

ANNEXURE B – SERVICE LEVEL AGREEMENT

1. Introduction

This document describes the Service Level Agreement (SLA) in regards to the Claratti Voice and Data services, specifically in relation to the following data communications services (together referred to as the “Services”):

- 1.1. Claratti Voice and Data Secure Private IP Data & Public Internet
- 1.2. Claratti Voice and Data Co-location Connectivity
- 1.3. Claratti Voice and Data VPNs and IPSEC Tunnels
- 1.4. Claratti Voice and Data Managed Network Security
- 1.5. Claratti Voice and Data Managed Wi-Fi

2. Definitions and Scope

- 2.1. Definitions
 - 2.1.1. ‘We, Our, Us’ is Intelligent IP Hosting Pty Ltd, T/A Claratti Workspace “Claratti”;
 - 2.1.2. ‘Client, You, Your’ is the business Client using Claratti provided Service(s);
 - 2.1.3. ‘Client Premises Equipment’ or ‘CPE’ is the equipment at your site, which may be owned by Claratti or You, which has is used to provide the Service(s);
 - 2.1.4. ‘Communication’ means the method by which we will endeavour to contact the nominated;
 - 2.1.5. ‘Technical Client Contact’ is the person or persons which You will be directed to communicate with via email, SMS or telephone call;
 - 2.1.6. ‘Coverage Window’ refers to our hours of operation for service response and restoration activity. Our Support team are operational 24 hours per day, 7 days per week and 365 days per year; otherwise, stated as 24x7x365;
 - 2.1.7. ‘Critical Faults’ are all issues affecting the Service(s), including degradation of a ll of the Service(s) requiring immediate attention;
 - 2.1.8. ‘Support Tickets’ is the process of allocating, tracking and reporting on the issues which relate to the Service(s) We provide to You. For the avoidance of doubt all Faults must be allocated a Support Ticket, regardless of the nature of the Fault or the time or resources required to resolve the Fault. Furthermore, all Faults shall be logged against Your account within our ERPM system;
 - 2.1.9. ‘Non-Critical Faults’ are issues affecting the Service(s), including degradation of some of the Service(s) requiring attention;
 - 2.1.10. ‘Packet Loss’ means the average percentage of IP packets transmitted that are not successfully delivered, as measured by Us;
 - 2.1.11. ‘Point of Aggregation’ or ‘POA’ means Point of Aggregation;

- 2.1.12. 'Response Time' is the time from when we receive a Critical Fault or Non-Critical Fault notification from You and from the time in which a technical resource is allocated to conduct the initial diagnosis and fault rectification. Where possible, we will endeavour to provide a status advice to you with an indication of the nature of the fault and estimated time to restore the service;
 - 2.1.13. 'Restoration Time' is the time from when we receive a Critical Fault or Non-Critical Fault notification from You and from the time the Service(s) are restored;
 - 2.1.14. 'Service Activation' means the date from which we determine the Service has been delivered, tested and ready for use;
 - 2.1.15. 'Service Availability' is defined as the percentage of time each service (or if redundancy has been included, the solution) is available to the Client during the course of a year;
 - 2.1.16. 'Service Centre' is the online customer portal and is accessible <https://claratti.com>;
 - 2.1.17. 'Service Installation Lead Time' is the estimated number of business days from when we receive confirmation that the required infrastructure is available to provide the Service(s) to the time that the Service(s) are physically installed at Your premises;
 - 2.1.18. 'Service Levels' means the service levels as specified in this Service Level Agreement and as updated by us from time to time;
 - 2.1.19. 'Service Level Agreement' means this document published (and any updates published from time to time by Claratti Systems Engineering Team) which describes the Service Levels for our relevant services and the applicable rebates (if any);
 - 2.1.20. 'Site Visit' is where Claratti, a nominated representative or field engineer is required to attend your premises;
 - 2.1.21. 'Unavailable Hours' is the total number of hours that the service is unavailable due to issues with our network, except for planned service outages. Our monitoring system will be the basis for determining Service Availability;
- 2.2. Scope
- 2.2.1. This document outlines the Service Levels associated with our data communications services;
 - 2.2.2. This document relates to the physical and network technologies, which we use to deliver our Service(s);

3. Fault Reporting

You are responsible for notifying Us of technical Faults, which You believe are impacting your business, whether the Fault may be a Critical Fault or Non-Critical Fault.

