Action360

Security & Compliance Documentation Pack

Prepared for client procurement and SOW review, covering the handling of client data outside the CP360 environment.

Item	Detail
Product	Action360 operational governance and action management platform
Vendor / legal entity	**[CONFIRM — legal entity name]**
Document version	1.0
Date	17 August 2026
Review cycle	Annual
Classification	Confidential — share under NDA
Security contact	**[CONFIRM — security contact address]**

Items marked [CONFIRM] must be completed by the vendor before this pack is issued. They are facts we will not assert on your behalf.

Contents

Action360 — Security Questionnaire Response

Vendor / legal entity: **[CONFIRM — legal entity name]** **Product:** Action360 operational governance and action management platform **Document owner:** **[CONFIRM — security contact name and email]** **Version:** 1.0 · **Date:** 17 August 2026 · **Review cycle:** annual

Answers use **Yes**, **No**, or **Compensating control**. Items marked **[CONFIRM]** require a fact from the vendor before the document is issued to a client.

1. Governance and policy

#	Question	Answer	Notes
1.1	Is there a documented information security policy?	Yes	Reviewed annually by **[CONFIRM — policy owner]**.
1.2	Is there a named individual accountable for security?	Yes	**[CONFIRM — name and title]**.
1.3	Do staff receive security awareness training?	Yes	On joining and annually thereafter.
1.4	Are background checks performed on staff with data access?	**[CONFIRM]**	
1.5	Are confidentiality/NDA terms in place with all staff and contractors?	Yes	
1.6	Is a risk register maintained and reviewed?	Yes	Managed in Action360 itself.

2. Access control and authentication

#	Question	Answer	Notes
2.1	Is access granted on least-privilege principles?	Yes	Six roles: Super Admin, Admin, Manager, Owner, Viewer, Client.
2.2	Is multi-factor authentication enforced?	Yes	Enforced at **[CONFIRM — identity layer: corporate IdP / application login]** using **[CONFIRM — TOTP / push / hardware key]**. See section 2.9.
2.3	Is single sign-on supported?	Yes	**[CONFIRM — SAML or OIDC]**, IdP **[CONFIRM]**, **[CONFIRM — enforced or optional]**.
2.4	Can end users self-register?	No	Accounts are provisioned by a Super Admin or Admin only. Public sign-up is disabled.
2.5	Are users forced to change an administrator-set password?	Yes	A first-login password change is mandatory for every role, and again after any admin-led reset.
2.6	Are passwords stored securely?	Yes	Salted one-way hashes held by the managed authentication service; never accessible to application code or staff.
2.7	Is access reviewed and revoked on leaver events?	Yes	Admins deactivate the profile, which immediately revokes application access.

#	Question	Answer	Notes
2.8	Is client data segregated between tenants?	Yes	Every tenant table enforces row-level security bound to the caller's active account, plus group-level visibility rules. See document 04.
2.9	Does the application itself prompt for a second factor?	Compensating control	The Action360 login is email plus password. MFA is enforced at **[CONFIRM — identity layer]**, combined with admin-only provisioning, forced first-login password change and full audit logging.

3. Data protection and encryption

#	Question	Answer	Notes
3.1	Is data encrypted in transit?	Yes	TLS 1.2+ (TLS 1.3 preferred) on all browser, API and database connections; HTTPS enforced with HSTS.
3.2	Is data encrypted at rest?	Yes	AES-256 for the database, object storage and backups.
3.3	Are keys managed by a dedicated key management service?	Yes	Provider-managed KMS with automatic rotation; no keys in source code.
3.4	Are secrets kept out of source control?	Yes	Held in the platform secret store and injected at runtime.
3.5	Is client data used to train AI models?	No	Copilot requests are inference-only; no training or retention by the model provider.
3.6	Is production data used in test environments?	No	

4. Application security

#	Question	Answer	Notes
4.1	Is input validated server side?	Yes	Schema validation on every server function.
4.2	Is authorisation enforced server side rather than in the UI?	Yes	Database row-level security is the enforcement point; the UI only reflects it.
4.3	Are dependencies scanned for known vulnerabilities?	Yes	Automated dependency and platform security scanning.
4.4	Is a secure development lifecycle followed?	Yes	Change review before release, versioned migrations for all schema changes.
4.5	Has a penetration test been performed?	**[CONFIRM — date and tester, or state "planned"]**	
4.6	Is there a vulnerability disclosure route?	Yes	**[CONFIRM — security@ address]**.

