heylogin

ISMS Integration Guide

Guidance and templates for integrating heylogin into your organization's Information Security Management System

heylogin GmbH

August 11, 2025, Version: v1.0

Contents

1 Introduction

1.1 Purpose of this document

This guide helps organizations that use heylogin to integrate it into their own Information Security Management System (ISMS). It provides factual summaries of heylogin's security properties alongside ready-to-adapt template text for common ISMS policy documents.

Whether your ISMS is based on ISO/IEC 27001, TISAX, or a comparable framework, you will need to document the use of a password management solution across several policy areas. This guide consolidates the information you need in one place and provides template language you can tailor to your organization.

1.2 How to use this guide

Each section covers one ISMS policy area that is affected by the implementation and use of heylogin. Sections are structured as follows:

- **Context** explains why the policy area is relevant and which ISO 27001 controls apply.
- **What heylogin provides** summarizes the relevant facts, drawn from heylogin's advices, published whitepapers and ISMS documentation.
- **Template text** (shown with a line on the left side) offers language you can copy into your own policy documents and adapt. Placeholders are marked as `[YOUR ...]` and must be replaced with your organization's specifics. Please be aware of generalized language. Certain terms may vary for your organization.

1.3 About heylogin's security posture

heylogin GmbH operates an ISMS that is **ISO/IEC 27001:2022 certified** by TÜV Rheinland (test mark number 9000032416). The certification scope covers the development, operation, and marketing of the heylogin password management solution.

Key security properties of the heylogin service:

- **End-to-end encryption** of all customer content (passwords, credentials, metadata). The heylogin server acts only as a synchronization relay for encrypted data and has no technical means to access content data (zero-knowledge architecture).

- **Hardware-backed two-factor security by design.** Decryption requires both the user's device (possession factor) and biometric or PIN authentication (knowledge/biometrical factor). No master password is used.
- **Data sovereignty.** All production infrastructure and backups are located in Germany, operated by ISO 27001-certified data center providers.
- **External privacy review.** The data protection classification has been reviewed by an independent external data protection officer (Projekt 29 GmbH & Co. KG), confirming suitability for use in highly regulated environments.

For full details, refer to:

- heylogin Security Whitepaper: current version in our Trust Center
- heylogin Compliance Whitepaper: current version in our Trust Center
- ISO 27001 certificate: current version in our Trust Center

2 Supplier Security Assessment

2.1 Context

Any ISMS requires the evaluation and ongoing monitoring of suppliers that process or store information on behalf of the organization. As your password management provider, heylogin is a supplier that handles highly sensitive data (authentication credentials) and must be assessed accordingly.

Relevant ISO 27001:2022 Annex A controls: A.5.19 (Information security in supplier relationships), A.5.20 (Addressing information security within supplier agreements), A.5.21 (Managing information security in the ICT supply chain), A.5.22 (Monitoring, review and change management of supplier services)

2.2 What heylogin provides

- **Supplier:** heylogin GmbH, Sophienstraße 40, 38118 Braunschweig, Germany
- **Service:** Cloud-based enterprise password management
- **Certification:** ISO/IEC 27001:2022
- **Data processing location:** Germany (Nürnberg, Falkenstein, Frankfurt)
- **Data center providers:** Hetzner Online GmbH, IONOS SE (both ISO 27001 certified)
- **Sub-processor list:** Available at heylogin.com/en/dpa

- **DPA:** Available at heylogin.com/en/dpa; bilateral signing via Yousign on request
- **Architecture:** Zero-knowledge, end-to-end encrypted; provider cannot access content data
- **Vulnerability disclosure:** Public VDP at heylogin.com/security; security@heylogin.com

2.3 Template: Supplier register entry

> - **Supplier:** heylogin GmbH
> - **Service:** Enterprise password management (cloud-based)
> - **Data classification of processed data:** Classified / Highly sensitive (authentication credentials)
> - **Contractual basis:** `[YOUR reference to subscription agreement]`
> - **DPA:** Signed on `[DATE]`, version `[VERSION]`
> - **Certification:** ISO/IEC 27001:2022
> - **Data processing location:** Germany
> - **Sub-processors:** Available at heylogin.com/en/dpa; no non-European processors
> - **Review schedule:** `[YOUR review cycle, e.g. annually]`
> - **Risk owner:** `[NAME / ROLE]`