In cases where you believe the Fault is not related to Your equipment, but in our network, the Fault is to be logged by phone 1300 073 085 (+61 8 6494 1000 if overseas), or online <https://Claratti.com/> or email support@Claratti.com by you. All Faults logged will be issued with an incident number. This incident number, all email correspondence and notes relating to the Fault will be stored within our systems.

Response times may vary depending on the nature of the Fault, technical staff availability and the coverage window, the type of service affected and how the Fault is reported. Response times and coverage windows are described in sections 4 and 5 respectively. Non-Critical Faults will be attended too, once Critical Faults have been resolved and/or within a 24 hour period, from the time the Fault has been lodged by phone or by emailing support@Claratti.com.

Please note that fees may be charged for time expended by our technical staff in response to Faults logged that are deemed to be the responsibility of You or Your devices or otherwise conditions outside of our control “force majeure” which are impacting our Service(s).

4. Response and Restoration Targets

4.1. Response Times

4.1.1. Response Times for Faults Logged via Telephone

TIME PARAMETER (AS PER SECTION 5) FOR CRITICAL FAULTS	TARGET TIMES	APPLICABLE SERVICES
All hours	Up to 30 Minutes	All Services

4.1.2. Response Times for Faults Logged via Email

TIME PARAMETER (AS PER SECTION 5)	TARGET TIMES	APPLICABLE SERVICES
All Hours	Up to 24 Hours	All Services

4.2. Restoration Times

4.2.1. Faults Logged During Business Hours

PARAMETER	SERVICE LOCALITY	TARGET TIMES	APPLICABLE SERVICES
Restoration Time	CBD/Metropolitan	Up to 12 Business Hours	All Services
Restoration Time	Regional	Up to 24 Business Hours	All Services

NOTES: Restoration time targets apply on the basis that a site visit is not required to rectify the Fault. If an engineer is required to visit Your premises, longer restoration times can be expected.

5. Coverage Window

TIME CATEGORY	TIME DEFINITION
Business Hours	Monday to Friday*: 8:30am to 5:30pm Local Time
Non-Business Hours	All other times outside of Business Hours

NOTES: *National public holidays are considered Non-Business hours

6. Fault Restoration

6.1. Service restoration targets are conditional on our or an approved representative having access to Your premises and equipment;

- 6.2. Upon restoration of the service, We will contact You and confirm that the Service(s) is operating satisfactorily;
- 6.3. In the case of a prolonged outage, We may provide a more detailed response on Your request.

7. Proactive Notifications

7.1. **Unscheduled Service Outage Monitoring and Notifications**

- 7.1.1. By default, all network attached devices and all hosted Service(s) which We provide, will be proactively monitored;
- 7.1.2. You will be provided notifications from our monitoring platform(s) as the state of the device or Service(s) change from up to down or vice versa;
- 7.1.3. It is Your responsibility to supply Us with a “how to respond” policy, so both parties can understand how outages and state changes are to be communicated in respect to who, how and when;
- 7.1.4. Our monitoring system operates 24x7x365 and pro-actively monitors our Service(s), as well as automatically generates a new ticket, as well as automatically closes a ticket once the state of a Service(s) returns to a normal condition. You are not required to log a ticket in this instance;
- 7.1.5. You may also be provided a web-based portal or interface, where You can view the status of any Service(s) which we provide.

NOTE: It is Your responsibility to maintain the correct contacts email addresses and contact details for Your nominated staff members.

7.2. **Planned Service Outage Notifications**

- 7.2.1. We may plan a service outage to conduct necessary maintenance and upgrades our Service(s) or our infrastructure which we use to provide the Service(s). We will use reasonable efforts to provide a minimum of 5 business days notification of any planned service outage;
- 7.2.2. We will notify all affected clients and will provide details of the Planned Service Outage(s);
- 7.2.3. In circumstances where an emergency service outage is required, we reserve the right to undertake the Planned Service Outage(s) without notice. In such cases we will endeavour to notify you prior to any Planned Service Outage(s).

