w

tambla
Intelligent workforce solutions

Support & Maintenance Policies

Version v12.0 6th November 2023
Commercial in Confidence

Document Information

Document ID	Support and Maintenance Policies
Document Owner(s)	David Thompson
Issue Date	6th November 2023

Document History

Version	Date Issued	Author	Comment
5.7	19/10/2018	Lee Alexander	Branding update
5.8	22/01/2019	Lee Alexander	Updated telephone numbers
5.9	09/09/2019	Nathan Thomas	Tambla branding & service desk update
6.0	04/12/2019	Nathan Thomas	Updated contacts
7.0	25/02/2020	Richard Mitton & Nathan Thomas	Tambla SaaS updates
8.0	01/04/2021	Dave Thompson	Organisation update
9.0	23/07/2021	Nathan Thomas	Completed review
10.0	21/11/2022	Nathan Thomas	Updated 24/7 Hours of Operation for P1
11.0	10/07/2023	Dave Thompson	Update to organisation and escalation
12.0	06/11/2023	Dave Thompson	Change to organisation and escalation

Table of Contents

1. Tambla Support and Maintenance Policies

1.1 Purpose

The Tambla Support and Maintenance Policies ("Policies") form part of our agreement with each of our end-user customers and are an integral part of our engagement and ongoing relationship with our customers. Following the successful implementation and delivery of our software solutions, the responsibility for your account within Tambla moves from our project team to our service desk and account management teams.

This document describes that change of relationship and establishes the framework in which Tambla, and the Customer will continue to engage with one another. It also describes the scope and details of our Support and Maintenance Services for your solution.

This document constitutes the Policies referenced in the Tambla Software Licence, Equipment and Services Agreement and the Master Hosted Service, Managed Service and Consultancy Agreement.

1.2 Tambla Contacts

Key contact persons are available to assist you. It would be best to refer to the contacts template completed as part of your account implementation. The below includes the template of Key Contacts for your account.

Tambla Contact	Contact Details	
Tambla Service Desk	Australia: 1800 848 908 International: +61 2 9122 6200 Standard: Mon Fri 08:30 to 17:30 AEST, excluding national public holidays.	tsd@tambla.net Tambla Customer Portal https://tambla.accelo.com/portal
CX Manager Brent Tweedale	+61 3 9907 9711	brent.tweedale@tambla.com.au
Director of Sales and Customer Experience Dave Thompson	+61 2 9122 6232 +61 404 183 344	david.thompson@tambla.com.au
Chief Operating Officer Nathan Thompson	+61 2 9122 6280	nathan.thomas@tambla.com.au
Account Management Ily Dean	+61 2 9122 6200	Ily.dean@tambla.com.au
Partnership Account Manager Kimberly De Leon	+61 2 9122 6200	Kimberly.deleon@tambla.com.au

1.3 Overview

Tambla's Support and Maintenance Services includes the following components:

- Support Services for our Software, including:
    - Service Desk
    - the right to receive Updates and New Releases.
- Maintenance Services for our Equipment, including:
    - Service Desk
    - Warranty claim services and Servicing (Clocks).
    - Support for our Hosted Service and Self Hosted.
- Service Desk
    - Updates and New Releases to the Software component of the Hosted Service.
    - Maintenance of the hosting infrastructure.

These Policies form part of your Agreement with Tambla and may be updated. Updated versions of the Policies will be posted on our website. Upon agreement, updated policy versions can be provided by the customers' respective account managers.

If you have any comments on our Policies, please send your feedback to tsd@tambla.net

2. Tambla Service Desk

The Tambla Service Desk (TSD) provides a Single Point of Contact (SPoC) for advice, guidance and service restoration. All TSD Services will be provided in English.

The TSD should be contacted only by your internal support team, who are technically competent and knowledgeable about our Software, Equipment and Services and the technical and business environment in which they operate.

You are responsible for triaging any end-user issue and using your best efforts to resolve the issue before calling the TSD. Your support team is responsible for liaising with end-users when we provide a solution, remedy or workaround.

The TSD handles all incoming calls and automated tickets and is staffed by a combination of first, second and third-tier TSD team members.

2.1 Service Hours

The table below outlines the Service options. The Customer Agreement will include which optional components are contracted.

Service Hours	Level 1 (TSD)	Level 2 (Functional SME)	Level 3 (Product SME)
Standard Service Hours	✓	✓	✓
Extended Business Day Hours of Operation (Optional, priced separately)	✓	✓	On-Call
24/7 Hours of Operation for P1 Incidents (Optional, priced separately)	✓	On-Call	On-Call

Table 2: Service Hours

2.2 Standard Service Hours

For all customers who have not signed up for Optional Support Hours, the TSD is staffed by service desk team members between 08:30 and 17:30 AEST on business days (Monday to Friday, excluding days that are gazetted as National Public Holidays).

2.3 Extended Business Day Hours of Operations (Optional)

The extended hours of operation of the TSD are Monday to Friday, 07:00 to 19:00 AEST on business days (Monday to Friday, excluding days that are gazetted as National Public Holidays).

2.4 24/7 Hours of Operation for P1 Incidents (Optional)

The 24/7 hours of operation for P1 incidents of the TSD are seven days a week – 24 hours a day, including national public holidays. P1 Incidents outside of standard operating hours must be logged as a ticket through the usual method, and a call placed to 1800 848 908. Follow the voice prompts to reach the correct team. Refer to the Service Levels – P1 definition/symptom.

2.5 Desktop Remote Access

The TSD team utilises desktop remote access through FastSupport.com. This allows the team to provide a faster resolution; as phone tag and data gathering steps are eliminated, more issues are resolved at first contact. To enable the Support team access, www.fastsupport.com has to be added to the safe customer list, allowing end-users access to the tool.