2.4 Template: Supplier risk assessment

> **Disruption risk:** Low.
>
> heylogin GmbH holds ISO 27001:2022 certification. The service architecture includes redundancy across geographically separated data centers in Germany, with a demonstrated Recovery Time Actual of less than 2 hours and a Recovery Point Objective of 60 minutes. The client applications maintain a local cache, allowing continued use of credentials during a service outage.
>
> **Disruption consequence:** `[Evaluate based on your organization's dependency. Consider: How many systems are accessed via heylogin? Is there an export/offline fallback?]`
>
> **Data confidentiality risk:** Low.
>
> The zero-knowledge architecture ensures that heylogin GmbH has no technical means to access stored credentials. All content data is end-to-end encrypted on the user's device before being transmitted to the server. Even in the event of a full infrastructure breach at the

> provider, the encrypted vaults cannot be decrypted without access to the user's hardware security chip.
>
> **Overall supplier risk:** `[Calculate per your methodology]`
>
> **Accepted by:** `[NAME / ROLE]` on `[DATE]`

3 Access Control and Password Management Policy

3.1 Context

The introduction of a centralized password management solution is one of the most impactful changes to an organization's access control posture. Your access control policy should document which system is used, how credentials are managed, and what rules apply to employees.

Relevant ISO 27001:2022 Annex A controls: A.5.15 (Access control), A.5.16 (Identity management), A.5.17 (Authentication information), A.8.02 (Privileged access rights), A.8.05 (Secure authentication)

3.2 What heylogin provides

- **Centralized credential storage** with end-to-end encryption. Credentials are organized into personal vaults and shared team vaults.
- **Automatic strong password generation** (default 16 characters, configurable) - The default password policy follows recommendations from the CIS Password Policy Guide and NIST SP 800-63B.
- **Two-factor security by design.** Every credential access requires the user's authenticated device (smartphone with biometrics/PIN, or FIDO2 security key). This is not an optional add-on; it is the fundamental architecture.
- **Team-based sharing.** Administrators can assign credentials to teams and control who has access. It is possible to share access to accounts without revealing the underlying password.
- **Audit log.** Significant events concerning the use and management of logins are recorded.
- **Admin visibility without content access.** Administrators can see which logins exist and whether they comply with security guidelines (e.g., password strength), but cannot technically view passwords in plain text.
- **Automatic locking.** Browser extension locks automatically at the end of the working day.

- **Private vault separation.** Employees may use a private vault for private credentials. Administrators have no technical access to or visibility into private vaults, including metadata.

3.3 Template: Password management policy

> **Password Management**
>
> `[YOUR ORGANIZATION]` uses **heylogin** as its enterprise password management system. All employees are required to use heylogin for the management of work-related credentials. This is not just a recommendation.
>
> **Scope.** This policy applies to all credentials used to access systems, applications, and services on behalf of `[YOUR ORGANIZATION]`.
>
> **General rules:**
>
> 1. All work-related credentials (usernames, passwords, TOTP secrets, and related data) shall be stored exclusively in heylogin.
> 2. Credentials must not be stored in other password managers, browser built-in storage, text files, spreadsheets, or similar.
> 3. Credentials must not be transmitted in clear text (e.g., via email or chat). Where credential sharing is necessary, it shall be done through heylogin teams or externally with the heylogin sharing feature.
>
> **Password generation:**
>
> 1. For all new accounts and during credential rotation, passwords shall be generated using heylogin's built-in generator with a default length of 16 characters.
> 2. Manually chosen passwords are only acceptable where technical constraints prevent the use of generated passwords. In such cases, the password must be at least `[YOUR POLICY]` characters long.
>
> **Authentication and unlocking:**
>
> 1. heylogin may be unlocked using the following methods:
>
> a. The employee's smartphone, secured with biometrics or a non-trivial PIN. This is the default method.

b. A FIDO2 security key with user verification `[BIOMETRICS OR NON-TRIVIAL PIN]` configured.