8. Service Availability, Latency and Packet Loss

8.1. Service Availability Targets

- 8.1.1. Service availability is calculated in accordance with the following formula:
- 8.1.2. Service Availability = Total hours for the period (30 calendar days) less Unavailable Hours / Total hours for the period (30 calendar days) x 100.
- 8.1.3. Managed Wi-Fi coverage and Uptime is offered on a Best Effort basis only.

PARAMETER TARGET SERVICE	AVAILABILITY	APPLICABLE NETWORK ACCESS SERVICES
Service Availability	Not applicable	All VPN and IPSEC tunnel products, NBN Residential
Service Availability	99.5%	NBN Business
Service Availability	99.5%	All DSL and Wireless Ethernet services
Service Availability	99.9%	All Ethernet

8.2. Target Service Latency Parameters

Service Latency is defined as the amount of time in milliseconds that is required for one single packet of 56 bytes to travel between our core and the CPE and back to our core. The latency is measured over a time interval of 15 Minutes, during which time your service is no more than 70 per cent utilised. Latency Targets are only applicable to services terminating in Australia.

Parameter	Max. Time in Milliseconds	Applicable network access Services
Service Latency	80 Milliseconds	All Ethernet services
Service Latency	100 Milliseconds	All DSL and NBN Residential based services
Service Latency	Not Applicable	Mobile Broadband, Co-location Connectivity, Virtual Hosting Connectivity, VPNs, Managed Network Security

Out of parameter latency is proactively monitored by our Monitoring Software, but you are not notified when such events are detected due the transient nature of data network behaviour. Out of parameter latency does not automatically entitle you to a Fee Rebate.

8.3. Service Packet Loss

Measurement of packet loss by us is defined as a loss of transmission of IP packets between our core and the CPE and back to our core. The packet loss is measured over a time interval of 15 Minutes, during which time your service is no more than 70 per cent utilised.

PARAMETER	MAX. PACKET LOSS TARGET	APPLICABLE SERVICES
Service Packet Loss	1%	All Ethernet, services
Service Packet Loss	2%	All NBN residential and DSL based services
Service Packet Loss	5%	Mobile Broadband

9. Fee Rebates Due to Service Unavailability

9.1. Fee Rebate

Where a service unavailability is attributed to our network and your service does not meet the target service availability stipulated in Section 8.1, then you may request us to provide a service fee rebate as follows:

CONTINUOUS SERVICE UNAVAILABILITY	SERVICE LOCALITY	REBATE AS A % OF MONTHLY RECURRING FEE†	APPLICABLE SERVICES
More than 90 Minutes but less than or equal to 4 Hours	CBD/ Metropolitan	5%	All Ethernet, Managed Network Security services and all services with a Claratti Voice and Data Failover service
More than 24 Hours but less than or equal to 48 hours	Regional		
More than 4 Hours but less than or equal to 6 hours	CBD/ Metropolitan	15%	All Ethernet, Frame Relay, Managed Network Security services and All services with a Claratti Voice and Data Failover service
More than 48 Hours but less than or equal to 72 Hours	Regional		
More than 6 Hours	CBD/ Metropolitan	25%	All Ethernet, Frame Relay, Managed Network Security services and All services with a Claratti Voice and Data redundancy solution
More than 72 Hours	Regional		

†The Monthly Recurring Fee mentioned above only refers to our invoiced charges and does not include charges invoiced directly to you by any other provider, e.g. ISDN charges incurred by you from a provider other than us.