2.6 Tambla Customer Portal

The Tambla Customer Portal (TCP) allows customers to raise, view and update tickets directly to the TSD via https://tambla.accelo.com/portal. Access to the TCP will be provided via a request to tsd@tambla.net

All tickets should be logged directly in the TCP (via the URL above). However, for urgent service tickets, it is required that the TSD be called immediately after raising the ticket on 1800 848 908 or +61 2 9122 6280.

2.7 The TSD Focus

The primary focus of the TSD is incident management, request fulfilment and change management.

The TSD focus also includes configuration changes, moves, additions, and changes of existing data configuration, work rules and other items deemed to work as designed but require alteration of any solution-based configurations. The TSD team will handle and may manage these enquiries; however, fulfilment may be completed outside of the support team and will be subject to our Professional Services rate table pre-agreed charges. (Refer to Request Fulfilment Process).

The TSD should not be used for any 'how to use' enquiries. Where we receive these requests, we will recommend talking to your account manager to organise structured training for your employees.

2.8 The TSD Objectives

- The end-to-end management of incidents and service requests.
- Escalate incidents/service requests that cannot be resolved within agreed timescales.
- Provide quality, consistent customer service.
- Effectively communicate the status of your request/incident.
- Provide issue investigation & diagnosis.
- Ensure all relevant Tambla SPGs (service provider groups) and suppliers are informed of incidents and their responsibilities in resolution.
- Provide details of resolution and completion to enable closure of incidents.

Unless otherwise agreed, the TSD will provide updates through the Tambla Customer Portal, and you will be notified of any updates via email. To maintain focus on and provide timely responses to current issues, tickets waiting for your response or classified as "pending customer" may be closed after ten days of inactivity unless otherwise agreed in writing.

2.9 Escalation Management

Below is the Tambla Customer Escalation Hierarchy.

<table>
<tr><th colspan="5">Escalation Hierarchy</th></tr>
<tr><th>Focus Area</th><th>Level 1</th><th>Level 2</th><th>Level 3</th><th>Level 4</th></tr>
<tr><td>Support</td><td>Ticket Owner</td><td>CX Manager</td><td rowspan="2">Dir. CX</td><td rowspan="3">Managing Director</td></tr>
<tr><td>Account Management</td><td colspan="2">Account Manager or CX Manager</td></tr>
<tr><td>Projects</td><td colspan="2">Project Manager</td><td>COO</td></tr>
</table>

Table 3: Escalation Hierarchy

Details of staff escalation points can be found in Table 1: Tambla Contacts.

3. Service Champions

Every customer will be required to nominate and maintain a minimum of one Service Champion (SC). It is recommended that at least one of the SCs be operations and at least one be an SME in one of the following areas: Payroll, Administration, HR, or Operations.

All customer support requests MUST be filtered through the Service Champion(s). Support requests initiated by non-service Champions will receive a support response informing the user that the support request must come through the Service Champion.

All Service Champions must receive formal facilitated training with Tambla and be formally accepted as nominated Service Champion(s). New Service Champion(s) must also receive Tambla training (i.e., Service Champions cannot be transferred internally within the organisation).

It is the role of the Service Champion in your organisation to:

- Triage and Resolve Level 1 user-initiated requests.
- Complete all Tambla Support requests (via the TCP).
- Communicate support resolution back to their relevant users.
- Formally approve all change requests, bug fixes, and enhancements.
- Act as the primary contact between the Tambla Support team and the Customer and the provision of contact details.

Service Champions must provide the following assistance:

3.1 Single Point of Contact

- Act as the single point of contact for all of your end-users
- Dealing with basic 'user' issues, troubleshooting and general technical and business advice about the performance, functionality and operation of the Software or Equipment in the user's hardware, software, networking and business environment (including issues with [clocks]
- Being the sole liaison between the Tambla team and the Customer. Unless Tambla requests, Tambla will not deal directly with end-users; Tambla will only deal with your Service Champion(s).

3.2 Software

- The Service Champion is required to reproduce/replicate the error they have encountered in an unmodified version of the software (i.e. the current version of the software they are using) before raising an issue with Tambla;
- Initial diagnosis of functionality issues. If, after using reasonable efforts to diagnose and resolve a functionality issue, the issue remains unresolved, then your support team may raise an issue with Tambla
- Make reasonable attempts to resolve the issue first, including by consulting the Software online help, any documentation and Tambla's knowledge base of support-related issues
- Provide details of any error message.

3.3 Customer Hosted Software

- For customer-hosted software, provide details of the software installed, including the version number, hardware platform and operating system details;
    - Downloading, installing and testing patches, workarounds, updates and new releases in a non-production environment
    - Installing tested patches, workarounds, updates and new releases in your production environment.

4. Equipment (if applicable)

- Installing or managing the installation of 'user-installable' parts:
    - Asset tracking of all Equipment
    - Collecting Equipment from your end-users in the event of a product recall or safety issue
    - Sending and receiving shipments and deliveries of equipment and spares.

5. Service Levels

5.1 Priority Allocation

The TSD's priority allocation combines Impact and Urgency. The ticket priority focuses resource allocation so that appropriate actions are taken to deliver the Service Level Agreements (SLAs) to Tambla customers.

5.1.1 Key Terms

- Impact = is a measure of the extent of the Incident and of the potential damage caused by the Incident before it can be resolved.
- Urgency = is a measure of how quickly a resolution of the Incident is required.
- Priority = is a function of Urgency & Impact.

5.1.2 Impact Scale

Level	Impact Description
High	The Tambla solution is severely impacted; the systems are down, payroll cannot be processed, and no workaround is available.
Medium	The Tambla solution prevents specific business functions from being performed, an issue that impacts a business deadline, and no workaround is available.
Low	Various reporting/enquiry functions impacted/cosmetic, a workaround is available.

