innov8@comtrac.com.au | 1300 292 939

Master Terms & Agreements

Comtrac Cloud Environments

INTRODUCTION AND GENERAL TERMS

Relationship with Comtrac's Master Services Agreement

This document forms part of the Comtrac Master Services Agreement (MSA). This document should be read in concert with all other documents which constitute Comtrac's MSA and other referenced material found at the Comtrac Trust Portal (https://trust.comtrac.com.au).

Definitions

In this document, unless the contrary intention appears, terms have the meaning given to them in the Comtrac Definition Schedule.

SOFTWARE-AS-A-SERVICE TERMS

General

To deliver the Comtrac Services, Comtrac maintains a number of infrastructure environments. The environment that the Customer's instance of the Comtrac Services runs on depends on the Customer requirements, Customer status as an Agency or Non-Agency customer, legal jurisdiction, and the Order Form that the Customer has agreed to and which forms part of the MSA.

COMTRAC CLOUD ENVIRONMENTS AVAILABLE TO THE CUSTOMER

Single-Tenancy Environment for Agencies & Non-Agencies

Comtrac's Single-Tenancy Environment for Agencies and Non-Agencies is available to Agency and enterprise Non-Agency customers only and not Individuals.

The Comtrac Single-Tenancy Environment for Agencies and Non-Agencies is hosted on Microsoft Azure datacentres exclusively in Australia and provisioned in accordance with the Australian Government ISM. Comtrac relies on disclosures made by Microsoft of the security, availability, and regulatory compliance against the ISM, which are available on Microsoft's public facing websites.

Resources used to support the provision of Comtrac Services, including databases and storage are not shared amongst other Agencies, Non-Agencies, or Individuals consuming the Comtrac Services in this environment and is for the exclusive access and use of the Agency or Non-Agency Customer.

Agencies and Users may at their discretion, handle and store information classified up to Protected Classification in line with the PSPF, however Comtrac does not guarantee or attest compliance against the ISM Controls at PROTECTED level in the Comtrac Multi-Tenancy Environment for Non-Agency Individuals. Comtrac does maintain a Single-Tenancy Environment for Protected & Sensitive Data where compliance against the ISM Controls at PROTECTED level is documented and attested to by Comtrac.

Customer Data is only able to be accessed by the Customer and Users, not by any other person, Individual, Agency, Non-Agency or User group, unless otherwise directed by Law. The Customer's Comtrac Single-Tenancy Environment for Agencies and Non-Agencies will be made accessible through a URL specific to their environment.

Expenses relating to the running of this Comtrac Cloud Environment are included in the Customer's Managed Service as outlined in the Order Form.

Limitations: Excessive or abusive use of data, data storage, or resource usage may result in the Comtrac Services being limited with 28 days' notice to the Customer and may require a renegotiation of Comtrac Fees and an amended Order Form. In the event that the Customer's usage of Comtrac Services increases during the Term of this MSA and necessitates additional Comtrac Services beyond those initially agreed upon, the Customer and the Comtrac may renegotiate the scope of services.

The Customer may request additional Comtrac Services by submitting a new Order Form detailing the specific services required. Comtrac agrees to evaluate the

Customer's request for additional Comtrac Services promptly and provide a response within a reasonable timeframe.

Single-Tenancy Environment for Protected & Sensitive Data

This Single-Tenancy Environment for Protected & Sensitive Data is available to Agencies and Non-Agencies. The Single-Tenancy Environment is hosted on Microsoft Azure datacentres exclusively in Australia and provisioned in accordance with the Australian Government ISM. Comtrac rely on disclosures made by Microsoft of the security, availability, and regulatory compliance against the ISM, which are available on Microsoft's public facing websites.

Resources used to support the provision of Comtrac Services, including databases and storage are not shared amongst other Agencies, Non-Agencies or Individuals consuming the Comtrac Services in this environment and is for the exclusive access and use of the Agency or Non-Agency Customer.

Agencies and Users may at their discretion, handle and store information classified up to Protected Classification in line with the PSPF and Comtrac asserts compliance against the ISM Controls at PROTECTED level as per Comtrac's Information Security Registered Assessors Program (IRAP) Cloud Security Assessment Outcome Report and Cloud Controls Matrix dated June 2023 (or its successor in place from time to time).

Customer Data is only able to be accessed by the Customer and Users, not by any other person, Individual, Agency, Non-Agency or User group, unless otherwise directed by Law.

The Customer's Comtrac Single-Tenancy Environment will be made accessible through a URL specific to their environment. Expenses relating to the running of this Comtrac Cloud Environment are included in the Customer's Managed Service as outlined in the Order Form.