- 9.2. Application for Rebate
- 9.2.1. Rebates will be provided upon submission of a written request from you to our Client Manager. The written request should be received by us within 14 days of the service unavailability.
- 9.2.2. Upon receipt of the written request, we will assess and calculate the rebate due to you. All applicable rebates will be provided in the form of a credit on your next monthly bill.
- 9.2.3. You are only eligible for a rebate if a ticket was logged directly relating to the fault experienced and the service is in contract with us.
- 9.2.4. The fee rebate corresponds to the accumulated service unavailability, as measured by our Monitoring System, in a given month and can only be claimed once.
- 9.2.5. A rebate does not apply in instances where:
- 9.2.5.1. You failed to provide access to their premises to repair a service outage
- 9.2.5.2. You failed to co-operate with our technical staff in undertaking basic diagnostic tasks required to rectify the fault
- 9.2.5.3. The service unavailability is the direct result of a Planned Service Outage (See Section 7.2)
- 9.2.5.4. The service unavailability is the direct result of events beyond our control
- 9.2.5.5. You have modified or changed any aspect of the original installation without our consent
- 9.2.5.6. You failed to notify us of a fault with the service.

10. Service Installation Lead Times

DESCRIPTION	ITEM
ADSL	20-25 Business Days
NBN - (TC-4 - Residential Grade)	25-30 Business Days (depending on NBN NTD's being installed onsite)
NBN Biz - (TC 2) / EoNBN	40 Business Days
NBN Enhance (TC-4 with 4G Failover)	10 Business Days with provision of Claratti Voice and Data SIM service
3G/4G - Fixed Mobile Broadband	10 Business Days
Ethernet over Copper - On Net	30-40 Business Days
Ethernet over Copper - Off Net	40 Business Days
Fixed Wireless	25-30 Business Days
Ethernet over Fibre - On Net	40 Business Days

Ethernet over Fibre - Off Net (Complex Build involved)	80 Business Days
Dark Fibre - On Net	40 Business Days
Dark Fibre - Off Net (Complex Build involved)	80 Business Days
Co Lo Rack Space (excludes Cross connects)	10 Business Days
Co Lo BPIP	10 Business Days
Co Lo Internet	10 Business Days
Virtual Ethernet	5 Business Days
Virtual Firewall Internet	5 Business Days
Virtual DMZ	5 Business Days
Domain Hosting (Nameserver / zone files setup only)	5 Business Days
Domain Registration / Transfer and Hosting	7 Business Days
IP Address	5 Business Days
PSTN Lines (New Install to the MDF and not including patching to the socket)	10-15 Business Days
SIP Trunk Setup only (dependent on Claratti WAN Link being active) and New Numbers assigned	5 Business Days
SIP Lines including Porting of Numbers (dependent on Claratti WAN Link being active)	40 Business Days
Hosted PBX - Handset and Licenses only (dependent on Claratti WAN Link being active and New Numbers being assigned) No Porting included	20 Business Days
Conversion between Internet and BPIP services	5 Business Days
Compatible Router Changes and Policy Configurations	5 Business Days
Managed Network Devices Setup - Existing Hardware - No Network Discovery required	7 Business Days
Managed Network Devices Setup - New Claratti Procured Hardware	20 Business Days
IPSec / Secure Site with CPE	20 Business Days

IPSec / Secure Site without CPE	10 Business Days
Managed Wi-Fi Network Service	Configuration - 10 Business Days from Hardware receipt Management - 7 Business Days from site installation and controller connectivity

- 10.1. Actual service delivery timeframes may be longer depending on the nature of the work to be completed.
- 10.2. A more precise estimate of the actual service delivery time will be provided once an order has been received and assessed. This may not be available until any third party has performed their own assessment.
- 10.3. If a more precise estimate of service delivery time is required, a survey can be requested (charges may apply).
- 10.4. All service delivery times are approximate.
- 10.5. Modifications to Ethernet Fibre services such as speed changes vary in lead time depending on carrier, backhaul transmission technology and hardware capabilities. Lead times and pricing on service modifications to Ethernet Fibre services will be quoted on application.

11. Service Installation Communications

- 11.1. We will complete service provisioning within the timeframes stipulated in section 10. Service provisioning will be conducted during business hours. Orders cannot be processed without all relevant information.
- 11.2. While we cannot be liable for the acts or omissions of third parties, we will proactively communicate with you through the provisioning process and manage the installation so as to minimise any service provisioning delays.
- 11.3. Service provisioning milestones:
 - 11.3.1. Orders are acknowledged within one (1) business day of being received
 - 11.3.2. Confirmation of available infrastructure from Carrier, notification will be provided if service is unavailable
 - 11.3.3. You will be contacted to advise date of service installation
 - 11.3.4. We will arrange the appointment for the service installation
 - 11.3.5. We will contact you to confirm activation of the service
 - 11.3.6. Billing of the service will commence from date of Service Activation
- 11.4. Service delivery is conditional on access to third party suppliers, access to your premises and the installations being completed by us or an approved representative.