Table 4: Impact Scale

5.1.3 Urgency Scale

Level	Urgency Description
High	Has an immediate effect on the performance of time-sensitive or mandatory business activities. The absence of immediate action is likely to bring the department/business or the CEO into disrepute. A financial loss or penalty will be incurred if not resolved immediately.
Medium	Has an immediate effect on the performance of time-sensitive and/or mandatory business activities, but a viable workaround is available. A prolonged disruption is likely to bring the department/business or the CEO into disrepute.
Low	Has a limited effect on normal business operations and can be mitigated through an effective workaround(s). Has occurred outside business hours and restoration is achievable before the normal start of business.

Table 5: Urgency Scale

5.2 Priority Matrix

The Priority Matrix defines incident priority and is a function of Urgency & Impact.

		Impact		
		High	Medium	Low
Urgency	High	Critical - P1	High - P2	Normal - P3
	Medium	High - P2	Normal - P3	Low - P4
	Low	Normal - P3	Low - P4	Low - P4

Table 6: Priority Matrix

5.3 Service Level Agreements (SLAs)

Priority	Initial Response Time*	Status Updates*	Target Workaround *	Target Restoration (as soon as possible but a maximum of)
Critical P1	Within 30 minutes. Dependency: The Customer must call the TSD for P1 urgent priority issues.	Hourly or as agreed with the customer.	6 hours	Four business days.
High P2	Within 60 minutes. Dependency: The customer must call the TSD for high-priority P2 issues.	Every 2 hours or as agreed with the customer.	8 hours	14 business days.
Normal P3	Within one business day.	None	None	Next quarterly release.
Low P4	Within two business days.	None	None	A fix may be included in a future release.
Service Request	Within two business days.	None	None	Not applicable

Table 7: Service Level Agreements

Note: Best efforts will be used. Service levels for workarounds and full resolution will start once an environment can be set up that replicates the issue. At times, this may require the use of a copy of the Customer's database, in which case, target Service levels will begin from the time that the database is received and restored to an appropriate environment.

* Initial Response Time, Status Updates and Target workarounds are all measured against the Standard Service Hours.

Service Champion(s) must be available (and have access to your software) to assist when we are working on resolving an issue. If you do not provide a Service Champion during this time, we may downgrade the Priority status of the call.

