



Security, hosting and recovery — procurement reference

Customer summary · Version 1.3 · 6 October 2026 · v5ultimate.com/security#procurement

V5 Ultimate hosted services (Cloud and Private Cloud). On-Premises and customer-managed cloud deployments are operated by the customer; see the On-Premises specification.

How to read this document. Where a signed Order or customer-specific agreement exists, it governs. Otherwise the current S.G. Systems SLA and the applicable commercial terms set the commitments; Orders that accepted MSA V1.24 keep its terms. This page describes how the service currently operates; it does not change, add to or replace any contract term.

Where V5 Ultimate runs

Layer	Provider	Location
Application	Google Cloud Run	the Netherlands and Oregon (United States), with traffic shared between both
Database, sign-in and file storage	Supabase, running on Amazon Web Services	United States — Oregon (as recorded 30 September 2026); confirmed for your deployment
Independent backup and archive copies	Google Cloud Storage	United States multi-region (as recorded 30 September 2026); confirmed for your deployment
Source code and deployment tooling	GitHub	Not a store of Customer Data

Service levels and support

1. Is there an uptime SLA, and how does it differ from a 2-hour response?

They are different measures. Uptime measures how much of the month a hosted service is available. A response target measures how quickly a person at S.G. Systems starts working on your issue. For critical (Severity 1) issues that is 2 hours, 24/7/365. It is not uptime, automated recovery or a guaranteed fix time.

- Uptime, backups, RPO/RTO and service credits apply only to V5 Ultimate Cloud and Private Cloud, under the S.G. Systems SLA (§5 and §6).
- Severity 1 (critical): a person from S.G. Systems responds within 2 hours, 24/7/365, for every supported deployment, including V5 Classic and on-premises. Hosted services also keep a 1 business hour target during business hours. Other severities run in business hours.
- A response time is when a person starts working on the issue. It is not a fix time, an automated recovery, an uptime figure or a recovery objective.

Contract references: SLA §4 response targets (v5ultimate.com/legal/sla#s4); SLA §5 hosted service levels (v5ultimate.com/legal/sla#s5); SLA §6 service credits (v5ultimate.com/legal/sla#s6)

2. What happens in a critical outage, and is support 24/7?

A Severity 1 incident gets a human initial response from S.G. Systems within 2 hours, 24/7/365, whether you bought directly or through a reseller, and is worked with engineering until service is restored. You can always report directly to S.G. Systems; the clock starts when your report reaches the S.G. Systems support channel.

- The commitment is set in the S.G. Systems SLA §4.1. Severity 2 to 4 targets run in business hours (09:00-18:00 local, weekdays) unless your Order says otherwise.
- Orders that accepted MSA V1.24 keep their accepted support terms until renewal on the new documents.
- Security incidents follow the notification commitment in Commercial Terms §9.2.

Contract references: SLA §4.1 critical support (v5ultimate.com/legal/sla#c4-1); SLA §3 reporting an issue (v5ultimate.com/legal/sla#s3); Commercial Terms §9.2 security incidents (v5ultimate.com/legal/commercial-terms#c9-2)

Hosting and data location

3. Who hosts the service?

The V5 Ultimate application runs on Google Cloud Run. The database, sign-in and file storage run on Supabase, which operates on Amazon Web Services. Independent backup and archive copies are kept in Google Cloud Storage. Source code and deployments are managed in GitHub.

- This describes the V5 Ultimate application. The public marketing website is hosted separately and holds no Customer Data from the application.
- Operating servers in more than one location does not by itself provide failover for the database or for a whole provider.
- The sub-processors that process Customer Data are listed on the Sub-processors page.

Contract references: Sub-processors (v5ultimate.com/legal/sub-processors)

4. Where is our data stored geographically?

The V5 Cloud application runs in two locations, the Netherlands and Oregon (United States), and traffic is shared between them, so a visitor may be served from either. The database, sign-in and file storage remain in Oregon, United States, so EU-only data storage is not implied. The locations of your database, files and recovery copies are confirmed for your deployment.

