AXION SECURITY OVERVIEW

ENGLISH MASTER — Draft v1

1. Security Approach

Axion applies a layered technical and organisational security approach designed to protect the Service, User data, uploaded content and AI-powered workflows.

The measures are intended, among other things, to prevent, detect, contain and mitigate risks relating to unauthorised access, malicious inputs, data leakage, abuse of the Service and manipulation of AI systems.

Axion follows a defence-in-depth approach: rather than relying on a single control point, the Service may apply complementary controls from User input through AI orchestration and source access to execution and handling of results.

2. AI and Prompt Security

Axion may apply security checks at interfaces and within workflows where Users can provide instructions to AI systems.

These controls are designed to address risks including prompt injection and instruction manipulation, attempts to override system or internal instructions without authorisation, attempts to bypass security or access restrictions, unauthorised influence over AI workflows, and attempts to obtain unauthorised data or system information.

Security checks may be applied at multiple points in an AI workflow. The system therefore does not rely solely on a single inspection of the User's initial input.

3. Separation of AI Execution and Orchestration

User instructions are not automatically passed directly to execution. Axion separates User input, AI orchestration processes, selection of sources and context, and individual execution operations.

This layered execution model reduces the risk that malicious or manipulated input can directly influence a privileged system function or another unauthorised resource.

4. Workspace, Project and Artifact Access Boundaries

Axion applies access and scope-based restrictions to operations involving workspaces, projects and Artifacts.

The system uses relevant User, project, workspace and Artifact context to determine which resources an operation may use.

One purpose of these controls is to reduce the risk that an AI workflow uses information belonging to an inappropriate User, project, workspace or Artifact.

5. RAG and Source Security

In source-based and retrieval-augmented workflows, Axion handles retrieved information subject to scope, source and access restrictions.

The system may verify which Artifacts and workspace sources may be used for a query, their User and project context, their active and available state, and the evidence and context actually available for the request.

Evidence-based workflows are intended, among other things, to reduce the risk of treating missing or inaccessible sources as evidence that is actually available.

6. Uploaded File Security

Axion may subject User-uploaded files to multiple security checks before processing.

Controls may include detection of malicious files and malware, validation of file types, MIME types and file extensions, restrictions on permitted file formats, file-size limits and additional validation before further processing.

Layered file-upload controls are intended to reduce risks associated with malicious, unsupported or unexpected content entering the system.

7. Web Application and Browser Security

Axion may apply HTTP- and browser-level security controls designed to reduce risks from attacks against the web application.

These may include Content Security Policy (CSP), Cross-Origin Resource Sharing (CORS) restrictions, trusted-host checks, framing and embedding restrictions, restrictions on loading external resources, limitations on active web content and objects, and additional HTTP security-header protections.

These policies are designed to permit resources required for operation of the Service while restricting unnecessary external execution and communication paths.

8. Input, Context, Execution and Output Validation

Across different workflows, Axion may apply validation and policy-based controls between User input, context supplied to AI systems, execution operations and generated results.

These controls reduce the risk that manipulated input, unauthorised context or inappropriate AI output directly triggers further privileged operations.

9. Defence in Depth

Axion's security model does not rely on a single defensive mechanism. The Service may apply multiple complementary controls at different points involving User input, AI workflows, source access, file handling, application communications and execution environments.

The objective is that bypass or failure of a single security control should not, by itself, automatically result in bypass of additional security boundaries.

10. Continuous Improvement and Security Limitations

Axion applies and develops technical and organisational measures appropriate to the nature of the risks and operation of the Service. Controls may evolve as the system, its capabilities and the threat environment change.

No information technology or artificial intelligence system can be considered completely secure in all circumstances. Axion's security measures are therefore intended to prevent, detect, contain and mitigate security risks and do not constitute an absolute guarantee that every security incident can be prevented.

11. Scope of this Document

This Security Overview is a high-level, publicly shareable description of Axion's security approach. It is not a complete technical specification, penetration-test report, audit report or the Technical and Organisational Measures (TOMs) annex to a Data Processing Agreement under Article 28 GDPR.

For security reasons, Axion does not publicly disclose detailed configuration, infrastructure or defensive information where disclosure could unnecessarily increase the attack surface of the Service.

Security or privacy enquiries: support@axionaiapp.com

Last updated: [DATE]
Version: [VERSION]