2. If a smartphone or security key used to unlock heylogin is lost or stolen, this must be reported **immediately** to `[YOUR IT CONTACT / ROLE]`. Access will be revoked without delay.

Shared credentials:

1. Credentials used by multiple employees shall be organized in heylogin teams. Each team shall have a designated team administrator responsible for managing membership *(e.g. Team-Administrator, Team-Leader etc.)*
2. Access to heylogin teams shall be granted on a need-to-use basis and reviewed `[YOUR CYCLE, e.g., quarterly]`.

Exceptions:

1. Any exception to this policy must be approved by `[ROLE, e.g., CISO or IT Manager]` and documented.

3.4 Template: Multi-factor authentication policy

Multi-Factor Authentication

`[YOUR ORGANIZATION]` requires multi-factor authentication (MFA) for access to all work-related systems and applications, wherever technically feasible.

Implementation: The primary mechanism for MFA is the heylogin password manager, which enforces two-factor authentication by design for every credential it manages. heylogin's architecture binds credential decryption to a hardware security chip on the user's smartphone (TPM chip) or security key (possession factor), which must be unlocked via biometrics or PIN (inherence/knowledge factor). This ensures that every login performed through heylogin is inherently two-factor authenticated, without requiring per-service MFA configuration.

For systems that support additional authentication factors (e.g., TOTP, FIDO2 WebAuthn) independently of the password manager, these shall be enabled where the system's data classification warrants it. TOTP secrets shall be stored and automated within heylogin where supported.

> **Coverage:** All systems and applications for which credentials are managed in heylogin are covered by heylogin's built-in two-factor mechanism. A separate inventory of MFA-enabled services is therefore not required for heylogin-managed credentials.

4 Use of Cryptography

4.1 Context

Organizations that store or process sensitive authentication data must document their approach to cryptography. Because heylogin manages the cryptographic protection of credentials on behalf of the user, this should be reflected in your cryptography policy.

Relevant ISO 27001:2022 Annex A controls: A.8.24 (Use of cryptography)

4.2 What heylogin provides

- **End-to-end encryption:** Symmetric encryption and integrity of vault content with XSalsa20 + Poly1305
- **Asymmetric encryption:** Key exchange and vault key management with Curve25519
- **Transport encryption:** Encryption of data in transit with TLS 1.3 / 1.2 (HSTS enforced)
- **Backup encryption:** Encryption of server-side backups with ChaCha20 + Poly1305
- **Key protection:** Protection of cryptographic seed material in Hardware Secure Element (Secure Enclave / TPM)

The cryptographic seed is generated in the security chip of the user's device and never leaves it unencrypted. This provides protection against offline brute-force attacks that are possible with master-password-based architectures.

4.3 Template: Cryptography policy addition

> **Cryptographic protection of authentication credentials**
>
> Authentication credentials managed by the organization's password management system (heylogin) are protected by end-to-end encryption. The encryption is performed client-side on the user's device before any data is transmitted to the service provider. The following cryptographic measures are in effect:

- **Confidentiality:** XSalsa20 stream cipher with Poly1305 message authentication (AEAD construction)
- **Key exchange:** Curve25519 elliptic curve Diffie-Hellman
- **Transport:** TLS 1.3 or 1.2 with HSTS enforcement
- **Key material protection:** Cryptographic seed generated and stored in the device's hardware security chip (Secure Enclave on iOS, StrongBox/TEE on Android, or FIDO2 authenticator). Key material never exists in unencrypted form outside the security chip.

The provider (heylogin GmbH) has no technical means to access the encryption keys or the unencrypted content data. This zero-knowledge architecture ensures that a breach of the provider's infrastructure does not compromise the confidentiality of stored credentials.

The cryptographic algorithms used are consistent with current best practices. heylogin GmbH documents its cryptographic architecture in a publicly available Security Whitepaper.

5 Personnel Management: Onboarding and Offboarding

5.1 Context

The introduction of a password manager affects employee onboarding and offboarding procedures. These must be documented to ensure consistent provisioning and *critically* complete deprovisioning of access when an employee leaves.