5. Logging, monitoring and audit

#	Question	Answer	Notes
5.1	Are security-relevant events logged?	Yes	User creation, role changes, password resets, approvals, status changes and deletions are written to an append-only audit log.
5.2	Can audit logs be altered or deleted by users?	No	Update and delete are denied at database policy level.
5.3	Is an activity timeline available per record?	Yes	Every action carries a full timeline, exportable to PDF for audit review.
5.4	How long are audit logs retained?	13 months	Aligned to the client data retention period.

6. Incident response

#	Question	Answer	Notes
6.1	Is there a documented incident response plan?	Yes	**[CONFIRM — last tabletop exercise date]**.
6.2	What is the breach notification commitment?	Yes	Affected clients notified without undue delay and within 72 hours of confirmation.
6.3	Is there a named incident contact?	Yes	**[CONFIRM — incident reporting address]**.

7. Business continuity

#	Question	Answer	Notes
7.1	Are backups taken?	Yes	See document 05.
7.2	Has a restore been tested?	Yes	Last tested restore: **[CONFIRM — date]**.
7.3	Are RPO and RTO defined?	Yes	RPO **[CONFIRM]** · RTO **[CONFIRM]**.
7.4	Is infrastructure redundant across availability zones?	Yes	Managed platform with multi-AZ storage.

8. Data handling, retention and subprocessors

#	Question	Answer	Notes
8.1	What client data is processed?	—	See document 02.
8.2	How long is client data retained?	13 months	See document 06.
8.3	Is data deleted on request?	Yes	Within 30 days of a verified request; backups age out inside the backup retention window.
8.4	Is client data transferred outside the agreed hosting region?	No	Primary hosting region **[CONFIRM]**.
8.5	Are subprocessors disclosed?	Yes	See document 08.
8.6	Will you sign a DPA?	Yes	

9. Compliance and certification

#	Question	Answer	Notes
9.1	Are certifications held?	Yes	**[CONFIRM — SOC 2 Type I/II, ISO/IEC 27001, other]**, certifying body **[CONFIRM]**, scope **[CONFIRM]**, report date **[CONFIRM]**.
9.2	Can the report be shared?	Yes	Under NDA on request.
9.3	Do you rely on certified infrastructure providers?	Yes	Hosting and database platforms hold their own independent attestations; copies available on request.