Limitations: Excessive or abusive use of data, data storage or resource usage may result in the Comtrac Services being limited with 28 days' notice to the Customer and may require a renegotiation of Comtrac Cloud Fees and an amended Order Form.

In the event that the Customer's usage of Comtrac Services increases during the Term of this MSA and necessitates additional Comtrac Services beyond those initially agreed upon, the Customer and the Comtrac may renegotiate the scope of services.

The Customer may request additional Comtrac Services by submitting a new Order Form detailing the specific services required. Comtrac agrees to evaluate the Customer's request for additional Comtrac Services promptly and provide a response within a reasonable timeframe.

Multi-Tenancy Beta Test/UAT Environment

Comtrac maintains a development, beta, and testing environment to allow for troubleshooting, demonstration, training, development and beta-testing of new features and functionality prior to being released into Customer Owned Environments.

Comtrac may at its sole discretion invite a Customer to participate in User testing in the Comtrac Cloud Multi-Tenancy Beta Test/UAT Environment. All Customers accessing Comtrac Services provided through Verinote-Beta.comtrac.com are obtaining the Contract Services through a Multi-Tenancy Beta Test/UAT Environment.

Customers accessing the Multi-Tenancy Beta Test/UAT Environment are strictly prohibited from entering any information or data which is real, legitimate, or sensitive. Comtrac cannot and will not guarantee the confidentiality of Confidential Information or Customer Data, integrity, or availability Comtrac Services in the Multi-Tenancy Beta Test/UAT Environment.

There are no Fees and Charges to the Customer for consuming this Comtrac Cloud Multi-Tenancy Beta Test/UAT Environment, however the Customer's access to this Comtrac Multi-Tenancy Beta Test/UAT Environment and duration of access is at the sole discretion of Comtrac.

Risks from multi-tenancy (general): The workloads of different clients may reside concurrently on the same system and local network, separated only by access policies implemented by a provider's software. A flaw in the implementation or in the

provider's management and operational policies and procedures could compromise the security of Confidential Information and Customer Data and Users.

Customer Owned Environments for Comtrac Services

Comtrac may, at the Customer's request contained in the Order Form deploy Comtrac Services within Customer managed cloud infrastructure, either in Australia or otherwise. This is deemed a Customer Owned Environment.

If a Customer Owned Environment for Comtrac Services is requested by the Customer, Comtrac will work with the Customer to establish the required resources to supply the Comtrac Services in this environment. The Customer must provide all access, information and assistance required by Comtrac in order for Comtrac to provide the Comtrac Services in the Customer Owned Environment.

The provision of and use by a Customer of a Customer Owned Environment for Comtrac Services will attract a one-off dee and bespoke development fees payable to Comtrac as outlined in the Order Form.

Expenses, including cloud storage costs, relating to the running of this Customer Owned Environment for Comtrac Services are the sole responsibility of the Customer.

Limitations: The Customer acknowledges and agrees that using the Customer Owned Environment:

- Limits Comtrac's ability to ensure the same security provisions as with Comtrac Cloud Environments. Comtrac will provide template infrastructure documents and provisioning guides, however, Comtrac takes no responsibility for any Claim, Loss, or failings within the Customer Owned Environment for Comtrac Services, or in respect of the infrastructure or provisioning guides provided by Comtrac;
- Limits Comtrac's ability to comply with Service Level Commitments within the Service Level Agreement. Service Level Credits will not be applicable to a customer who uses a Customer Owned Environment; and

- The deployment of Revisions, Minor Versions and Major Versions, updates, patches, fixes, and new features or functions may also be delayed in the Customer Owned Environment.

Cloud Security - Disclosure of Risk

All Customers and Users should be aware of the security issues that exist in cloud computing and of applicable NIST publications such as NIST Special Publication (SP) 800-53 "Recommended Security Controls for Federal Information Systems and Organizations." As complex networked systems, clouds are affected by traditional computer and network security issues such as the needs to provide data confidentiality, data integrity, and system availability.

By imposing uniform management practices, clouds may be able to improve on some security update and response issues. Clouds, however, also have potential to aggregate an unprecedented quantity and variety of customer data in cloud data centres. This potential vulnerability requires a high degree of confidence and transparency that cloud providers can keep customer data isolated and protected. Also, cloud users and administrators rely heavily on Web browsers, so browser security failures can lead to cloud security breaches.

The privacy and security of cloud computing depends primarily on whether the cloud service provider has implemented robust security controls and a sound privacy policy desired by their customers, the visibility that customers have into its performance, and how well it is managed.