WHITEPAPER · SECURITY OF THE SOLUTION

REVIEWIT security whitepaper

How REVIEWIT protects the platform, the connections to your systems and your data: identity, isolation, encryption, evidence, the RITA assistant, operations and continuity. This whitepaper describes the measures in service at the date of publication and states plainly which ones are planned.

VERSION

1.0 · November 2026

SCOPE

REVIEWIT SAS · REVIEWIT SaaS solution, all regions

DISTRIBUTION

Public

CONTENTS

01 REVIEWIT at a glance
02 Security principles
03 Shared responsibility
04 Identity and access
05 Isolation and data residency
06 Encryption, keys and secrets
07 Evidence and audit trail
08 Connections to customer systems
09 RITA assistant
10 Development and operations
11 Incidents and continuity
12 Privacy, retention and compliance
13 Contact and documents

PURPOSE

REVIEWIT is a SaaS solution for access review and certification. To do so, it collects identity and entitlement metadata from its customers' systems and produces evidence of the decisions taken. This whitepaper is written for security officers and for procurement and compliance teams; it presents the security architecture of the solution, without any detail that would weaken its protection.

HOW TO READ

Each measure carries a status. **In service**: operating at the date of publication. **Known limit**: in service, with the limit described. **Planned**: on REVIEWIT's roadmap, with no date committed. **Commitment**: a contractual obligation of REVIEWIT. The contractual reference is Annex 1 of the data processing agreement (technical and organisational measures); where they differ, it prevails over this document.

SECTION 01

REVIEWIT at a glance

REVIEWIT brings together, in a single loop, the discovery of access, its review by designated people and the evidence of the decisions. The solution connects to the customer's collaboration suites, identity directories and business applications, through dedicated connections or file import.

METADATA

Metadata, not content

Identities, accounts, groups, memberships, roles, resources and permissions. Never the content of messages, documents or files, never passwords.

NATIVE CONTROLS

Your controls stay in charge

REVIEWIT replaces neither the authentication nor the authorisation of connected platforms: it reads them, read only, with the permissions you grant.

HUMAN DECISION

A person decides

Every review decision is taken by a named person and recorded. The RITA assistant takes, recommends and drafts no decision.

EVIDENCE

Evidence that verifies

An audit trail chained and sealed every day, exportable with its digests and seals so it can be verified outside REVIEWIT.

SECTION 02

Security principles

PRINCIPLE	WHAT IT MEANS AT REVIEWIT
Zero Trust	No user, service, connection or network is trusted by default: every call is authenticated, and the subscription it targets is the one carried by its access token, checked at entry.
Least privilege	Roles held by REVIEWIT, with a mandatory expiry for named roles; read-only connections; each component reaches only the secrets its function needs.
Defence in depth	Layered controls: identity, authorisation, database isolation, private network, encryption, secrets vault, sealed audit trail.
Secure by default	The RITA assistant runs in deterministic mode by default, with no AI model; generative AI mode is active only on the customer's decision.
Data minimisation	Queries restricted to the attributes needed; each collection plan covers a single resource chosen by the customer; RITA only receives aggregates.
Customer control	The customer chooses its connections and collected scopes, its hosting region, its retention profile, whether RITA is enabled, and where its audit trail is sent.
Nothing announced unverified	A measure is called in service only once it has been observed; what is planned is called planned.

SECTION 03

Shared responsibility

The security of the solution is shared between four parties.

PARTY	RESPONSIBILITY
REVIEWIT	Application, connections, programming interfaces, subscription isolation, stored data, encryption and secrets vault, audit trail, development and release, vulnerability management, incident notification, access by its staff.
Our cloud hosting provider	Data centres and their physical security; compute, storage and network infrastructure; availability of managed services. Its security is attested by its ISO/IEC 27001 certifications and SOC reports.
Connected platforms	Native authentication and authorisation, exposed interfaces, enforcement of the permissions granted to REVIEWIT, availability of their service.
Customer	Choice of connected systems and scopes; permissions granted to connections; identity provider and its strong authentication policy; assignment of REVIEWIT roles; designation of reviewers; protection of its own credentials and of the key it imports.

