet.
- Disabled unnecessary features in Microsoft Office (e.g., OLE), web browsers and PDF viewers.

- Restricted administrative privileges to operating systems and applications based on user duties.
- Regularly revalidated need for privileges and how these are used (e.g., do not use privileged accounts for reading email and web browsing).
- Configured Microsoft Office macro settings to block macros from the internet, and only allow vetted macros in 'trusted locations' with limited write access, or digitally signed with a trusted certificate.
- Assurance that only macros digitally signed by trusted publishers are enabled.

Security Patching

Any Customer device (including BYOD devices), server, system, or network element, including APIs that store, process or facilitate Customer access to, and use of, the Comtrac Services must be patched by the Customer in accordance with the applicable Standards, and as a minimum on the following timelines:

- Critical vulnerabilities with a known available patch – immediately.
- Critical vulnerabilities without a known available patch - as soon as possible, but no later than within 48 hours.
- High level vulnerabilities - within 7 days.
- Medium to low level vulnerabilities - within the current monthly patch cycle.

Security Incident and Breach Management

Incidents

The Customer must not, and must ensure that Users do not, do anything in connection with access to, or use of the Comtrac Services, which could reasonably be expected to have an adverse impact on the security of the Comtrac Services or on Comtrac.

On becoming aware of any incident (meaning an actual or potential compromise of information security) which negatively impacts the Comtrac Services or Comtrac, the Customer must immediately notify Comtrac of the incident or risk, and provide the details reasonably required in order for Comtrac to respond appropriately and timeously; and Provide all assistance necessary and reasonably requested by Comtrac to respond to, protect against, or prevent further incidents or risk.

Notification

In the event of a security breach, (being any event or circumstance, which compromises the confidentiality, integrity, or availability of the Comtrac Services) the Customer must as soon as reasonably possible, and at least within 48 hours notify Comtrac of the breach and provide all the details known at the time of notification; and Provide on-going notification of the details of the breach as they become known, including the affected infrastructure, devices and/or Users.

Response

In response to a security breach the Customer must provide Comtrac with all assistance reasonably requested for Comtrac to recover from and protect against the breach. The Security Executive (or his/her Nominee) must work with Comtrac to coordinate communication and activities between the Customer and Comtrac in response to the breach.

The Customer must co-operate with Comtrac to promptly resolve the problem and provide details of the mitigation steps taken and actions performed to restore the confidentiality, integrity, and availability of the Comtrac Services. Under no

circumstances will the Customer notify any third party about the breach without first obtaining the prior written consent of Comtrac.

Audit

For internal audit and reporting purposes, the Customer must undertake an annual security assessment against the requirements of 1 above. Where any non-compliance with mandatory requirements is reasonably likely to result in risk to Comtrac and/or the Comtrac Services, the Customer must notify Comtrac of the nature of the risk; Remedial action taken; and Plan for risk treatment.

Customer Data and Information Classification

The Customer must identify all Customer Data (text, sound, video, image files, software, data, records, evidence etc.) in its possession or under its control; Assess the sensitivity and security classification of Customer Data; and Implement security and operational controls for the Customer Data that are proportional to their value, importance, and sensitivity.

The classification and operational controls must comply with relevant regulation, government requirements, policy frameworks and relevant law (security, privacy, evidence etc.) and codes of conduct. Access to, and associated privileges to Customer Data shall be Role-Based and apply the principle of lease privilege.

Compliance with Law

So as not to compromise the admissibility of evidence recorded and/or infringe individual rights, including privacy rights, the Customer must instruct and train Users on relevant legislation that applies to recording notes and evidence when using the

Comtrac Services, including national (domestic) law applicable to the Customer, including at a minimum:

- Telecommunications and surveillance laws.
- Human rights and privacy laws.
- Law of evidence.
- Criminal, civil, and procedural law.
- Tort law.
- International law, including mutual assistance treaties.

The Customer must, and ensure that Users, comply with the Customer policy, procedure, guidelines, and best practice when recording notes and evidence, including requirements for the admissibility of evidence. Notes and evidence must be contemporaneously recorded; Relevant; and Reliable.

Outsourcing in 3rd Party Relationships

The Customer is responsible for managing all third parties providing services to the Customer (Customer service providers) and shall ensure that all its service providers are legally bound through contractual arrangements which require them to meet all the same standards that the Customer itself must meet in accessing and using the Comtrac Services.