6. Incident Management Process

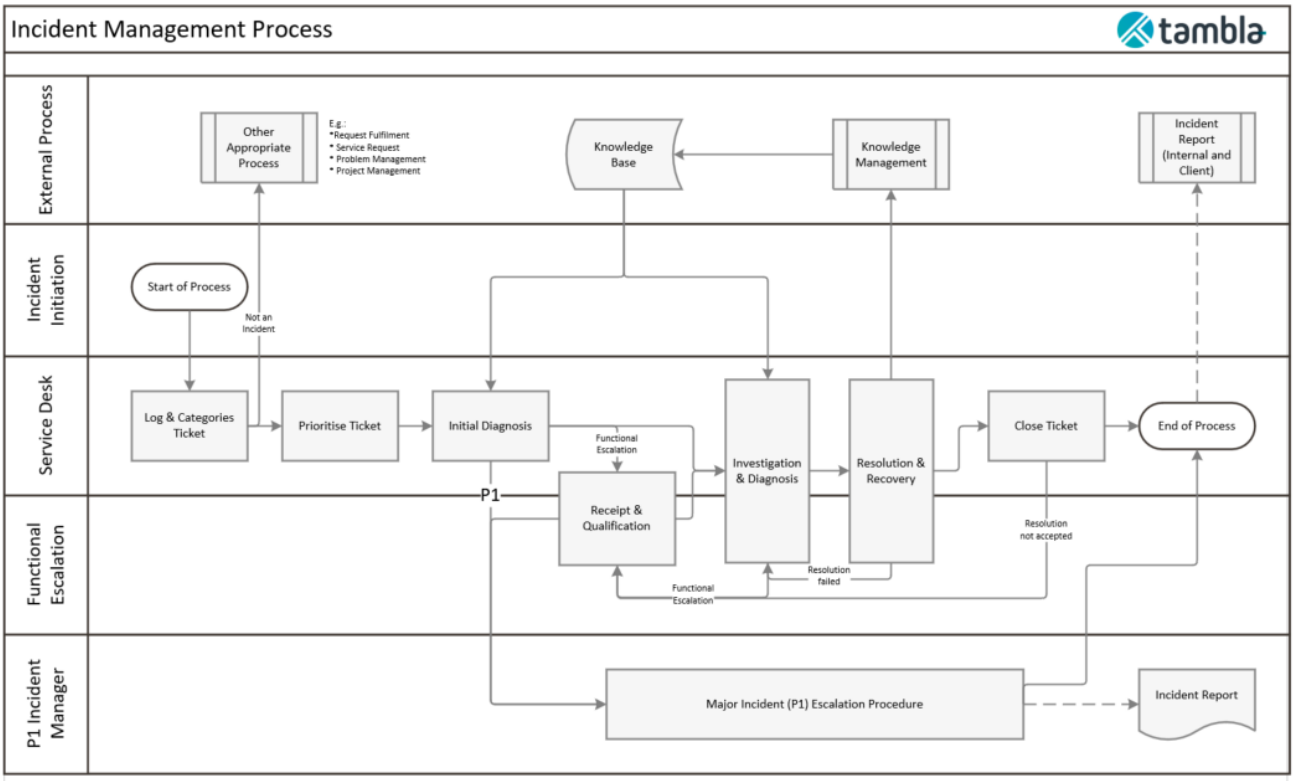

Figure 1: Incident Management Workflow Diagram

7. Update and New Release Process

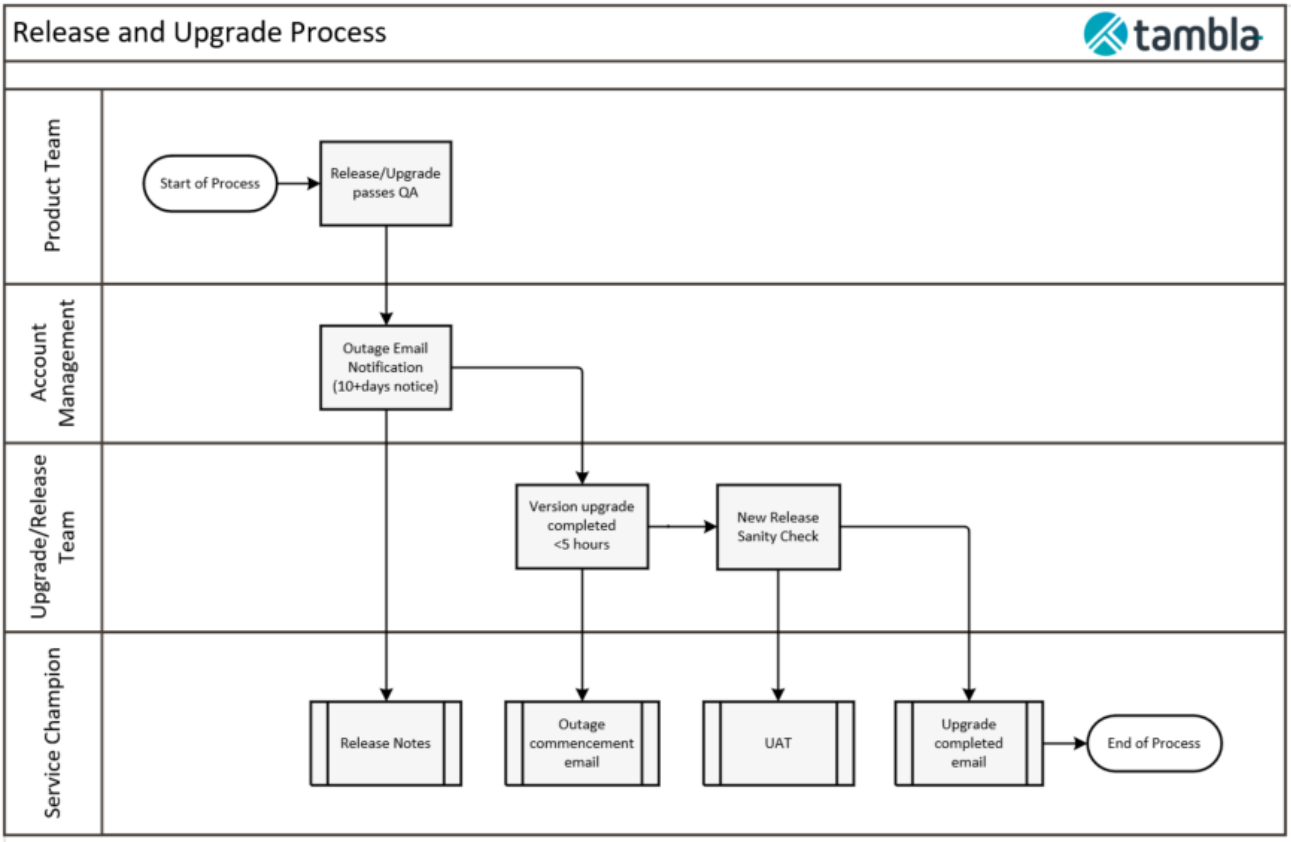

Figure 2: Release and Upgrade Workflow Diagram

7.1 Tambla SaaS Multi-tenant Shared Environment Customers

- When a new Software version update is ready for release, the deployment process is initiated.
- After the build has passed internal Testing (QA), an outage window is scheduled for deployment.
- You will be notified at least 10 Business Days in advance of any outage. This may be reduced for urgent or high-priority hotfixes.
- Outage windows are scheduled to occur in periods in which Tambla believe the least number of customers will be impacted.
    - This is typically completed on a Wednesday or Thursday night AEST.
    - Outage windows can last up to 5 hours.
- The customer will receive email notifications of Release Notes (including any bug fixes or issue resolution) and New Functionality Notes.
- The Tambla Update/Release team then facilitate the deployment.
- You will receive another email prior to the actual outage.
- You will receive another email upon completion of the outage.
- Tambla does not guarantee that any Update or New Release will be compatible with:
    - Any interfaces, whether made by Tambla or any other person

  - A version of any third-party software that is not included in the technical environment
  - Any independent scripts (SQL or stored procs) developed specifically for a Customer.
- Tambla is not under any obligation to create any future programs or functionality.

7.2 Tambla SaaS Dedicated Environment Customers

- All Tambla SaaS Dedicated Environment customers are eligible to receive Updates and New Releases for Tambla Software if and when they are generally available from Tambla during the support period as set out in the Customer agreement.
- When a new software version update is ready for release, the deployment process is initiated.
- After the build has passed internal Testing (QA), an outage window must be scheduled for the deployment.
- Customers will need to manage the outage window. If Tambla services are required, any assistance should be scheduled to accommodate both parties and resourcing.
- Outage windows can last up to 5 hours for minor upgrades of the product where the same version of Microsoft's .Net framework is used, and the upgrade is within the same Major Version release of the product.
- Where a deployment is deemed to be a major or advanced update, where a change is required for the Microsoft .Net Framework version and/or where the Major Version release within the product is upgraded, the outage window can be up to 10 hours.
- Release Notes (including any bug fixes or issue resolution) and New Functionality Notes will be emailed to the Customer.
- The Tambla Infrastructure team then facilitate the deployment.
- After the deployment to the Customer test environment, it is the Customer's responsibility to verify the release and approve the released version for production deployment.
  - Where the Customer does not maintain a test environment, it is the Customer's responsibility to complete any UAT on their production environment.
- Tambla will use reasonable efforts to ensure that any update is backward compatible with the New Release of which it is a part. For example, if the current version of the Software is v 2.1.0.0, then all Updates numbered v 2.1.x.x will be binary compatible with v 2.1.0.0. However, Tambla does not guarantee that any Update or New Release will be compatible with:
  - Any interfaces, whether made by Tambla or any other person.
  - A version of any third-party software that is not included in the Tambla solution or specified as part of the integration.
- Tambla may be able to create additional functionality based on agreed terms; however, it is not under any obligation to do so.