Action360 — Data Flow and Hosting

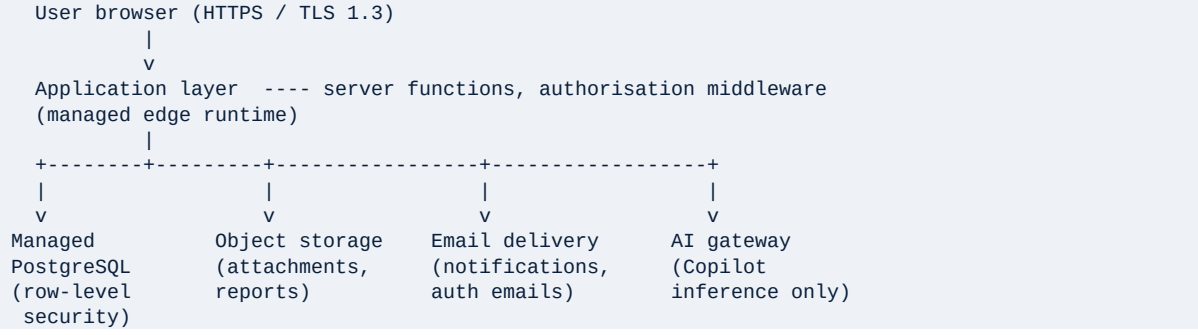
Version: 1.0 · **Date:** 17 August 2026

1. What data Action360 holds

Category	Fields	Source
Account (tenant) records	Account name, slug, industry, logo	Created by a Super Admin
User profiles	Name, work email, job title, department, active flag, last seen	Created by an Admin; no self sign-up
Roles and groups	Role assignment per account, group membership	Admin-managed
Action records	Reference, subject, description, owner, priority, status, due date, progress, SLA window	Entered by users
Risk records	Reference, title, description, likelihood, impact, mitigation, owner, review date	Entered by users
Change records	Reference, title, description, change type, impact level, go-live date, owner	Entered by users
Sub-tasks, comments	Title, body, author, timestamps	Entered by users
Attachments	Uploaded files and metadata linked to a record	Uploaded by users
Readiness	Workstream, criteria, score, target, assessment date	Entered by users
Notifications	Title, body, severity, delivery status	System-generated
Activity and audit logs	Actor, event, target, severity, metadata, timestamp	System-generated

Action360 is a governance tool for operational records. It is **not** designed to hold special-category personal data, payment card data or health records, and clients should not upload such data as attachments.

2. Data flow



1. The browser authenticates against the managed authentication service and receives a short-lived bearer token.

2. Every request to the application layer carries that token. Server functions verify it before touching data.
3. All database reads and writes execute **as the calling user**, so PostgreSQL row-level security decides what is visible — never the UI alone.
4. Attachments and generated reports are stored in private object-storage buckets; access is granted through short-lived signed URLs only.
5. Notification emails are queued in the database and dispatched by a background job through the email provider.
6. Copilot prompts are sent to the AI gateway for inference. Responses are not stored by the model provider and are not used for training.

3. Hosting

Item	Detail
Application hosting	Managed serverless edge platform
Database	Managed PostgreSQL, multi-AZ, encrypted at rest
Object storage	Managed private buckets, encrypted at rest
Primary region	**[CONFIRM — e.g. eu-west-1 / us-east-1]**
Data residency commitment	Client data remains within the primary region; no replication outside it
Network exposure	HTTPS only; the database is not exposed to the public internet
Environments	Production is separate from preview/development; no production data in non-production environments

4. Data outside the CP360 environment

Client data is processed by the platform described above rather than inside the CP360 corporate network. Controls applied specifically for that reason:

- Single-tenant isolation per client account enforced in the database.
- Admin-only provisioning — no client-side self sign-up.
- Append-only audit trail of every privileged action.
- 13-month retention with contractual deletion on request.
- Subprocessors disclosed in document 08 and covered by data-processing terms.

Action360 — Encryption Standards

Version: 1.0 · **Date:** 17 August 2026

1. In transit

Channel	Protection
Browser to application	TLS 1.2 minimum, TLS 1.3 preferred; HTTP redirected to HTTPS; HSTS enabled
Application to database	TLS-encrypted connections over the provider's private network
Application to object storage	HTTPS with signed, short-lived URLs
Application to email provider	TLS-encrypted API calls; opportunistic TLS on SMTP delivery
Application to AI gateway	HTTPS

Certificates are provider-managed and rotated automatically. Legacy protocols (SSL 3.0, TLS 1.0/1.1) and weak ciphers are disabled.

2. At rest

Store	Protection
PostgreSQL database	AES-256 full-volume encryption
Object storage (attachments, exported reports)	AES-256 server-side encryption
Backups and snapshots	AES-256, encrypted with the same managed keys
Application logs	Encrypted at rest by the platform

3. Key management

- Keys are held in the provider's managed key management service.
- Rotation is automatic and provider-managed; application code never handles raw encryption keys.
- API keys and service credentials live in the platform secret store, injected as environment variables at runtime and never committed to source control.
- Privileged service credentials are not retrievable by application users or by support staff through the product.