SECTION 04

Identity and access

MEASURE	IMPLEMENTATION AT REVIEWIT	STATUS
Federated authentication	REVIEWIT's own identity authority (OpenID Connect), connected to the customer's identity provider, whose authentication policies apply.	IN SERVICE
Strong authentication for administrators	Required on the administration consoles and verified on return from the identity provider.	IN SERVICE
Reviewer authentication	Not enforced by REVIEWIT on the review console: its strength depends on the policy of the customer's identity provider.	KNOWN LIMIT
Roles and authorisation	Roles held by REVIEWIT and assigned in REVIEWIT: platform operator, subscription administrator, workspace roles, read-only auditor. Mandatory expiry for named roles.	IN SERVICE
Four-eyes approval	Sensitive operations are approved by two distinct people; this applies to the export and deletion of a subscription's databases at the end of the contract.	IN SERVICE
Access by REVIEWIT staff	Limited to need, recorded in the audit trail and, except in an emergency, performed at the customer's request.	IN SERVICE
SAML federation	Connection of identity providers through SAML 2.0.	PLANNED

SECTION 05

Isolation and data residency

MEASURE	IMPLEMENTATION AT REVIEWIT	STATUS
Dedicated databases	Each subscription has its own databases, with access roles specific to each and no connection right granted by default.	IN SERVICE
Subscription check	The subscription targeted by a call is the one carried by its access token, verified at the platform's entry.	IN SERVICE
Residency	Data stored and processed in the hosting region chosen by the customer (Paris by default); backups kept in that region.	IN SERVICE
No copy outside the region	No copy in another region, except on the customer's written instruction for a copy of backups in a second region of the same geography.	IN SERVICE
Databases not exposed	No database reachable from the Internet; no public IP address on the subnets; administration through a bastion, with neither SSH nor a public IP address.	IN SERVICE
Network	Virtual private network spread over two availability zones; chained filtering between the entry point, the services and the databases.	IN SERVICE
Web application firewall	Web application firewall, network flow logs and outbound flow filtering.	PLANNED

SECTION 06

Encryption, keys and secrets

MEASURE	IMPLEMENTATION AT REVIEWIT	STATUS
In transit	TLS 1.2 and 1.3 on entry points, redirection to HTTPS, HSTS in the consoles; TLS enforced to the databases.	IN SERVICE
At rest	Databases encrypted at storage level; archives encrypted with a dedicated key rotated every year; signing vault on a rotated key; infrastructure state files encrypted (AES-GCM).	IN SERVICE
Platform secrets	No secret in configuration or in logs; our cloud hosting provider's secrets manager; an internal certificate authority that renews service identities and keeps a revocation list of callers.	IN SERVICE
Connection credentials	In the custody of REVIEWIT SEAL: encrypted under a master key dedicated to each customer and bound to their holder; no function, administrative or otherwise, can read their value.	IN SERVICE
Credentials predating custody	Credentials deposited before custody went into service are taken over under their customer's master key, holder by holder; until then they are protected only by the databases' encryption at rest.	KNOWN LIMIT
Customer key for signing	The customer can import its own connection private key into the SEAL vault, which signs with it; the key is never exported.	IN SERVICE

Encryption with a customer key	Encryption under a master key held or imported by the customer.	PLANNED
Key rotation	Master key of each subscription: automatic yearly rotation. Each customer's keys in the SEAL vault: rotated every year. SEAL signing key: fixed expiry, alert before its term. Service identities: automatic renewal.	IN SERVICE

The **SEAL Security Sheet** (public) and the **Key and Secret Management Annex** (customers and prospects under a non-disclosure agreement) detail key models, revocation and deletion of secrets.

SECTION 07 Evidence and audit trail

The value of an access review lies in its evidence. REVIEWIT builds it so that an auditor can verify it independently, without having to trust REVIEWIT.

MEASURE	IMPLEMENTATION AT REVIEWIT	STATUS
Event content	UTC timestamp, actor, effective role, action, outcome.	IN SERVICE
Chaining and seals	Events canonicalised and chained by SHA-256 digest; each chain is sealed every day by the REVIEWIT SEAL sealing authority; any alteration becomes detectable.	IN SERVICE
Purge	By whole sealed segment, never row by row; the register of purges is protected against modification and deletion.	IN SERVICE
Streaming to your SIEM	Events streamed to the customer's SIEM (BEACON).	IN SERVICE
Verifiable export	Audit trail exportable with its sequence, chained digests and signed seals; the customer verifies its integrity following a documented procedure.	IN SERVICE

SECTION 08 Connections to customer systems

MEASURE	IMPLEMENTATION AT REVIEWIT	STATUS
Read only	Collection is read only: no write to Microsoft 365 or to Google Workspace.	IN SERVICE
Permission broader than read	Where a platform offers no sufficient read permission, as for reading the permissions of SharePoint sites, the permission requested is only ever exercised to read.	IN SERVICE
Chosen scope	Each collection plan covers a single resource chosen by the customer; queries are restricted to the attributes needed.	IN SERVICE
Up-to-date mirror	Mirror refreshed at every collection: an account that disappears from the source disappears from the mirror.	IN SERVICE

Credentials in custody	Connection credentials in the custody of SEAL (section 06); the customer can withdraw its consent at the source platform at any time.	IN SERVICE

SECTION 09 RITA assistant

RITA helps read access and campaigns. It takes, recommends and drafts no review decision.