12. Rebates Due to Service Installation Delays

- 12.1. Where we do not activate the service within the Service Installation Lead Time and it is our fault, a rebate will be provided. Service installation rebates apply to new services and service relocations only.
- 12.2. Rebates will be provided upon submission of a written request from you to our Client Manager. The written request should be received by us within 14 days of the relevant service installation lead time target not being met.
- 12.3. Rebates will not be applicable for service installation delays that were requested or caused by you, or for orders with an agreed installation date that falls outside of the

service installation lead time target. The service installation lead time target is subject to confirmation of infrastructure availability.

SERVICE ACTIVATION DELAY (WHOLE BUSINESS DAYS BEYOND SERVICE INSTALLATION LEAD TIME TARGET)	REBATE % OF SETUP FEE	APPLICABLE SERVICES
From 1 to 10 Days	10% ^{*1}	All Claratti Voice and Data Services
From 11 to 20 Days	20% ^{*1}	All Claratti Voice and Data Services
More than 20 Days	25% ^{*1}	All Claratti Voice and Data Services

^{*1} - Rebate excludes NBN services

13. The Claratti Voice and Data Network

13.1. Network Bandwidth Availability

We maintain a strict policy of active capacity management on our Australia wide core network. This policy is one of intensive monitoring that result in national bandwidth/backhaul being highly available at all times.

13.2. Claratti Voice and Data Managed Network Devices

13.2.1. We maintain ownership of, monitor and manage routers supplied by us as part of a Data Networking or Business Internet service.

13.2.2. Our router management includes the initial configuration and subsequent additions, modifications and changes to the configuration as deemed necessary by us or as required by you.

13.2.3. In addition, and subject to prior approval by us, we will also manage compatible routers supplied by you.

13.2.4. It is an express condition of this SLA that the entire SLA will only apply to services where we have the sole exclusive management access to the router for management and monitoring purposes.

13.3. Claratti Voice and Data Router "Hot Swap" Policy


As a component of our router management, we maintain a router "Hot Swap" policy to minimise service disruption resulting from a faulty router. The features of this policy are:

13.3.1. This policy applies if you are within the initial term of your agreement with us, or a subsequent term. If your agreement term has expired and you are now on a month by month arrangement this policy doesn't apply.

13.3.2. This policy only covers routers that are found to be faulty in the normal course of their intended use. It does not extend to insurable damage such as accidental or malicious damage, fire, water damage and the like.

13.3.3. Only routers supplied and managed by us are covered by this policy.

13.3.4. We will configure and courier, at no cost to you, a like model



replacement router (the same as the model originally provided to you, or if not available, one with similar functionality necessary to provide the same service) to You provided that the faulty router is simultaneously returned to us.

We will use reasonable efforts to achieve this swap within 24 hours or better. This time period may vary where extended courier times are experienced.

13.4. Claratti Voice and Data Redundant (Failover) Services

We recommend that all data services deemed critical to your business should have redundant services provisioned.

14. Service Level Agreement Terms and Conditions

- 14.1. The SLA terms and conditions set out in this document are incorporated into and form part of our Product Terms.
- 14.2. All terms have meanings as per the Interpretations section in our Standard Form of Agreement.
- 14.3. We will use reasonable endeavours to meet the Service Levels for the Service.
- 14.4. If we fail to achieve the relevant Service Levels as set out in the Service Level Agreement, you will be entitled to a rebate, calculated by reference to the percentage rate rebate specified in the Service Level Agreement.
- 14.5. Notwithstanding any other provision of the Service Level Agreement, you will not be entitled to a rebate where our failure to achieve the relevant Service Level is caused directly or indirectly by:
 - 14.5.1. any act or omission by you or any third party;
 - 14.5.2. planned service outages;
 - 14.5.3. unscheduled maintenance in cases of emergency service interruption; or
 - 14.5.4. components of the Service provided using facilities outside the direct control of us;
 - 14.5.5. a Force Majeure event such as natural disasters and power failures.
- 14.6. You agree that to the extent permitted by law, any rebate payable by us to you pursuant to this clause, will be the sole remedy available to you in respect of the event giving rise to the rebate entitlement.
- 14.7. Your continued use of existing Services and the ordering of new Services after the introduction of this Service Level Agreement shall be deemed to constitute acceptance of our Standard Form of Agreement of this Service Level Agreement.