4. Credentials and tokens

Item	Handling
User passwords	Salted one-way hash (bcrypt-class) stored by the managed auth service; never visible to application code, administrators or support
Session tokens	Short-lived signed JWTs, refreshed automatically, transmitted over HTTPS only
Administrator password resets	Set a temporary password and flag the account so the user must choose a new one at next sign-in

Item	Handling
File access	Time-limited signed URLs; buckets are private with no public read

5. Cryptographic assurance

- No custom or home-grown cryptography is used anywhere in the platform.
- All primitives come from the managed platform and standard, maintained libraries.
- Third-party attestation of the underlying cryptographic controls is available from the hosting provider on request.

Action360 — Access Control

Version: 1.0 · **Date:** 17 August 2026

1. Identity and authentication

Control	Position
Self sign-up	Disabled. Accounts are created by a Super Admin or Admin.
Application sign-in	Email and password against the managed authentication service.
Multi-factor authentication	Enforced at **[CONFIRM — corporate identity provider / application login]** using **[CONFIRM — TOTP, push or hardware key]**.
Single sign-on	**[CONFIRM — SAML 2.0 or OIDC]** with **[CONFIRM — IdP name]**; **[CONFIRM — enforced or optional]**.
First-login password change	Mandatory for every role. The profile carries a `must_change_password` flag set on creation and on any admin-led reset; the user cannot reach the workspace until a new password is set.
Password storage	Salted one-way hash held by the managed auth service.
Session handling	Short-lived tokens with automatic refresh; sign-out clears the client cache.
Deactivation	Admins deactivate a profile, immediately revoking access.

2. Role model

Role	Capabilities
Super Admin	Create and delete accounts, move users between accounts, delete tickets, all Admin rights
Admin	Manage users, groups, departments, account settings, reset passwords, view audit logs
Manager	View and manage records for the groups they belong to; approve or reject actions
Owner	Create and update records they own, change due dates, close records
Viewer	Read-only access to permitted records
Client	Read-only external stakeholder: dashboard, governance calendar and reports only; locked to one account; account switching blocked in the database

Roles are stored in a dedicated `user_roles` table, never on the user profile, and are evaluated through security-definer functions to prevent privilege escalation through policy recursion.

3. Authorisation enforcement

Authorisation is enforced in the database, not the interface. Every tenant table has row-level security enabled with policies that combine:

1. **Account scope** — rows must belong to the caller's active account (`current_org_id()`).

2. **Group scope** — where the caller belongs to groups, they see records created by members of those groups (`can_view_record()`).
3. **Capability** — write and approval operations are gated by `can_write()` and `can_approve()`.
4. **Explicit grants** — each table grants only the privileges its policies allow; no default public access.

Because these run in PostgreSQL, a user cannot reach another account's data by manipulating the client, calling the API directly, or replaying a request.

4. Multi-account isolation

- Each client is a separate account (tenant) with its own records, users, groups, departments, branding and settings.
- Users may belong to more than one account and switch between them; the switch is validated server-side and re-scopes every subsequent query.
- Users with the Client role cannot switch accounts — the database function rejects the attempt.
- Owner and assignee pickers list only users in the active account.

5. Administrative access

Control	Position
Privileged actions	User creation, role changes, password resets, account deletion and record deletion are logged to an append-only audit log with actor, target, severity and timestamp
Audit log integrity	Update and delete are denied by policy for all application roles
Break-glass platform access	Restricted to **[CONFIRM — named administrators]**; access is logged by the platform
Access review	**[CONFIRM — review cadence, e.g. quarterly]**

