

tjecco software bv
Pantheon 16
NL-7521 PR Enschede

🌐 www.tjecco.com
✉ hello@tjecco.com
☎ +31 85 303 7000

KvK 68602596
BTW NL8575.15.779.B01
IBAN NL25 RABO 0370 7864 16



Service Level Agreement

Document Number: I00101002-1233

Date: 06-11-2025

Public

Table of Contents

1	Definitions	3
2	Service Level Agreement overview	4
3	The game rules	5
3.1	Notification	5
3.2	Response time	6
3.3	Resolution times	6
3.4	Wish	6
3.5	Backup & Recovery	7
3.6	Maintenance.....	7
4	SupportDesk.....	8
5	ISO27001 Information Security	9
	Exhibit 1: Data Recovery Plan.....	10
	Schematic Overview	10
	Emergency plan and service levels	10
	Incidents	11
	Service Level RPO	11
	Service Level RTO	11
	Technical implementation	12

Document history		
Date	Version	Description of changes
01-01-2025	1.	Initial document
06-11-2025	1.1	ISO27001 certification

1 Definitions

tjecco	tjecco software BV based in the Netherlands with its own software development team.
Client	The client, as agreed in the assignment, authorized persons in the ACL
Software updates	Updates to the SaaS Service for which tjecco is responsible that are released periodically depending on the Priority (daily, weekly, monthly).
Device	Physical or virtual device, such as servers, switches, routers, firewalls, SAN, NAS, computers, data carriers, peripherals, the cloud, etc.
Data	All forms of data (storage) including databases, e-mail, documents, photos, movies, sound, software, etc.
SLA	Service Level Agreement; definitions to what level management will be performed, within what periods, expectations, obligations and associated costs.
SaaS Service	The Software-as-a-Service (SaaS) Services provided by tjecco that is available to Client via the Internet.
Monitoring notifications	Measured failures are automatically communicated to the development team 24/7 within minutes.
Response time	Time between Notification and when tjecco takes up the Notification.
Availability	The extent to which the SaaS service is available to the Client. The Availability is measured that maintenance (planned / unplanned) or circumstances beyond the control of tjecco is excluded. This includes failures caused by (incorrect) actions or neglect by the Client of the SaaS Service, by harmful actions of third parties (DDos, hacking, etc.), by failures in the Internet connection, other networks, equipment of the Client and/or suppliers.
Notification	A notification is notification from Client which may relate to a Query, an Incident or a Desire regarding the SaaS Service.
Incident	An event that results in a (severe) deviation from the normal operation of the SaaS Service, availability, data loss or data breach. Incidents are reported at a minimum by telephone.
Question	A request for explanation or clarification regarding the operation of the SaaS Service.
Feedback	Is a Notification of by the Client.
Wish	A Notification from Client to modify existing functionality of the SaaS Service.
Priority (designation)	The following priority designations are used by tjecco: • Serious issue - the progress of the SaaS Service is blocked (business process Client is severely hampered), no Workaround is available to the Client or there is an information security issue. • Workaround – the progress of SaaS Service is not blocked where a Workaround is available (business process of Client experiences some disruption). • Wish – the progress of the SaaS Service is not blocked, the SaaS Service is usable (Client's business process continues), expansion and/or modification of existing functionality or user demand.
Resolve time	The time that has elapsed between the time of a Report until it is resolved or a Workaround is made available or a Question is answered. The Resolve time does not include the waiting time for failure to answer Questions as well as the situations described under 'Availability'.
Workaround	An alternative solution to the notification that allows work to continue.
Best Effort	Maximum reasonable effort.
Working hours	Daily hours from 8:00 a.m. to 5:00 p.m. on weekdays, excluding holidays.
ISO27001	The internationally recognized standard for information security management and assurance in accordance with the tjecco Information Security Management System (ISMS).
ACL	Access Control List of authorized persons.
Web-app	The tjecco application which is used through the web browser.