7.3 Self-hosted Customers

- All supported customers are eligible to receive Updates and New Releases for Tambla Software if and when they are generally available from Tambla during the support period as set out in the Customer agreement.
- When a new software version update is ready for release, the deployment process is initiated.
- After the build has passed internal Testing (QA), an outage window must be scheduled for the deployment.
- Customers performing their own update/upgrade/hotfix should also manage the outage window. If Tambla services are required, any assistance should be scheduled to accommodate both parties and resourcing.
    - Outages will be discussed with the Customer and scheduled and charged according to the contract.
    - Outage windows can last up to 5 hours for minor upgrades of the product where the same version of Microsoft's. Net framework is used, and the upgrade is within the same Major Version release of the product.
- Where a deployment is deemed to be a major or advanced update, where a change is required for the Microsoft .Net Framework version and/or where the Major Version release within the product is upgraded, the outage window can be up to 10 hours.
- Release Notes (including any bug fixes or issue resolution) and New Functionality Notes will be emailed to the Customer.
- The Tambla Infrastructure team then facilitate the deployment.
- The Tambla Infrastructure team then liaises with the Customer's nominated technical contact to gain access to their environment to facilitate the deployment.
- The Customer must provide a remote client-based VPN or remote access to the environment where the product is installed. Where a client is unable to provide a client-based solution, a Site-to-Site VPN may be implemented.
    - A Site-to-Site VPN may incur an additional monthly charge.
- After the deployment to the Customer test environment, it is the Customer's responsibility to verify the release and approve the released version for production deployment.
    - Where the Customer does not maintain a test environment, it is the Customer's responsibility to complete any UAT on their production environment.
- Tambla may be able to create additional functionality based on agreed terms; however, it is not under any obligation to do so.

7.4 Software End of Life Policy

Tambla will ensure that Support and Maintenance Services are available for the major version of the Software that is the then-current release of the Software [e.g. v 2.2.x.x] and will offer Support (during the support period as set out in the agreement) for the previous two versions of the Software [e.g. v 2.1.x.x or v 1. x.x.x] for 90 days from the date that the major version [e.g. v 2.2.x.x] was made generally available to its supported customers.

Thereafter, Support and Maintenance Services for Software may be available only by prior separate written agreement and may be subject to different service levels, technical restrictions, and pricing.

8. Equipment Maintenance

This warranty service is in addition to your rights under the Australian Consumer Law. Details of how to claim under the Statutory Guarantees under the Australian Consumer Law are set out in your agreement with Tambla.

8.1 Clock Warranty

- BioStations include a 12-month manufacturer's warranty.
- BioMinis include a 12-month manufacturer's warranty.
- FaceStations include a 12-month manufacturer's warranty.
- Warranty excludes any malicious or accidental damage.

8.2 Clock Warranty Claim

If you have a warranty claim or need to replace/repair a damaged clock (out of warranty) you should raise a ticket using the Support Portal. You will be responsible for returning the device to the Tambla head office (at your own expense). Tambla will send a replacement clock on receipt of the returned clock. Once the replacement clock has been installed, you will need to contact Tambla support to configure the clock to connect to the Tambla network.

If the clock has malicious or accidental damage upon return, then you will be charged for the replacement clock.

8.3 Clock Server

Tambla provides a locally installed (within the customer LAN/WAN), clock server to manage the communication between deployed clocks and the Tambla Hosted Service and Tambla Self-Hosted Service. Tambla provides support to ensure the ongoing connectivity between clocks, the clock server and the hosted solution. There is a minimum specification for installing and hosting the clock server.

The customer is required to provide login access to Tambla personnel to their Clock Server SQL Database for clock tracking purposes on an ongoing basis.

8.3.1 Mandatory Clock Server Changes

Where any software updates are required to maintain the clock server (for example a new .Net platform or other technology changes), the Customer will be notified, and changes or updates made accordingly.

8.4 Software Clock

Tambla supplies a software application called Software Clock with a finger-scan device (Bio-mini). This software is used to capture the clock-in and clock-out of employees. It also verifies the finger images of the individual employee and communicates that to the hosted application. Normally, Software Clock is installed on the user's computer, or a shared computer, and a minimum specification is required.

8.5 Clock Repair and Spares

Tambla will ensure that it can provide spares and a reasonable repair facility for any Equipment for a period of at least 12 months from the date of purchase. Thereafter, spares and repair facilities are not guaranteed, and you should not rely on them being available.

Tambla may choose to provide refurbished equipment as an alternative to repairing it, or we may use refurbished parts to repair the equipment.

We give you notice as follows: "Goods presented for repair may be replaced by refurbished goods of the same type rather than being repaired. Refurbished parts may be used to repair the goods."

8.5.1 Clock Repair and User Generated Code

Tambla advises that where the equipment includes user-generated code, we give you notice as follows: "User-generated code may be lost during our repair of the Equipment".

You should back up your user-generated data prior to providing us with the equipment for servicing.

9. Tambla SaaS Environment

9.1 Availability Zones

The Tambla SaaS (Software-as-a-Service) platform is located across multiple Availability Zones.