Action360 — Backup and Disaster Recovery

Version: 1.0 · **Date:** 17 August 2026

1. Backup regime

Item	Detail
Database backups	Automated daily full backups with continuous write-ahead logging for point-in-time recovery
Backup retention	**[CONFIRM — e.g. 7 days point-in-time, 30 days daily snapshots]**
Object storage (attachments, reports)	Redundant multi-AZ storage with versioning
Encryption	All backups encrypted at rest with AES-256
Backup location	Same region as the primary data store; no cross-region copies outside the agreed region
Access to backups	Restricted to platform administrators; restores are logged

2. Recovery objectives

Objective	Target
Recovery Point Objective (RPO)	**[CONFIRM]**
Recovery Time Objective (RTO)	**[CONFIRM]**
Maximum tolerable outage	**[CONFIRM]**

3. Resilience of the running service

- Application runs on a managed serverless edge platform with automatic failover; there is no single application server to lose.
- Database and object storage are multi-AZ within the hosting region.
- Deployments are versioned and can be rolled back to the previous release.
- Schema changes ship as forward-only, versioned migrations held in source control, so an environment can be rebuilt from scratch.

4. Restore procedure

1. Declare the incident and notify the incident contact.
2. Identify the recovery point (snapshot or point-in-time timestamp).
3. Restore the database to a new instance from the chosen recovery point.
4. Verify integrity: record counts per tenant table, most recent audit log entries, and a sample of attachments resolved through signed URLs.
5. Repoint the application, re-run smoke tests (sign-in, dashboard, create and close an action, generate a report).

6. Notify affected clients and record the event in the audit trail and the incident log.

5. Testing

Item	Detail
Last tested restore	**[CONFIRM — date]**
Test type	**[CONFIRM — full restore to an isolated environment / point-in-time restore]**
Outcome	**[CONFIRM — result and any remediation]**
Test frequency	**[CONFIRM — e.g. annually]**
Next scheduled test	**[CONFIRM — date]**

6. Dependency failure

Dependency	Impact if unavailable	Mitigation
Email provider	Notification emails delayed	Notifications are queued in the database with retry and delivery status; in-app notifications are unaffected
AI gateway	Copilot unavailable	Core governance functionality is unaffected
Object storage	Attachment upload and download unavailable	Record data remains readable and editable

Action360 — Data Retention and Deletion

Version: 1.0 · **Date:** 17 August 2026

1. Retention standard

Client data is retained for 13 months.

Data category	Retention	Trigger
Action, risk and change records	13 months	From record closure
Sub-tasks, comments, readiness entries	13 months	From closure of the parent record
Attachments	13 months	From upload, or closure of the linked record if later
Generated reports and report history	13 months	From generation
Notifications	13 months	From creation
Activity and audit logs	13 months	From event
User profiles	Life of the engagement	Deactivated immediately on leaver notification
Account (tenant) records	Life of the engagement	Deleted per section 3

The 13-month window is chosen so a client can review a full year of governance history plus a reporting month, and no longer.

2. Deletion on request

- A client or Admin may request deletion of specific records or of an entire account at any time.
- Verified deletion requests are completed within **30 days**.
- Deletion removes the primary records, their comments, sub-tasks, approvals, attachments and generated reports.
- Backups are not edited. Deleted data ages out of backups inside the backup retention window (**[CONFIRM — e.g. 30 days]**), after which no copy remains.
- A deletion event is recorded in the audit log: who requested it, what scope, when it completed. The log entry itself contains no deleted content.

3. End of contract

1. On termination, the client may request a full export. Action360 provides multi-sheet Excel, CSV, PDF and PowerPoint exports covering all records.
2. Access is revoked at the agreed date.
3. Unless a longer period is agreed in writing, all client data is deleted within 30 days of contract end, and purged from backups within the backup retention window thereafter.
4. A written confirmation of deletion is issued on request.

4. Data minimisation

- Only work-context personal data is collected: name, work email, job title, department, role and group membership.
- No payment data, government identifiers, health data or other special category data is collected by the platform.
- Clients are contractually asked not to upload special category data as attachments.

