DÉTENTEIQ LLC

BUSINESS CONTINUITY AND DISASTER RECOVERY SUMMARY

Effective date: August 2026

Please accept this summary as a plain statement of how DétenteIQ protects a firm's continued access to its data and how the service is recovered if something goes wrong, including the arrangements that apply if the company itself is disrupted. It is written candidly, including about the fact that DétenteIQ is a small, focused company, because a defense firm is entitled to understand both the safeguards in place and how they are designed to work independently of any one person.

Hosting and architecture

DétenteIQ runs as a hosted application on Amazon Web Services, with a PostgreSQL database and a reverse proxy that terminates TLS using managed certificates. Data is encrypted at rest and in transit, every query is scoped to the requesting firm's tenant, and firms may elect end-to-end encryption under which matter content is encrypted in the browser with a key the company never holds. The security architecture is described in detail in our Architecture, Security, and Data Handling memorandum.

Recovery objectives

Our recovery point objective (RPO) is **not more than 24 hours** of data: backups are taken at least nightly, so in the worst case a recovery loses no more than the work since the last backup. Our recovery time objective (RTO) is **restoration of service within 8 business hours** of a declared disaster. These are the objectives we operate to today; both improve as additional backup frequency and infrastructure redundancy are added, and we will state stronger figures as they are in place rather than before.

Backups

Client data is backed up automatically on at least a nightly schedule to encrypted storage held separately from the running instance, under write-only credentials so that a compromise of the server cannot reach and destroy the backup history. The ability to restore from backup is verified on a recurring, at-least-quarterly basis; a backup that has never been restored is treated as unproven, which is why we test it rather than assume it.

Disaster scenarios and response

The service is rebuilt from documented, version-controlled procedure rather than from memory. If the running instance is lost, it is recreated from an image and the database is restored from the most recent verified backup. If data is corrupted, it is restored to the last good point. If the

hosting region is disrupted, the service is restored to an alternate region from the off-instance backups. Detection is not left to a firm's report: the service is continuously monitored for errors, for availability against its health endpoint, and for resource exhaustion such as low disk, with alerts routed to the operator in real time.

Continuity of operations

Because DétenteIQ is operated by a small team, continuity is deliberately built so that operation does not depend on any single individual's institutional knowledge. The system is documented in a written operations runbook covering deployment, backup and restore, rollback, and incident response, in enough detail that a qualified engineer can operate and recover the service without prior familiarity with it. Access credentials and recovery materials are held in secured storage. Continuity does not rely on the founder alone being reachable; the runbook is written so that recovery is a matter of following documented procedure rather than reconstructing knowledge that lives in one person's head.

Continuity of the company

If DétenteIQ LLC were unable to continue operating, a firm's data is never trapped. Client data is exportable in a standard, usable format at any time on request, so a firm can leave with its own records at any point, independent of the company's status. Reasonable wind-down and transition assistance is available under the Master Services Agreement.

Data ownership, export, and deletion

The firm owns its matter data. On request, the firm's data is exported in a standard format. On termination, data is removed from active systems and rolls out of backups on the normal retention cycle. Client data is never pooled with other firms; any benchmarking is opt-in and de-identified before anything leaves the firm.

Testing and review

Backups and the restore procedure are verified at least quarterly. This continuity and disaster-recovery plan is reviewed at least annually and after any material change to the architecture, and is updated as recovery objectives are strengthened.

Questions may be directed to hello@detenteiq.com or (941) 800-1923.