"Availability Zones" are discrete Tier III fault-tolerant data centres, providing redundant power, cooling, and networking. The Tambla SaaS Availability Zones includes the following features:

- Access to the Tambla application running from the Tambla Cloud platform located in the S1 and M1 Availability Zones.
- Application hosted across discrete certified tier 3 Data Centres facilities, providing:
    - N+1 Redundancy for all critical subsystems, including Air-conditioning, UPS and Emergency Power Generation; and
    - 24 x 7 Security including staged manlock, biometric scanners, CCTV and electronic proximity cards.
- Physical network redundancy between the Tambla Availability Zones (inter-cloud).
- Redundant Internet services.
- Data Protection services between availability zones.
- DR Recovery between availability zones is available for customers who have contracted this service.

9.2 Data Centre Locations

The Tambla Cloud environment is physically located in the following data centres:

- S1 - NEXTDC: 4 Eden Park Dr, Macquarie Park NSW 2113
- M1 - NEXTDC: 826-830 Lorimer St, Port Melbourne, VIC 3207

9.3 Virtual Server Infrastructure

The Tambla Cloud SaaS is built on hypervisor cluster nodes. The cluster nodes provide a highly available platform that supports the failure of individual nodes without impacting the production delivery of the service. The architecture also allows the SaaS environment to be scaled on-demand as required to support increased workloads.

Tambla SaaS utilises a three-tier architecture as follows:

- "Tier 1 Servers" or the "Presentation tier" contains the Web Client servers and Application Streaming Servers.
- "Tier 2 Servers" or the "Application Tier" contains the application middleware servers.
- "Tier 3 Servers" or the "Data Tier" houses the database servers.

9.4 SQL Database Service

The Tambla SQL Database service is a fully managed relational database with built-in high availability and geo-replication. It is a managed service that includes daily management, performance tuning, threat monitoring, and vulnerability assessments and patching and updating.

The SQL Database service is multi-tenanted; however, each customer's data is stored within its own separate database.

The SQL Database service is replicated between the Tambla availability zones for very high service availability.

The Tambla SQL Database service includes the following features:

- Multi-tenanted SQL Enterprise Server with dedicated customer databases.
- SQL Database with Failover Clustering and AlwaysOn Availability Groups.
- SQL Transparent Data Encryption (TDE) providing data encryption at rest.
- Database replication and recovery between availability zones.

9.5 Storage

The storage environment for the Tambla Cloud is based on highly available, highly scalable software-defined storage nodes.

- Production Storage - All production servers (Tier 1, 2 and 3) utilise Solid Stage Disks (SSD) to deliver the highest storage performance characteristics for all workloads.
- Test/Dev/Staging Environments - Data is located on Nearline storage with RAID 6 redundancy.
- Archive Storage - Data is located on Nearline storage with RAID 6 redundancy.

9.6 Software Licenses

Tambla SaaS includes the software licenses required to deliver the SaaS, such as the operating system, database, backup, application gateway, and antivirus software.

Any additional Tambla application software licenses can be acquired as:

- Per Employee, Per Month (PEPM) either included or in addition to the SaaS cost.

- And can be purchased under an existing contract.

9.7 Internet Service

The Tambla Internet service comprises multiple Internet services, which are load-balanced across both availability zones, providing a highly available service to all Tambla customers.

Internet Service includes:

- Load Balanced Shared Internet Service across both availability zones.
- Dedicated Internet IP address(es).
- Tambla DNS records (e.g. ess.[customer].tambla.net). Customer-owned domain names are supported (e.g. ess.[customer].com) but configuration and ongoing management of the DNS is the responsibility of the customer.

9.8 Client Access

Access to the Tambla Could is via the Internet and is secured and encrypted in-flight using 256-bit HTTPS encryption.

Client access over the Internet includes:

- Tambla Web Client access - HTTPS (web) access from the user's computers and mobile devices.
- Tambla Mobile App access - native Android and Apple (IOS) applications.
- Tambla eTivity WinClient access - HTTPS access from the user's computers.
- Tambla Application Gateway access - Allows Tambla Windows-based applications to run within a user web browser using HTML5 and requires no client software to be installed. It supports desktops, iPads, iPhones and Android devices.

9.9 Security Management

Tambla will provide security for the aspects of the service over which it has sole physical, logical, and administrative level control.

Tambla will provide:

- Physical Security: Tambla will protect the data centres housing the Tambla Cloud from physical security breaches.
- Information Security: Tambla will protect the information systems used to deliver the Tambla Cloud Service.
- Network Security: Tambla will protect the Tambla Cloud Internet Service and local and wide-area networks containing its information systems.
- Security Monitoring: Tambla will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the Tambla Cloud Service. All activity is stored in the Tambla SIEM (Security and Information Event Management), compliant with regulatory standards such as GDPR, SOX and the Australian Notifiable Data Breaches scheme (NDB).
- Patch Management: Tambla will maintain the systems it uses to deliver the SaaS, including the application of patches it deems critical for the target systems.

- Vulnerability Management: Tambla will perform routine vulnerability scans to surface critical risk areas for the systems it uses to deliver the SaaS. Critical vulnerabilities will be addressed in a timely manner.

The Customer retains responsibility for:

- End-User Device Security: Securing the end-users devices used to access the Tambla Cloud services is the responsibility of the customer. This includes, but is not limited to, antivirus/malware protection, patching and vulnerability management.
- End-user passwords.

9.10 Dedicated Environment

The Tambla dedicated SaaS environment provides production and test environments with an optional disaster recovery site.

The optional disaster recovery site terms and conditions for this need to be agreed upon with Tambla, and incremental costs will be incurred.