2 Service Level Agreement overview

Description	Service Level
Visual Monitoring	✓
Documentation	✓
ISO27001 certified	✓
- tjecco - hosting AWS	✓ ✓
Availability Guarantees: - Network uptime - Server availability - Application availability	99,9% 99,9% 99,5%
Guaranteed response times: - In web-app notifications - By phone - Other channels (E-mail, Whatsapp, etc)	Directly Directly Maximum of 4 working hours
Guaranteed resolution times	Serious issue: start within 2 working hours until the Notification is resolved. Workaround: work is sheduled. Wish: work will be placed on the Roadmap.
Support facilities: - In web-app support - Video / interactive demo - By phone support - WhatsApp support - Online support (Teams) - Discipline support - Safety updates - Monitoring Notifications - Application specific Notifications	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓

3 The game rules

This chapter describes the principles and conditions under which tjecco offers its service levels.'

3.1 Notification

tjecco will, upon receipt of a Notification from the Client on a Best Effort basis, answer questions and resolve Incidents that the Client experiences when using the tjecco SaaS Service. The service level described in this SLA relates to implementation, direction, functional management and support of the SaaS Service purchased by the Client. If resolution of a Notification is not immediately possible, tjecco strives to create a temporary workable solution ("Workaround") pending a permanent solution.

Wijze van melden

- Incidents can be reported to the tjecco support department
 - Through in app feedback tool. This Feedback allows the user to quickly and efficiently communicate a defect or a wish without the user having to type a large amount of text so that the support department understands what happened. The Feedback button allows the support department to reproduce the click sequence as well as the corresponding program component directly to each other allowing debugging to be performed faster and more efficiently. Via e-mail
 - Via Whatsapp
 - By phone

All Notifications are managed in the tjecco ticketing system with the exception of telephone Notifications that are answered or resolved immediately. Received Calls are reviewed and prioritized and categorized by tjecco:

- Serious issue
- Workaround
- Wish

Quality

A notification should be described as precisely as possible to be able to reproduce the Question or Incident and preferably reported through the in app Feedback function. Without sufficiently clear information tjecco will not be able to start the work associated with the solution. tjecco checks the information provided and will ask for additional information where necessary. The table below (Table 1) shows the minimum information to be supplied as well as some additional data:

Description	Mandatory	Part of in App feedback feature
Name Client +Email address of reporter	✓	✓

Incident or Wish	✓	✓
Clear title and discription of Notification	✓	-
Video, screenshot and/or actions taken before the Notification occurred.	✓	✓
Is the SaaS Service blocked for one or more users? Can work continue?	✓	-
Error texts	-	✓
What did the user expect how the SaaS Service should work?	-	✓
What actions solve the problem of the Notification?	-	-

Table 1: Minimum information and additional data to be supplied

3.2 Response time

The time frame for tjecco to start solving Notifications is as follows and will be carried out by the in-house staff of the tjecco software engineering team based in the Netherlands:

- In all cases, the user receives immediate digital confirmation of the Notification made if the Notification was submitted via the in-app Feedback feature.
- In all other cases and if not already answered and solved immediately, Reports will be fed back to the application administrator according to the ACL within a maximum of 4 Working Hours after the moment of registration of the Report. In the feedback the Report will be confirmed, the Priority as well as the solution direction indicated.

3.3 Resolution times

The Resolution Time of a Report depends on being able to reproduce the Report made where tjecco uses the following Resolution Times per Priority based on Best Effort:

- **Serious issue:** work starts no later than 2 working hours after tjecco's response and continues until the Notification is resolved or a Workaround is available; If the resolution time is estimated to be longer than 4 working hours then tjecco will inform the application administrator of the time frame involved in the resolution work..
- **Workaround:** work is scheduled to be included as part of a new release.
- **Wish:** work is posted on the tjecco Roadmap.

If Client is not satisfied with tjecco's handling of the Report, Client may contact its tjecco relationship manager.

3.4 Wish

Each wish is periodically evaluated by tjecco. This evaluation can be answered as follows:

- Through a software update or configuration change
- By placing the Wish on the roadmap
- Via [‘Sponsor een feature’](#)

- Rejection of the Wish

In all cases, the Application Manager will be informed where the Relationship Manager will be contacted when sponsoring a feature for the commercial agreement for the preparation of the Functional Design (FO) and possible realization. The FO will be made available by tjecco to Client for approval. Based on the final FO, tjecco will make a proposal for realization available to Client. After approval by Client, tjecco will start scheduling the work.