- As recorded on 30 September 2026, the database, sign-in and files were in Oregon (AWS, via Supabase) and independent backup copies in a Google United States multi-region location. Which of these apply to your deployment is confirmed in your Order.
- Running the application in the Netherlands does not mean every part of the service, or every backup, is held in the EU. Ask us to confirm each layer for your deployment.
- On-Premises customers keep data in their own environment.

Contract references: On-Premises specification (v5ultimate.com/resources/on-prem-specification)

Backup and recovery

5. What is the Recovery Time Objective (RTO)?

Contractually, the S.G. Systems SLA sets an RTO of 8 hours for Severity 1 incidents on Cloud and 4 hours on Private Cloud. Internally we work to a 4-hour target for restoring the complete service, but that target is provisional and has not yet been proven in a full recovery exercise.

- The internal 4-hour figure is an objective, not a tested result, and does not replace the contract.
- A complete takeover of production at another provider has not yet been exercised end to end (see Latest recovery test).

Contract references: SLA §5.1 Cloud (v5ultimate.com/legal/sla#c5-1); SLA §5.2 Private Cloud (v5ultimate.com/legal/sla#c5-2)

6. What is the Recovery Point Objective (RPO)?

Contractually, the S.G. Systems SLA sets an RPO of 24 hours on Cloud and 12 hours on Private Cloud. How much data could be lost in practice depends on what fails: if data is corrupted while our database provider is still running, we aim to recover to within about 5 minutes; if the provider itself is unavailable, the latest independent database copy can be up to about 24 hours old, plus the time taken to recover.

- The 5-minute figure is a working objective for that one scenario and is still being qualified. It is not a guaranteed data-loss limit for the whole service.
- Private Cloud backup timing is deployment-specific. Ask for the evidence for your deployment before relying on a figure other than the SLA.

Contract references: SLA §5.1 Cloud (v5ultimate.com/legal/sla#c5-1); SLA §5.2 Private Cloud (v5ultimate.com/legal/sla#c5-2)

7. How often is the database backed up?

Point-in-time recovery is switched on for the database, and a full independent copy of the database and files is taken every day. Files are also copied on a separate 5-minute schedule, and archive transfers run hourly.

- Point-in-time recovery is configured for 7 days. The history actually available varies and has recently been slightly under 7 days, so we do not promise an uninterrupted 7-day window.
- The 5-minute schedule applies to files only. The whole database is not copied every 5 minutes.
- The S.G. Systems SLA commitment for Cloud is encrypted backups every 24 hours (§5.1).

Contract references: SLA §5.3 disaster recovery (v5ultimate.com/legal/sla#c5-3)

8. How long are backups and records kept?

Rolling recovery copies are kept for at least 30 days and operational evidence for 365 days. Scoped manufacturing and contract-signature records are also archived with a 15-year minimum retention setting. No automatic deletion of archives is currently enabled.

- The archive retention setting is not yet locked, so it can be changed by administrators. We do not describe it as tamper-proof (WORM) storage, and proving that complete, readable historical records can be produced for the full period is still in progress.
- Backup retention is separate from your contract rights. After termination, Customer Data is retrievable on request for 90 days under Commercial Terms §5.4 (MSA §5.4 for prior Orders), then deleted from active systems subject to the DPA, legal holds and backup rotation. You remain responsible for your own regulatory record retention (§7.3).

Contract references: Commercial Terms §5.4 after termination (v5ultimate.com/legal/commercial-terms#c5-4); Commercial Terms §7.3 data retention (v5ultimate.com/legal/commercial-terms#c7-3)

9. When was recovery last tested, and what did it show?

On 30 September 2026 we restored the previous day's real backup copies into an isolated environment. The database tables, rows and available files were checked, stored signature hashes were verified, and a sample of encrypted values was successfully decrypted.

- Not yet proven: a full production takeover at another provider, a hosted point-in-time restore, restoring original passwords, MFA and single sign-on, every external dependency, and end-to-end service timings.
- A separate test showed application traffic rerouting in about 79 seconds. That was an application-only routing test, not a database recovery and not a service-level commitment.
- Our policy requires restore tests at least every 90 days and an annual regional or provider exercise.