The additional benefits of the dedicated Cloud environment are:

- Each customer Tier 1 and Tier 2 servers are deployed to their own dedicated virtual servers. This allows for improved security controls for each customer environment as well as ensuring that the activity from one customer does not impact another customer's service.
- Choice of Web URL for access, e.g. etivity.customername.com.au. In a multi-tenanted environment, all clients access the solution via a single fixed URL.
- Ability to skin the current web kiosk interface. In a multi-tenanted environment, the web kiosk interface cannot have different skins applied for different clients. Dedicated Cloud customers can continue to have a custom skin applied in their dedicated cloud environment.
- Control over releases and patch maintenance dates. In a multi-tenanted environment, clients do not have control over when and at what time releases, upgrades or maintenance are carried out. With a dedicated cloud environment, Tambla and the customer will liaise on all releases and maintenance work for operationally viable scheduled dates.
- Control over customisations. In a dedicated environment, the customer has greater control over the deployment of customisations.

9.11 Data Protection Service

The Tambla SaaS service and customer data are continually backed up using different technologies, which include:

- Asynchronous database replication to the secondary data centre.
- Daily full database backups
- 15-minute transaction log backups
- Daily virtual server backups
- Restoration of deleted data is performed by the Tambla service desk upon request, and if caused by the Customer, is a chargeable service

Backup Data Retention: 3 months (standard). NOTE: Tambla uses soft deletes so that all data past and present, including deleted data, is retained in each customer database backup.

9.12 Synthetic Monitoring

Each Tambla SaaS production environment is proactively monitored for service availability and performance.

- Synthetic monitoring scripts are used to simulate real user activities such as logging on to the application and performing key application actions.
- The synthetic monitoring is run from external Internet locations to fully emulate an end-to-end connection to the Tambla SaaS over the Internet.
- Service availability and application performance metrics are captured.
- Alerts are generated and sent to the Tambla service desk.

9.13 SaaS Service Availability

Item	SLA
Monthly Uptime Percentage	99.9%

The Monthly Uptime Percentage is calculated using the following formula:

$$\text{Monthly Uptime Percentage} = \frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

"User Minutes" is the total number of minutes in a month, less all Scheduled Downtime, less Limitations, multiplied by the total number of users.

"Scheduled Downtime" means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish a notice or notify you at least five (5) days prior to the commencement of such Downtime.

"Downtime" is the sum of the length (in minutes) of each Incident (when end users are unable to login to the Tambla SaaS service) that occurs during that month multiplied by the number of users impacted by that Incident.

9.14 SaaS Recovery Objectives

Item	SLA
Recovery Point Objective (RPO)	See contract for details
Recovery Time Objective (RTO)	See contract for details

"RPO" Recovery Point Objective defines the maximum allowable amount of lost data measured in time from a failure occurrence to the last valid backup.

"RTO" Recovery Time Objective, represents how long it takes to recover the Tambla application from a full data centre outage or data centre component failure incident. The RTO does not apply to a data corruption or deletion incidents which require manual restoration of data from backup media.

9.15 Third-Party Operating Systems and Software Programs

The Software operates with, and interfaces with, many different third-party operating systems and software programs. A list of the Software that Tambla has tested as being compatible with third-party operating systems and software programs can be provided by the Support Desk at any time. Tambla disclaims any responsibility as to whether the Software will operate with any software programs that are not included in this list.

As software vendors are constantly updating their technology and ending support for older versions, Tambla will update these details on a regular basis.

9.16 Open-Source Code

The Tambla software includes open-source code, which is licensed by its copyright owners under their open-source licenses. Tambla is not responsible for open-source code and does not provide Support and Maintenance Services in relation to it. Where Tambla has used open-source code that is licensed subject to a license that is generally regarded as a "copyleft" license, Tambla confirms that it has only used an exact copy of the open-source code and not any modification or adaptation that would be subject to the "copyleft" licensing provision of the open-source licence.

Open-source code currently used includes JQuery and AngularJS. Tambla will update these details on a regular basis.

9.17 Application Routine / Housekeeping Jobs

Within the Tambla SaaS environment, Tambla will be responsible for running routine/scheduled jobs and performing application housekeeping routines. Examples of items include database/application jobs that run outside of the application scheduler, deleting redundant records from the database, etc.

See the contract for the defined routines and housekeeping jobs.

9.18 Scheduled Monthly Maintenance

The Tambla SaaS environment undertakes routine monthly maintenance, including multi-tenanted and dedicated environments. This maintenance occurs on the first Wednesday of each month, commencing at 9 pm AEST, and is scheduled for up to 5 hours.

Self-hosted customers are responsible for maintaining their own servers and databases.

10. Customer Responsibilities

The following items must be provided by you in order for Tambla to be able to provide Support and Maintenance Services efficiently. Tambla's ability to meet the Target Response Times and Target Resolution Levels is dependent upon the Customer meeting its obligations under this section.

For Customers with Customer hosted Software, you must:

- Provide high-speed remote access to the Software on a 24 x 7 basis.
- Allow the use of any tools that Tambla makes available to assist in Support and Maintenance Services, including web conferencing and tools that provide Tambla engineers with the ability to remotely see and control your computer. Tambla will seek consent on each occasion it seeks to use these remote access tools.
- Provide a non-intrusive test environment (NITE) for Tambla and the Customer to test any patches, bug fixes or updates prior to the Customer installing them into the Customer's environment.

In all cases, you must maintain any third-party software to which the Tambla Software interfaces at a version for which the licensor provides standard production support. Tambla may require you to upgrade its support with third-party software where it is necessary for Tambla to continue to provide standard Support and Maintenance Services in accordance with this Support and Maintenance Policy.

10.1 Minimum Operating End-User Requirements

You will need to refer to the minimum operating requirements for the specific build and version of the software you are using. These can be provided anytime by the TSD.

10.2 Self-hosted Environment

Customer self-hosted environments are subject to the customer's Policies and Governance. Tambla has published minimum requirements documentation for multiple sized customers. Application installation is provided by Tambla and installed in a best-practice scenario.