3.5 Backup & Recovery

tjecco is responsible for the backup and recovery of stored Data. The data center facilities are fully redundant and herein backup and recovery of the Data is integral.

Appendix 1: Data Recovery Plan details the DRP.

3.6 Maintenance

tjecco performs maintenance and updates to its SaaS Services on its own initiative. If maintenance results in reduced Availability of the SaaS Service, tjecco will inform the Client and, where possible, perform this maintenance work outside Business Hours.

Management and maintenance will be performed in accordance with the frameworks of GDPR laws and regulations and ISO 27001.

To keep the user experience optimal for all customers, the technical use of tjecco is monitored. This prevents improper use and ensures that every user is and remains satisfied. In case of notable or abnormal situations, we contact the Client and the possibilities are discussed.

4 SupportDesk

tjecco supports various forms of support with corresponding opening or availability times:

Description	Channels	Availability
Supportportal, including video instructions and interactive demo's	Internet	24 hours a day x 7 days a week
In app support, including video instructions and interactive demo's	SaaS Service	24 hours a day x 7 days a week
SupportDesk	By phone E-mail WhatsApp	8:00 a.m. to 5:00 p.m.
Consultancy	On-site Online Remote	Based on additional assignment from Client.

When calling the tjecco support desk, additional information will be requested, if necessary, about the actions taken prior to the Report. This is necessary to reach a solution as quickly as possible as well as to give the best possible estimate of the resolution time. Of course it will be assessed whether it is an already existing Report and/or a Workaround or Solution is available. The Client will be informed as soon as there is a solution and the Report is closed.

5 ISO27001 Information Security

Managing and maintenance of the hosting infrastructure is performed by tjecco partner Amazon Web Services (AWS). This global player continuously ensures the optimal functioning of the hosting with a team of dedicated professionals.

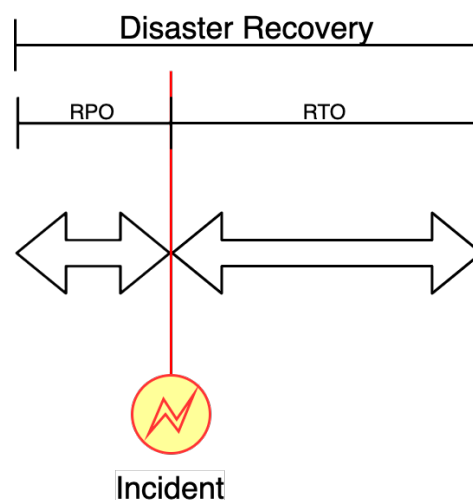
Information security is an integral part of the business strategy and development process of the tjecco SaaS Services. All product development is carried out by tjecco's in-house engineering team based in the Netherlands. This team is continuously trained in the latest (security) technologies. tjecco's business operations and software are ISO 27001 certified. In addition, the following measures are implemented to ensure information security:

- Authentication and authorization management - only those employees whose job duties allow them to access certain Data have that access, combined with 2Factor Authentication (2FA).
- Managed Devices – only equipment (laptops, mobile devices, etc) registered within tjecco's environment (tenant) has access to the tjecco network.
- Managed Locations – Only those devices located within authorized locations have the ability to access the tjecco network and also the ability to perform authorized operations. This limits access from unknown locations.
- Monitoring – All access to customer environments is logged and stored. Monitoring takes place at the network, system and application level. Alerting takes place if an irregularity occurs. Changes made by users through our application are stored in audit trails.

Exhibit 1: Data Recovery Plan

Schematic Overview

The Disaster Recovery Plan is designed to minimize data loss in an availability disaster and to determine recovery time. The time to data loss after an incident is expressed as the Recovery Point Objective (RPO). The recovery of availability is expressed as the Recovery Time Objective (RTO).



Emergency plan and service levels

tjecco's services are offered from a cloud solution. This cloud solution is hosted by Amazon Web Services (AWS).

All desktop web applications, such as tjecco compliance, tjecco inspect and the tjecco mobile pro app from the AppStore/PlayStore, the underlying database with all data and storage for files are available through the cloud.

