Security FAQ

General

SA01 - How are passwords stored in ISAAC®?

User's passwords are hashed using SHA-256, and ISAAC Connect's passwords are AES-CTR (128 bites) encrypted before being stored in the ISAAC database.

SA02 - How is defined the password policy in ISAAC®?

ISAAC offers several password policy levels. The basic policy requires a minimum of 6 characters. The intermediate level also requires at least 6 characters and must include one uppercase letter, one lowercase letter, one number, and one special character. The advanced policy is configurable by ISAAC administrators and can allow up to 100 characters, with customizable minimums for lowercase, uppercase, numeric, and special characters. Additionally, passwords can be configured to expire after 30 to 180 days, independently of the selected policy level.

SA03 - Is the communication with ISAAC® encrypted (data in transit)?

No. Communication between the browser and ISAAC services currently occurs over HTTP. However, it is possible to place a reverse proxy in front of ISAAC to enforce HTTPS, although some features are not yet fully compatible with this setup. In most cases ISAAC is deployed on-premises and within a dedicated VLAN, which limits security risks. Additionally, HTTPs native support is part of the roadmap.

SA04 - How is the ISAAC® API protected?

Only a part of the API is currently protected (the list of protected endpoints - in term of security - is available in the API specifications).

Protected endpoints require a token obtained after using the user login endpoint. The token is an opaque value which identifies the access rights of that user.

The API service does not enforce rate limiting, but there is a global time out for requests.

SA05 - How frequent and how ISAAC® updates are delivered?

ISAAC has 1 or 2 major releases per year and a patch release every 1 or 2 months in average. Occasionally a patch release can be quicker if necessary. Prior to ISAAC 2.5 or with 2.4 (or earlier) systems updated to 2.5 (non StageOS), the update requires Smart Monkeys support team intervention. For all 2.5 and later systems based on StageOS, updates can be done by ISAAC administrators when their are available.

Access Control

SB01 - What access control mechanisms are provided by ISAAC®?

Access to ISAAC is granted after the user logs in using her username and password. Upon login success a token is provided to the browser which require a token. The token is an opaque value which identifies the access rights of that user.

SB02 - How is authentication and sign-on handled?

ISAAC uses an internal authentication mechanism which uses the username and password provided by the user upon login to verify the user identity and returns a token. The token is an opaque value which identifies the access rights of that user.

SB03 - How is remote access handled?

ISAAC uses a browser for displaying its user interface over the LAN. If an external (off-site) access is required a VPN solution must be added.

SB04 - How does ISAAC handle role-based access controls (RBAC)?

ISAAC provides role-based access control (RBAC). Roles, created by administrators, define access levels for each part of the application (no access, read-only, or full access). Multiple roles can be assigned to a user to create combined access profiles.

SB05 - Does ISAAC enforces Multi-Factor Authentication (MFA)?

Not currently. However, Single Sign-On (through third-party identity providers) is part of the roadmap, which will offer MFA.

Data Privacy & Residency

SC01 - What data encryption does ISAAC® use for at rest data?

Data at rest is not encrypted except for passwords and secrets, which are either hashed or encrypted (see SB02 and SA01).

SC02 - Is the data stored into ISAAC® segregated between tenants?

ISAAC is not a multi-tenant system, so data segregation is not required. However, multiple user roles are available to limit access to specific data or features within the application (see below).

SC03 - Can the data stored into ISAAC® be selectively provided to users (is there an access rights management)?

Yes. ISAAC provides role-based access control (RBAC). Roles, created by administrators, define access levels for each part of the application (no access, read-only, or full access). Multiple roles can be assigned to a user to create combined access profiles.

SC04 - What happen to the user data entered in ISAAC®?

ISAAC requires minimal user information—typically name/username, email address, and password (the password itself is never accessible). This data is only visible to users with rights to access the Users & Roles management section. No other personal data is collected.

SC05 - What happens to our data if we do decide to stop using ISAAC®?

ISAAC Platform is an on-premise solution owned by the user. The data stored into ISAAC remains in the system installed on-premise, hence also owned by the user.

SC06 - What are ISAAC® policies regarding data retention and deletion?

User's data (typically name/username, email address, and password, see SC04) remains in ISAAC until the user is deleted. Media files and documents uploaded into ISAAC are also kept until they are deleted. Logs however can have a retention policy defined either in quantity or period, logs outside the set quantity limit or period are automatically deleted.

Certifications & Risks Analysis

SD01 - Does ISAAC® have a certification such as SOC2, ISO27001 or CSA STAR LEVEL 1?

Not currently. The current market does not require specific certifications. However, if customer or market demand arises, the ISAAC team will evaluate the requirements and feasibility of obtaining such certifications.

SD02 - Does ISAAC® conduct Threat Modeling and Risk Assessment?

Not currently. However, our development team makes as much effort as possible to follow “shift-left” security principles, integrating security considerations early in the design and implementation stages rather than as an afterthought.

SD03 - Does ISAAC® perform penetration tests?

Not currently. However, our development team makes as much effort as possible to follow “shift-left” security principles, integrating security considerations early in the design and implementation stages rather than as an afterthought.

Security Breaches & Patches

SE01 - Does ISAAC® receives regular security patches?

ISAAC runs on top of a Linux-based system. Starting with ISAAC 2.5 on StageOS, updates may include security patches. There are no scheduled patch releases; patches are provided as needed.

SE02 - What happens if a security issue is discovered in ISAAC®?

If a security vulnerability is identified, the ISAAC product team makes every reasonable effort to deliver a fix as quickly as possible. The time between discovery and patch availability depends on the nature and severity of the issue.

SE03 - Does ISAAC® have a incident response plan?

While ISAAC does not have a formal incident response plan, any security breach reported to our support team will be propagated to ISAAC product team which will make every reasonable effort to deliver a fix as quickly as possible. The time between discovery and patch availability depends on the nature and severity of the breach.

Product Development Practices

SF01 - What measures are in place to ensure that our codebase is resilient against common vulnerabilities?

The development team follows secure coding practices and “shift-left” security principles. External libraries are carefully selected for their reliability and popularity. Dependencies are updated regularly to ensure up-to-date versions are used whenever possible. Additionally, the codebase undergoes nightly static analysis (SAST), and results are

reviewed throughout the development lifecycle to address any medium or high-severity findings.

SF02 - How do we integrate security best practices into our code development process?

In addition to nightly SAST scans (and other practices described above), the development team conducts code reviews and pair programming sessions to detect potential vulnerabilities early.

SF03 - How does the organization ensure new team members are equipped with the necessary knowledge and skills to write secure code?

New developers are introduced to ISAAC's security practices during onboarding and ramp-up. Team members also participate in security training whenever possible.

SF04 - How do we stay updated on the latest security threats and best practices in secure coding?

There is no formal continuous-learning program at this time, but the team stays informed through regular development practices and the security measures mentioned above.

SF05 - Are we over-reliant on security tooling (SonarQube - SAST)?

No. While SAST tools like SonarQube are used, they are only one part of ISAAC's overall security approach. Secure coding practices and peer reviews complement automated tooling.

SF06 - Is the supply chain for ISAAC verified against possible attacks?

Not on a regular basis. However, external dependencies are carefully selected to ensure they are well-established and widely used. Dependencies are updated regularly to minimize supply chain risks.