ANNEXURE C – ACCEPTABLE USE POLICY

Introduction

Claratti Workspace takes the subject of information security very seriously. We have a duty to protect the information that we collect and use for the benefit of the organization and its customers. As an employee, you will be expected to comply fully with all of the information security policies that are in place and to report any breaches of these policies of which you may become aware.

This document gives a summary of the main points of the relevant policies and asks you to sign to say that you have read it and understand its provisions.

Anyone breaching information security policy may be subject to disciplinary action. If a criminal offence has been committed, further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, please seek advice from your immediate manager in the first instance.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Claratti Workspace systems.

The following policies and procedures are relevant to this document:

- *Information Security Policy*
- *Electronic Messaging Policy*
- *Internet Acceptable Use Policy*
- *Mobile Device Policy*
- *Teleworking Policy*
- *Privacy and Personal Data Protection Policy*
- *Cloud Computing Policy*
- *Asset Handling Procedure*
- *Software Policy*
- *Access Control Policy*
- *Anti-Malware Policy*
- *Information Security Incident Response*

Procedure


- *IP and Copyright Compliance Policy*
- *Social Media Policy*



Acceptable Use Policy

Please ensure you have read the following summary of the main points of the organization's policies with regard to information security.

1. I acknowledge that my use of a Claratti Workspace computer and communications systems may be monitored and/or recorded for lawful purposes.
2. I acknowledge that Claratti Workspace may monitor my keystrokes inputs on all Claratti Workspace owned and managed devices for analysis, audit and legal requirements
3. I acknowledge that authorized individuals within Claratti Workspace may monitor equipment, network and systems traffic at any time
4. I acknowledge that Claratti Workspace may reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
5. I accept that I am responsible for the use and protection of the user credentials with which I am provided (user account and password, access token or other items I may be provided with)
6. I will not use anyone else's user account and password to access company systems
7. I will not attempt to access any computer system to which I not been given access
8. I will protect any classified material sent, received, stored or processed by me according to the level of classification assigned to it, including both electronic and paper copies
9. I will ensure that I label any classified material that I create appropriately according to published guidelines so that it remains appropriately protected
10. I will not send classified information over the Internet via email or other methods unless appropriate methods (e.g. encryption) have been used to protect it from unauthorised access
11. I will always ensure that I enter the correct recipient email address(es) so that classified information is not compromised
12. I will ensure I am not overlooked by unauthorised people when working and will take appropriate care when printing classified information
13. I will securely store classified printed material and ensure it is correctly destroyed when no longer needed
14. I will not leave my computer unattended such that unauthorised access can be gained to information via my account while I am away

- 
15. I will make myself familiar with the organization's security policies and procedures and any special instructions relating to my work
 16. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security or if I observe any suspected information security weaknesses in systems or services
 17. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended
 18. I will not remove equipment or information from the organization's premises without appropriate approval
 19. I will take precautions to protect all computer media and mobile devices when carrying them outside my organization's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft)
 20. I will not introduce viruses or other malware into the system or network
 21. I will not attempt to disable anti-virus protection provided at my computer
 22. I will comply with the legal, statutory or contractual obligations that the organization informs me are relevant to my role
 23. On leaving the organization, I will inform my manager prior to departure of any important information held in my account

Declaration

I have read the information security policy summary above and agree to comply with its contents and those of any other relevant policies of which the organization may make me aware.

Name of User:

Signature of User:

Date:

A copy of this statement shall be retained by the User and Claratti Workspace.