The Customer's environment (Including server and network infrastructure) is wholly managed by the customer with Tambla providing support for the installed application Tambla Software only.

10.3 SSL Certificates

Tambla software uses SSL certificates to secure and encrypt network traffic over the public Internet and private network connections.

- Tambla is responsible for the provision, renewal and configuration of all SSL certificates that are associated with Tambla DNS names, i.e. tambla.net, comops.biz.
- Customers that use their own SSL certificates, which include self-signed certificates and certificates associated with the customer's own domain names, are responsible for:
    - the procurement and renewal of the certificate(s).
    - the implementation of the certificates within the Tambla application;
    - the ongoing management of the certificates and DNS records.

10.4 Customer Identity Providers (IdPs)

Tambla supports Single Sign-On using OpenID. This allows Customers to use their own Identity Provider (IdP) to authenticate to Tambla applications, and as such the Customer IdP is a critical component and needs to be available to process logins to the Tambla software.

Customers using their own IdP for SSO authentication are responsible for the following:

- Configuration of their Identity IdP to integrate with Tambla's OpenID services.
- Maintain the availability of their IdP.
- Ongoing management of their identity provider, i.e., the creation of users and the reset of passwords in the Active Directory.

NOTE: Unavailability of a customer's IdP will stop the Customers users from being able to authenticate to the Tambla application and will not count against the Tambla SaaS availability SLAs.

10.5 Tambla SaaS Third-party Application Integration

Tambla SaaS supports working with customers' third-party applications securely over the Internet using the following integration types:

- OData API – Allows the Tambla SaaS database views to be accessed. Typically used to ingest data into customers data warehouse, data analytics and reporting solutions
- RESTful API – Allows Tambla SaaS to be integrated with other third-party application workflows using direct calls between the Tambla and third-party APIs.
- Flat File Transfer – Files are securely transferred over Secure FTP to allow automated import and export of data.

All integration types support two-way integration, allowing both transfers of information into and out of the Tambla SaaS environment.

Tambla is responsible for maintaining and making available the APIs and Flat File transfers as part of the Tambla SaaS availability SLA.

The customer is responsible for:

- The configuration of their third-party application to work with Tambla SaaS.
- Ongoing management and monitoring of their third-party application integration.
- Testing of their Third-party application integrations as part of a Tambla SaaS version upgrade

11. Out of Scope Items

Tambla shall have no obligation to provide Support and Maintenance Services:

1. For Customer hosted Software, in respect of any Software that has not had any Update or New Release installed within 180 days from the date of the general release of the relevant Update or New Release to supported customers;
2. To any adaptations, translations or derivative works made to the Software, whether made by Tambla or any other person or
3. For any open-source code.

Tambla shall have no obligation to provide Support and Maintenance Services where the defect arises from:

1. Misuse, incorrect use of or damage to the Software from whatever cause (other than any act or omission by Tambla), including failure or fluctuation of electrical power;
2. Failure to maintain the necessary environmental conditions for the use of the Software;
3. Use of the Software in combination with any equipment, services or software other than the Technical Environment;
4. For Customer hosted Software, relocation of the Software to any place other than the Premises without Tambla's prior written consent;
5. Any breach of Customer's obligations under the agreement, including these Policies;
6. Having the Software maintained by a third party or
7. User error.
8. A customer interface or integration with Tambla software where the development of such interface or integration was not developed or approved by Tambla.

The SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centres, including at your site or between your site and our data centre);
2. That result from the use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;
3. Caused by your use of a Service after we advised you to modify your use of the Service if you did not modify your use as advised;
4. That result from your unauthorised action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;
5. That result from your failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or your use of the Service in a manner inconsistent with the features and functionality of the Service (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;
6. That results from faulty input, instructions, or arguments.

If it is necessary for Tambla to attend your premises to provide Support and Maintenance Services, or Tambla determines that the work is performed in relation to a logged issue was caused by any of the items in this

section, then you must pay for such work at our then-current fees and charges as well as any expenses we incur in performing such work and travelling to your premises.

12. Terms and Conditions

These Policies are subject to the terms and conditions of the agreement between the Customer and Tambla.

Support and Maintenance Services will be provided only for Tambla Software, which is properly licensed and subject to a valid Agreement that includes Support and Maintenance Services during the period in which the Support Service is provided.

The Customer acknowledges that not all errors or defects in the Software and documentation may not be remedied despite best endeavours.

Support and Maintenance Services should be acquired on a continuous basis. If you cease to have Support and Maintenance Services for the Software and subsequently want to reinstate Support and Maintenance Services, then you must pay Tambla's then-current support reinstatement fee in addition to the then-current Fees for Support and Maintenance Services prior to the Support and Maintenance Services being re-instated. The support reinstatement fee is 75% of the Support and Maintenance Services Fees that would have been payable during the period when no Support and Maintenance Services were acquired.

You must not provide Tambla with any Personal Information when dealing with Support unless it is absolutely necessary in order to enable Tambla to resolve the issue and you have the express informed consent of the individual concerned to provide that Personal Information to Tambla, its Affiliates and their respective contractors, (including consent to transfer that Personal Information to any country in the world) for any use that is connected with the provision of Support and Maintenance Services and/or in a way that is consistent with Tambla' Privacy Policy (a copy of which is available on the Tambla Website). You must never provide Tambla with any Personal Information that is also classified as "Sensitive" information within the meaning of privacy legislation anywhere in the world.

If Tambla acquires additional software programs through merger or acquisition activities, then there may be a transitional period during which the Support and Maintenance Services for the acquired software will not be provided in accordance with this Support and Maintenance Policies. Tambla will issue an updated Support and Maintenance Policies dealing with these issues if this occurs.