The disaster recovery plan is described based on the tjecco configuration at AWS and describes what actions are taken to mitigate data loss and reduce recovery time. There is continuous monitoring of application availability. In the event of a disaster or incident, responsible persons within tjecco are automatically notified so that this plan and associated actions are put into effect..

Incidents

In the event of a disaster or incident, the monitoring environment sets up which people are automatically notified via notifications. In the event of a disaster, the data and application must be available again as quickly as possible, with minimal or no data loss. To restore the applications, tjecco uses blueprints (replicas) of the software environment.

Based on the real-time copy of the data and the blueprints, immediate actions are taken to make the applications tjecco compliance and the tjecco mobile pro app available again. In case of an incident, actions are taken to limit data loss and restore availability of the applications. For limiting data loss, the term Recovery Point Objective (RPO) is used in the ICT world. For restoring the applications and environment, the term Recovery Time Objective (RTO) is used.

Service Level RPO

The Recovery Point Objective (RPO) represents the maximum amount of data loss in unit time after an incident. tjecco uses a real-time data replication service. Data is continuously copied to another environment. Thus, in the event of a disaster, data is immediately secured.

tjecco guarantees a maximum data loss of 60 minutes, but in practice this will usually be limited to a few minutes. Files uploaded into tjecco (documents, images) use the same replication service. These files are also secure and tjecco also guarantees a maximum data loss of 60 minutes for these, which will usually be limited to a few minutes.

Data once processed in the data center and where no disaster has occurred is replicated continuously.

Service Level RTO

The Recovery Time Objective (RTO) expresses within what unit of time the applications are available again and can be used normally.

To do this, tjecco uses blueprints of how systems providing the applications can be quickly reestablished. In this way, the same kind of environment is quickly built and made available. From the moment this action is taken, the system becomes available again.

During business hours, tjecco guarantees that applications will be available again within one hour of a disaster. Outside office hours, availability is guaranteed within 4 hours.

Technical implementation

The information below provides content about the RPO and RTO.

Schematic overview

To ensure continuity and availability, tjecco software bv hosts the software at Amazon Web Services in the Frankfurt region.

Amazon Web Services

To ensure continuity and availability, tjecco Software BV hosted the software at Amazon Web Services in the Frankfurt area. AWS has three data centers in Frankfurt, Germany, divided into zones. In the event of a disaster, it can quickly switch to another zone.

Zones

The tjecco environment is set up in the primary Zone 1. Application availability and supporting components are managed from Zone 1. AWS in Frankfurt has three available zones from which tjecco can be accessed, with one zone used as primary and the others serving as backups in case of emergencies. One zone houses the tjecco desktop application and the tjecco Mobile back-end. These two applications communicate with the database and the S3 bucket located in the same zone. The database contains the content customer data, while the S3 bucket is used for file storage. In the event of a disaster, it can be quickly switched to another zone. When the environment is available, a switch to that zone automatically occurs via a set load balancer. This ensures that communications are routed to the correct zone.

Loadbalancer

Access to the appropriate zone where applications are available is controlled by a load balancer. This system provides communication with the available environment. The load balancer is configured to communicate with the zone in which the tjecco applications can be accessed. This configuration ensures effective and seamless communication with the appropriate zone.

Database-replication

In order to switch to another zone, the data must be available. Replication of the database is set up for this purpose. Continuous data replication of the tjecco database takes place primarily between Zone 1 and Zone 2. With this real-time data exchange, tjecco ensures minimal data loss in the event of a disaster and thus a very low Recovery Point Objective (RPO).

In the absence of availability in Zone 1, it is possible to quickly switch to Zone 2. If Zone 2 becomes the primary environment, automatic data replication takes place from Zone 2 to Zone 3. Thus, data is re-secured in another zone, providing an additional safety net for the RPO.

The replication service between zones is real-time and provided by Amazon Web Services..

S3 bucket

The S3 Bucket is an AWS service primarily responsible for file storage. Documents, images and other files are stored in specially optimized AWS storage. This S3 bucket is available in three zones.

Because the data is spread across the three zones, it remains available when another zone becomes active in the event of a disaster. At this point, tjecco also ensures a low Recovery Point Objective (RPO). This setup ensures that data stored in the S3 bucket remains consistently available, contributing to the overall resilience of the system..