10. Do you have a business continuity and disaster recovery policy?

We have a documented backup and recovery policy and operating guide (current versions dated 30 September 2026). A summary and the latest test evidence are available on request, usually under NDA. We do not currently publish a separate, broader business continuity plan, and we don't claim one beyond what those documents cover.

- The infrastructure programme behind the policy closed with recorded exceptions. That is not a blanket compliance approval.
- An approved assessment (rev 3, 25 September 2026) covers the V5 Ultimate 5.10 manufacturing technical controls. It does not cover the QMS or QC areas and is not a disaster-recovery certification.
- The S.G. Systems SLA §5.3 commits to a disaster recovery plan and periodic recovery testing.

Contract references: SLA §5.3 (v5ultimate.com/legal/sla#c5-3)

Encryption and data protection

11. How is data encrypted?

The Commercial Terms (MSA V1.24 for prior Orders) commit to encryption for hosted services and encrypted backups. Connections from users to the service use TLS. We are confirming the exact algorithms and scope for each layer, and share that confirmation on request rather than publish unverified detail.

- One internal connection, between the database connection pooler and the database, is still being confirmed. For that reason we don't claim end-to-end encryption.
- On-Premises customers manage their own encryption and keys.

Contract references: Commercial Terms §7.3 (v5ultimate.com/legal/commercial-terms#c7-3); Commercial Terms §9.1 security (v5ultimate.com/legal/commercial-terms#c9-1)

12. How quickly will you notify us of a breach?

Without undue delay and in any event within 72 hours of becoming aware of a Security Incident, followed by a detailed report within 3 business days. The clock runs from awareness, not from later confirmation. Any shorter period required by law or the DPA applies.

Contract references: Commercial Terms §9.2 (v5ultimate.com/legal/commercial-terms#c9-2)

13. Can we export our data when we leave, and what does it cost?

Yes. You can export using the software's standard export methods during the subscription and for 90 days after termination on request. Standard exports are not charged as migration services. Custom formats or extra work need a separate written agreement.

- Standard exports keep records linked to their audit trail and e-signature information as far as the export format allows.

Contract references: Commercial Terms §12.5 data export (v5ultimate.com/legal/commercial-terms#c12-5); Commercial Terms §5.4 after termination (v5ultimate.com/legal/commercial-terms#c5-4)

Insurance and commercial terms

14. What cyber and professional indemnity insurance do you hold?

We don't publish insurance limits. Ask us for current certificates and we will share them through the document request below.

15. Can the deposit be reviewed?

Payment and deposit terms are set in your Order and the applicable commercial terms. Requests to change them are reviewed by our commercial team; nothing is agreed until it is confirmed in writing.

Contract references: Commercial Terms Section 6 fees and payment (v5ultimate.com/legal/commercial-terms#s6)

16. Can the liability cap be reviewed?

The current Commercial Terms (§17) limit total liability to the fees paid under the applicable Order in the 12 months before a claim, subject to its agreed terms and exceptions. Requests to change the cap are reviewed by our commercial team and apply only once agreed in writing.

Contract references: Commercial Terms §17.1 (v5ultimate.com/legal/commercial-terms#c17-1)

Sources and evidence dates

- S.G. Systems Support & Service Level Agreement (v5ultimate.com/legal/sla, provided by S.G. Systems, LLC for direct and reseller customers), V5 Commercial Terms for Software and Services (v5ultimate.com/legal/commercial-terms) and SG Systems EULA (v5ultimate.com/legal/eula) — contractual commitments; Orders that accepted Master Services Agreement V1.24 (v5ultimate.com/legal/msa) keep its terms
- SG Systems backup and recovery policy SG-POL-BR-001 v2.9 and guide SG-GDE-BR-001 v2.7, 30 September 2026 — current operating facts (internal; summarised here, not published)
- Isolated recovery check of 30 September 2026 using 29 September 2026 copies — latest evidence
- Owner/CTO confirmation, 6 October 2026: the application runs in the Netherlands and Oregon with traffic shared between them; the database is unaffected (internal)

Controlled documents (backup and recovery policy summary, recovery-test evidence, encryption scope, insurance certificates, deployment-specific terms) are shared on request, usually under NDA. Request them at v5ultimate.com/security#procurement.