Data Security Operating Summary

Didaxis Group approaches client data security as an operating discipline, not a marketing claim. The goal is to make data access, implementation work, and project closeout reviewable by internal IT, procurement, and executive stakeholders.

What this means in practice

Control area	Working standard
Access requests	Every access request is documented by system name, required data elements, access level, duration, and technical method before work begins.
Permission model	**Read-only** access is the default. Any elevated privilege must be explicitly justified and approved.
Identity and authentication	Institutional SSO and MFA are preferred wherever available. Access is tied to the named operator performing the work.
Data location	Client data stays inside the client-approved environment whenever possible. Data is not moved into personal storage, side spreadsheets, or unapproved tools for convenience.
Infrastructure approach	Repositories, staging databases, ETL orchestration, secrets storage, and dashboards are designed to live in client-owned or client-approved infrastructure when data work is in scope.
Credential handling	Credentials are stored in approved secrets tooling or a password manager. They are not hardcoded in code, config files, or informal messages.
Approved tools	Tools that directly process client data, indirectly touch supporting content, or have no data contact are disclosed in writing before work starts.
AI-use policy	No client data is submitted to third-party AI tools unless a specific use case is approved in writing in advance.
Incident response	Any actual or suspected unauthorized access is escalated to the client within **24 hours**, with written follow-up and full cooperation during response.
Closeout	Access revocation, repository handoff, and a written data destruction confirmation are treated as formal engagement deliverables.

Review-ready artifacts clients can expect

Clients should expect more than verbal assurances. A disciplined engagement can include the following review artifacts.

Artifact	Why it matters
Access inventory	Lets IT review the exact systems, permissions, and data elements requested before credentials are provisioned.
Tools disclosure exhibit	Shows which tools directly process client data, which only touch support materials, and which have no client-data contact.
Environment confirmation	Clarifies where repositories, orchestration, staging, dashboards, and secrets will live before implementation begins.
Incident response summary	Gives IT and procurement a defined escalation path rather than an improvised response.
Revocation confirmation	Proves access was removed at the end of the project or phase.
Data destruction letter	Documents that remaining extracts, credentials, and retained materials were handled according to the agreed schedule.

Operating principles

Least privilege. Access is limited to the minimum systems and permissions needed for the scoped work.

No informal sprawl. Client operational data is not treated as something that can be casually copied into ad hoc files or personal tools.

Named-user accountability. Access, approvals, and closeout actions are attributable to the specific operator performing the work.

Prepared security review. Vendor registration, tool disclosure, incident handling, and HECVAT-style review are approached as part of delivery readiness, not as afterthoughts.

Typical client questions

How is access controlled?

Access is requested by exact system, data element, duration, and access level. Read-only is preferred by default, and scope boundaries are reviewed before use.

Where does the data live?

Within the client-approved environment whenever possible. The intent is to avoid off-platform copies and keep operational work inside the client's security perimeter.

What happens if there is a suspected incident?

Work stops, the client is notified within 24 hours, and the response is coordinated with the client's IT or security team.

What happens at the end of the engagement?

Access is revoked, credentials are removed, required extracts are deleted, and a written closeout or destruction confirmation can be provided.

For security and procurement review

This summary is intended to support early-stage conversations with IT, security, procurement, and executive sponsors. More detailed operating documentation can be shared when a project moves into formal review.