MEASURE	IMPLEMENTATION AT REVIEWIT	STATUS
Customer control	Can be disabled per subscription and per provider; deterministic mode by default, with no call to an AI model; no write tool.	IN SERVICE
Generative AI mode	Active only if the customer enables it through an AI processing addendum; routes limited to the region's geography (European for the European Union); any other route is refused server side.	IN SERVICE
No training	Neither REVIEWIT nor its providers use customer data to train models.	COMMITMENT
Retention	Conversations never kept; a digest of each question kept 12 months in the audit trail; log of data questions purged at 30 days.	IN SERVICE
Filtering	Secrets filtered out before anything is sent to the model; pinned model version; RITA only receives aggregates.	IN SERVICE

SECTION 10 Development and operations

MEASURE	IMPLEMENTATION AT REVIEWIT	STATUS
Static analysis	Code analysers run at every build.	IN SERVICE
Automated tests	Automated test suites, including negative access tests on the consoles.	IN SERVICE
Release chain	Container images with immutable tags, scanned on push and deployed by digest; sealed release manifest, required for the stable channel.	IN SERVICE
Vulnerability management	Monitoring of code, dependencies, images and configuration; fix or mitigation within 14 days for a critical vulnerability, within 30 days for a high one, in the normal release cycle for the others.	COMMITMENT
Public status page	External probes run from several regions against every provisioned region; availability history and incidents published.	IN SERVICE
Penetration test	Yearly penetration test by an independent third party.	PLANNED
Centralised detection	Logging of administrative calls, threat detection and centralised alerting at the hosting provider; on-call duty.	PLANNED

SECTION 11

Incidents and continuity

MEASURE	IMPLEMENTATION AT REVIEWIT	STATUS
Personal data breach	Notification to the customer no later than 24 hours after becoming aware, including when the breach occurs at a sub-processor; updates as the investigation proceeds.	COMMITMENT
Security incident (NIS 2, DORA)	For the customers concerned: early warning within 24 hours, update within 72 hours, final report within one month; when in doubt, the incident is notified.	COMMITMENT
Backups	Automatic database backups, kept 35 days in production; database spread over two availability zones.	IN SERVICE
Verified export	Export of a subscription verified by an actual restore.	IN SERVICE
Recovery objectives	Recovery point objective (RPO) of 24 hours and recovery time objective (RTO) of 48 hours, for a service designated as supporting a critical or important function (DORA).	COMMITMENT
Timed restore test	Timed test verifying these objectives.	PLANNED

The **Backup and Recovery Strategy — summary** (public) details these measures.

SECTION 12

Privacy, retention and compliance

MEASURE	IMPLEMENTATION AT REVIEWIT	STATUS
GDPR roles	The customer is the controller and REVIEWIT the processor, under a data processing agreement (Article 28); processing on the customer's documented instructions.	IN SERVICE
Sub-processors	Each provider's processing agreement archived and assessed; any addition or replacement notified thirty days in advance, with a right to object.	IN SERVICE
Storage limitation	Catalogue of 37 data categories with ratified periods; retention profile chosen by the customer; purge by the product; deletion register kept outside backups; holds recorded.	IN SERVICE
Data subject rights	Search for a person across a subscription's databases, export and erasure, under the reference of the request.	IN SERVICE
End of contract	Verified export of the subscription, delivery of a return package, erasure of the databases, certificate of deletion; no switching charges.	IN SERVICE
REVIEWIT certification	REVIEWIT does not yet hold a certification of its own and claims none before obtaining it; the ISO/IEC 27001 process is under way.	PLANNED

The solution helps its customers produce the access review evidence expected under the GDPR, ISO/IEC 27001, NIS 2, DORA or SOC 2; this does not make REVIEWIT a certified entity under those frameworks.

SECTION 13 Contact and documents

Security questions and vulnerability reports: **security@we-reviewit.com**. REVIEWIT acknowledges every report and handles it under its vulnerability disclosure policy. We ask researchers not to access, modify or retain any customer data.

DOCUMENT	ACCESS
Vulnerability disclosure policy	Public
SEAL Security Sheet (sealing, key management)	Public
Backup and Recovery Strategy — summary	Public
Key and Secret Management Annex	Customers and prospects under a non-disclosure agreement
Technical and organisational measures (Annex 1 of the DPA)	Customers · authenticated access
Data processing agreement and its annexes	Customers · authenticated access
REVIEWIT ICT service providers	Customers · authenticated access

REVIEWIT SAS · Security: security@we-reviewit.com · Data protection: dpo@we-reviewit.com. Reviewed annually and after any major change to the solution. The French version is authoritative.