ANNEXURE D – PRIVACY POLICY

Contents

1 INTRODUCTION	16
3 PRIVACY AND PERSONAL DATA PROTECTION POLICY.....	17
3.1 The General Data Protection Regulation	17
3.2 Definitions.....	17
3.3 Principles Relating to Processing of Personal Data	17
3.4 Rights of the Individual	19
3.5 Consent.....	19
3.6 Privacy by Design.....	20
3.7 Transfer of Personal Data.....	20
3.8 Data Protection Officer	20
3.9 Breach Notification	21
3.10 Addressing Compliance to the GDPR	21
3.11 Our Obligations as a Cloud Service Provider	22

List of Tables

<i>Table 1 - Timescales for data subject requests</i>	<i>19</i>
---	-----------



Introduction

In its everyday business operations Claratti Workspace makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organization is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Claratti Workspace is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Claratti Workspace systems.

The following policies and procedures are relevant to this document:

- *Information Classification Procedure*
- *Information Labelling Procedure*
- *Acceptable Use policy*
- *Electronic Messaging Policy*
- *Internet Acceptable Use Policy*
- *Information Security Incident Response Procedure*
- *Information Security Roles, Responsibilities and*

Authorities



Privacy and Personal Data Protection Policy

The General Data Protection Regulation

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that Claratti Workspace carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is Claratti Workspace's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

Definitions

There is a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

'Personal data' is defined as: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'processing' means: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'controller' means: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the GDPR is based.



These are as follows:

1. *Personal data shall be:*

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

2. *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

Claratti Workspace must ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management

system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment.

Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within Claratti Workspace that allow the required action to be taken within the timescales stated in the GDPR.


These timescales are shown in Table 1.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Table 1 - Timescales for data subject requests

Consent

Unless it is necessary for a reason allowable in the GDPR, explicit consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 (Note – this age may be lower in individual EU member states) parental consent must be obtained. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.



If the personal data are not obtained directly from the data subject, then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

Privacy by Design

Claratti Workspace has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more privacy impact assessments.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.


Transfer of Personal Data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.



Based on these criteria, Claratti Workspace does not require a Data Protection Officer to be appointed.

Breach Notification

It is Claratti Workspace's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

Under the GDPR the relevant supervisory authority has the ability to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

Addressing Compliance to the GDPR

The following actions are undertaken to ensure that Claratti Workspace complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
 - Organization name and relevant details
 - Purposes of the personal data processing
 - Categories of individuals and personal data processed
 - Categories of personal data recipients
 - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
 - Personal data retention schedules

- 
- o Relevant technical and organisational controls in place

These actions will be reviewed on a regular basis as part of the management review process of the information security management system.

Our Obligations as a Cloud Service Provider

In addition to holding personal data on our own account, Claratti Workspace also stores and processes the personal data of our cloud customers. In doing so, there are a number of additional obligations that must be fulfilled to allow our customers to stay within the law. Our policy in this area is informed by *ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* which, as well as recommending specific enhancements to ISO/IEC 27001 controls, also provides the following policy guidance:

- We must provide our customers with the facilities to meet their obligations under law in activities such as accessing, amending and erasing individuals' PII
- We must only use the cloud customer's PII for their purposes, not our own
- The customer must be informed if we are required by law to disclose any of their data, unless we are prohibited from doing so
- Details of disclosures must be recorded
- We must tell our customers if we use sub-contractors to process their PII
- We must tell our customers if their PII is subject to unauthorized access
- It must be clear in which country or countries the customer's PII is stored

ANNEXURE E

PAYMENT AUTHORITY AUTHORISATION FORM

To: **Claratti Workspace**

MY DETAILS

Name:					
Company:	(the Company)				
Position:		ACN /		ABN:	
Address:					
City:		State:		Post Code:	

By completing the below, I authorise Intelligent IP Hosting Pty Ltd (ACN 619 361 018) trading as 'Claratti Workspace' (ABN 94 619 361 018) of Suite 10, 8 Welshpool Rd, East Victoria Park, Western Australia 6101 (**Claratti**) to direct debit my account or my credit card, as applicable, for any amounts which become payable by the Company to Claratti in connection with the Company's account. I certify that I, or we, in conjunction with the other signatory below (if applicable), am authorised to authorise the direct debit arrangement set out below and that I, or we, will not dispute any payments with my credit card company or bank, as applicable, so long as the transaction corresponds with the terms and conditions contained overleaf (**Direct Debit Terms**).

