# Security — Methodologies, Technologies and Communication

How simulator information is generated, protected, transmitted and consolidated, and which security controls back each stage.

DATE
November 6, 2026

CLASSIFICATION
Public

VERSION
1.1

Addressed to the IT and security teams evaluating Yoy as a supplier. It first describes the security baseline (infrastructure and monitoring, sections 01 and 02) and then follows the data in order: device (03), transmission (04), access (05), consolidation (06) and reporting (07). It complements the Network and Infrastructure Technical Requirements and the Technical, Operational and Continuity Policies. For detail on what personal data is processed, for what purpose and for how long, see the Privacy Policy.

# 01. Infrastructure architecture and security

Yoy Account — the backend that centralises licences, users and usage reports — runs entirely on cloud infrastructure managed by Yoy.

### Compute and data

- Hosted on **Oracle Cloud Infrastructure (OCI)**, Santiago de Chile region
- Data stored in a database with network-restricted access — that layer is never publicly exposed
- Administrative access only through private channels (a VPN and a zero-trust access service with corporate identity and two-factor authentication), with no management ports open to the internet; automated deployments connect with keys from an allow-listed set of IPs

### Perimeter and continuity

- Proxy, DNS and firewall managed by **Cloudflare**, with DDoS protection
- SSL certificates managed and renewed automatically
- Automated backups through periodic server snapshots

## 02. Continuous security monitoring and assessment

### Continuous monitoring and scanning

- An internal monitoring system watches authentication events, platform activity and the state of the cloud infrastructure
- Automatic alerts on anomalous activity (e.g. repeated failed access attempts, unexpected changes to the network configuration)
- Periodic review of the cloud security configuration (firewall, certificates, domains) against the expected configuration

### Security assessments

- Regular internal reviews of access control, infrastructure configuration and development practices
- External assessment (penetration test) of the platform's exposed surface, on an annual cadence; the next one is being procured
- Findings are prioritised and remediated, and controls are updated as risks evolve

# 03. Generating and protecting information on the device

The simulator generates two kinds of information while in use:

**Assessment results**

When an exercise ends, the headset automatically generates a results record: overall score and a breakdown for each parameter assessed.

**Simulation events**

Throughout the session, the simulator continuously records what happens in the experience — accidents, interactions, object handling, among others — with their parameters and timestamp. Yoy is progressively expanding the events its simulators capture in order to enrich performance analysis.

1. **Transient retention on the equipment:** while there is no connectivity, the information remains only on the device, never as the operator's permanent repository.
2. **Encrypted data at rest:** the information temporarily held on the headset is encrypted.
3. **Automatic synchronisation:** results are sent to Yoy's central server at the end of each exercise, and events in batches during the session; the server then becomes the definitive repository.

# 04. Secure device ↔ cloud communication

The headset does not authenticate as a human user: each device has its own application credentials, which validate every request against the platform.

### How it authenticates

- Each headset is registered once with a single-use code and receives **its own credentials**: an identifier, a token and a signing key (machine-to-machine authentication, with no user involvement)
- Every message is signed with the device's key and can be used only once (replay protection); server responses are signed as well
- Access control at the **application** level, not by source IP — no IP whitelisting required

### What travels, and how

- Single outbound port: **443/TCP (HTTPS)**, always initiated by the device
- No inbound port needs to be opened towards the customer's network
- All communication travels over **TLS 1.2+**, with no sensitive data in URL parameters
- Three types of traffic: licence status (periodic), assessment results (per exercise) and simulation events (in batches)

**100% outbound communication**

There is no inbound channel from the internet into the customer's infrastructure for the simulator to work.

## 05. Access control and user authentication

Controls applied to the Yoy Accounts platform, the panel where instructors and administrators manage courses, licences and reports.

- **Strict per-organization roles:** each profile accesses only its own organization's information, with no crossover between customers.
- **Authentication:** sign-in with username/password or with Google (OAuth).
- **Two-factor authentication (2FA):** available via TOTP (authenticator app) or WebAuthn/passkeys, with recovery codes, configurable as optional or mandatory per organization.
- **Audit logging:** application access and relevant events are recorded for traceability.
- **HTTP security headers:** HSTS, `X-Content-Type-Options` and `X-Frame-Options` applied at platform level.

## 06. Processing and consolidation of the information

On reaching the server, each report is automatically filed into a hierarchy that makes it possible to trace any result back to its origin:

| Level | Description |
|---|---|
| Organization | The report is associated with the corresponding customer company. |
| Course | It is placed within the course or training programme. |
| Unit / experience | It is associated with the specific unit or exercise taken. |
| Assessment record | The overall result of that assessment is stored. |
| Parameters assessed | Each individual metric making up that result is stored (time, accuracy, procedure, etc.). |

**Simulation events** are stored associated with the device, the experience and the activity in which they occurred, which makes it possible to reconstruct how each session unfolded and to complement the assessment results with the detail of what happened.

> **Restricted database access**
> All of this processing lives in Yoy Account's central database, with network-restricted access and no public exposure.

## 07. Access to reports and traceability

**Access by role**

Each user enters Yoy Accounts with their organization's role, with no visibility over other companies.

**Course selection**

They navigate to the course or programme and see the full list of assessments taken.

**Final report**

They download the individual PDF per assessment, or export a consolidated Excel file by course or date range.

In addition: assessment history per user, and transfer of assessments between accounts, to correct enrolments where appropriate.

## 08. Security and support contact

Technical or security queries, or incident reports:

**Phone / WhatsApp**

+56 9 7880 6021

**Email**

security@yoy.cl (security and incidents)
soporte@yoy.cl (support)

Service hours: Monday to Friday, 09:00 to 18:00 (Chile time).

Security or vulnerability reports sent to **security@yoy.cl** are acknowledged within **2 business days** and receive an initial assessment within **5 business days**.