5. Data subject requests

Request	Handling
Access	Export of all records naming the individual, provided within 30 days
Rectification	Admins can correct profile and record fields directly
Erasure	Profile deactivated and personal fields removed; governance records may be retained in pseudonymised form where required for audit, then deleted at the 13-month mark
Objection / restriction	Account deactivated pending resolution

Requests should be sent to **[CONFIRM — privacy contact address]**.

Action360 — Compliance and Certifications

Version: 1.0 · **Date:** 17 August 2026

1. Certifications held

Certification	Scope	Certifying body	Report / certificate date	Next assessment
[CONFIRM — e.g. SOC 2 Type II]	[CONFIRM — systems and services in scope]	[CONFIRM — auditor]	[CONFIRM]	[CONFIRM]
[CONFIRM — e.g. ISO/IEC 27001:2022]	[CONFIRM]	[CONFIRM]	[CONFIRM]	[CONFIRM]

Reports and certificates are shared with clients and prospects under NDA on request. Send requests to **[CONFIRM — security contact address]**.

Only certifications that are currently in force and evidenced by a certificate or report should be listed above. Remove any row that cannot be evidenced.

2. Infrastructure provider attestations

The underlying hosting, database, storage and email platforms maintain their own independent attestations (typically SOC 2 Type II and ISO/IEC 27001). Copies of the current provider reports can be supplied alongside our own on request.

3. Regulatory position

Topic	Position
Data protection regime	[CONFIRM — e.g. UK GDPR / EU GDPR / other]
Role	Processor, acting on the client's documented instructions
Data Processing Agreement	Available and signed on request
International transfers	Client data remains in the agreed hosting region ([CONFIRM]); where a transfer is unavoidable it is covered by Standard Contractual Clauses
Breach notification	Affected clients notified without undue delay and within 72 hours of confirmation
Sub-processing	Disclosed in document 08; clients notified before a new subprocessor is engaged

4. Control framework mapping

The controls described in documents 01–06 map to the following common control areas, which is usually enough for a client to close out a questionnaire:

Control area	Where evidenced
Access control and identity	Document 04
Cryptography	Document 03

Control area	Where evidenced
Operations security and logging	Documents 01 (§5) and 04 (§5)
Communications security	Documents 02 and 03
Supplier relationships	Document 08
Incident management	Document 01 (§6)
Business continuity	Document 05
Compliance	This document

5. Assurance available to clients

- Completed security questionnaire (document 01), refreshed annually.
- Certification reports under NDA.
- Penetration test summary: **[CONFIRM — date and tester, or "planned"]**.
- Named security contact for follow-up questions: **[CONFIRM]**.

Action360 — Subprocessors

Version: 1.0 · **Date:** 17 August 2026

The following third parties process client data on our behalf in the delivery of Action360. Clients are notified before a new subprocessor is engaged.

Subprocessor	Purpose	Data categories	Hosting region	Attestations
[CONFIRM — application and backend hosting provider]	Application hosting, managed PostgreSQL, authentication, object storage	All record data, user profiles, attachments, audit logs	**[CONFIRM]**	**[CONFIRM — e.g. SOC 2 Type II, ISO 27001]**
[CONFIRM — email delivery provider]	Transactional and notification email	Recipient name and work email, notification subject and body	**[CONFIRM]**	**[CONFIRM]**
[CONFIRM — AI gateway / model provider]	Copilot question answering, inference only	Prompt text and the workspace context included in the prompt	**[CONFIRM]**	**[CONFIRM]**

Notes

- **No training on client data.** Copilot prompts are sent for inference only. The model provider does not retain them for training.
- **No advertising or analytics resale.** No client data is shared with advertising networks or data brokers.
- **Contractual controls.** Each subprocessor is engaged under terms that include confidentiality, security obligations and, where personal data is involved, data-processing terms with Standard Contractual Clauses for any transfer outside the agreed region.
- **Change process.** New or replacement subprocessors are announced to clients with **[CONFIRM — e.g. 30 days]** notice, and clients may object under the DPA.

Questions about this list: **[CONFIRM — security contact address]**.