DIRECT DEBIT DETAILS (complete either Section 1 or Section 2)

Section 1 – Details of Bank Account to be Debited			
Bank Name:			
Bank Address:			
Account Name			
BSB:		ACC:	

Section 2 – Details of Credit Card to be Debited			
Cardholder Name:			
Credit Card No.:			
Credit Card Type:	Visa <input type="checkbox"/> Mastercard <input type="checkbox"/> Amex <input type="checkbox"/>		
BSB:		ACC:	
<input type="checkbox"/>	I / We acknowledge that this authority will stand in respect of the specified credit card and in respect of any card issued to me in renewal or replacement, until I notify Claratti of its cancellation.		


□	I / We agree that I have read and understood this credit authorisation form and the Direct Debit Terms set out overleaf and agree to be legally bound by signing below.
□	I / We consent to the use of personal information provided in connection with this Payment Authority Authorisation Form by Claratti for the purposes and on the terms set out within.

SIGNED

<i>Name of signatory</i>	<i>of</i>	<i>Signature</i>	<i>of</i>	<i>Name of signatory</i>	<i>of</i>	<i>Signature</i>
<i>Position</i>		<i>Date</i>		<i>Position</i>		<i>Date</i>

DIRECT DEBIT TERMS

1. These Direct Debit Terms form a part of, and are to be read with, our standard terms and conditions which govern your agreement with us (**Terms**).
2. In these Direct Debit Terms, capitalised terms that are defined within our Terms have the same meaning.
3. If there is any inconsistency between any of the provisions of these Direct Debit Terms and the Terms, the Terms will prevail to the extent of any inconsistency.
4. By executing this Payment Authority Authorisation Form, you authorise us to arrange for payments of all amounts due and payable to us pursuant to our Terms.
5. As set out in our Terms, an Invoice will be provided to you prior to us exercising this Payment Authority and payment will be made no earlier than 10 Business Days after providing you with an Invoice.
6. If any payment made pursuant to this Payment Authority is dishonoured or rejected by your financial institution, we will contact you to arrange for an alternative payment method and, in the event payment is not made by you by the relevant due date, we reserve the right to impose interest in accordance with our Terms. In the event that any charges are imposed on us by your financial institution in connection with a dishonoured or rejected payment, these charges will be passed on to you for payment as an Expense in accordance with our Terms.
7. You agree and acknowledge that you will:
 - (a) ensure your nominated account or card can comply with the direct debit arrangement that forms this Payment Authority;
 - (b) ensure there are sufficient clear funds available in your nominated account or card to pay all amounts due and payable by you at the time they are due for payment in accordance with our Terms;
 - (c) advise us if your nominated account or card is transferred or closed, or if the details change; and
 - (d) ensure that all account holders of the nominated account or card have signed and executed this Payment Authority Authorisation Form.
8. You may, on request, ask that we verify that your Payment Authority with us is in accordance with these Direct Debit Terms and your executed Payment Authority Authorisation Form.

- 
9. You may cancel this Payment Authority at any time by contacting us at [billingteam@claratti.com], at which point we will cancel this Payment Authority within 3 Business Days. However, by cancelling this Payment Authority, you will be responsible for paying all Invoices and any failure to pay an outstanding Invoice may result in interest being incurred in accordance with our Terms. If you elect to cancel this Payment Authority we may, in our absolute discretion, choose to terminate your agreement with us in accordance with our Terms.
 10. In the event that any payment made out of your account in accordance with this Payment Authority is incorrect, we will ensure that you receive a full and timely refund of any excess amount paid or, undertake any other appropriate action that both you and we agree, such as crediting your account with respect to any future payments.
 11. If you consider a payment has been made pursuant to this Payment Authority incorrectly, please contact [Claratti Billing team] as soon as practicable.
 12. We will provide you 30 days prior written notice of any amendments to these Direct Debit Terms.
- 