Relevant ISO 27001:2022 Annex A controls: A.6.01 (Screening), A.6.02 (Terms and conditions of employment), A.6.05 (Responsibilities after termination or change of employment), A.5.18 (Access rights)

5.2 What heylogin provides

- **Onboarding:** Administrators invite users to the organization via email. Users set up heylogin by pairing their smartphone (or FIDO2 key) with the browser extension via QR code. Team memberships and roles are assigned by team administrators.
- **Offboarding:** Administrators can disable a user's account, which immediately prevents further synchronization and access. Credentials in shared teams remain available to

other team members. If the departing employee had personal credentials for organization-owned accounts, these should be rotated.

- **Account recovery:** Organization administrators can initiate account recovery for users who lose their device, without gaining access to the user's vault content.

5.3 Template: Onboarding checklist additions

> **Password management setup (heylogin):**
>
> - ☐ Employee has been invited to the heylogin organization
> - ☐ Employee has installed the heylogin app on their smartphone and the browser extension
> - ☐ Employee has completed the pairing process (QR code scan)
> - ☐ Employee has been assigned to the relevant heylogin teams and roles
> - ☐ Employee has been informed of the password management policy
> - ☐ Employee has confirmed that no work credentials will be stored outside of heylogin
> - ☐ Private credentials are stored separately from the organization using the private account

5.4 Template: Offboarding checklist additions

> **Password management deprovisioning (heylogin):**
>
> - ☐ Employee's heylogin account has been disabled by an organization administrator
> - ☐ Employee has been removed from all heylogin teams
> - ☐ Credentials for shared accounts that the employee had access to have been assessed for rotation necessity
> - ☐ Personal credentials for organization-owned accounts have been identified and rotated where necessary
> - ☐ Employee has been informed that the private vault (private, non-organization credentials) remains accessible to them via their private heylogin account

5.5 Template: Device loss procedure

> **Lost or stolen device (smartphone or security key used with heylogin):**
>
> 1. Employee reports the loss immediately to `[YOUR IT CONTACT / ROLE]`.

2. A heylogin administrator revokes access for the lost device without delay.
3. If the lost device was the employee's only authenticator, account recovery is initiated by an organization administrator.
4. The employee sets up heylogin on a replacement device.
5. Evaluate whether credential rotation is warranted based on the circumstances of the loss (e.g., device was unlocked when stolen).

6 Security Incident Management

6.1 Context

Your ISMS must define how security incidents at suppliers are detected, communicated, and handled within your organization. This section covers how heylogin communicates incidents and how to integrate this into your own incident management procedure.

Relevant ISO 27001:2022 Annex A controls: A.5.24 (Information security incident management planning and preparation), A.5.25 (Assessment and decision on information security events), A.5.26 (Response to information security incidents)

6.2 What heylogin provides

- **Status page:** Service status and incidents are publicly communicated at status.heylogin.com.
- **Incident classification:** heylogin classifies incidents by severity (0 = small/no impact, 1 = moderate availability or small confidentiality/integrity impact, 2 = significant availability or moderate confidentiality/integrity impact).
- **Incident response:** The heylogin operations team investigates incidents, determines root cause, controls impact, and applies corrective action. Incident reports are documented internally.
- **Data breach notification:** In the event of a personal data breach, heylogin GmbH notifies affected customers within 24 hours of becoming aware of the breach, to enable compliance with the 72-hour reporting deadline under Art. 33 GDPR.
- **24/7 monitoring:** The production environment is monitored continuously (every minute). An employee is always on standby for incident response.

- **Vulnerability disclosure:** Third-party security researchers can report vulnerabilities to security@heylogin.com under a public Vulnerability Disclosure Policy (heylogin.com/security).

6.3 Template: Supplier incident handling procedure

> **Handling of security incidents at the password management provider**
>
> **Monitoring:** [RESPONSIBLE ROLE] shall periodically check the heylogin service status page at status.heylogin.com. [Consider: subscribing to status page notifications if available.]
>
> **Assessment:** If heylogin communicates a security incident, [RESPONSIBLE ROLE] shall evaluate its relevance and potential impact on [YOUR ORGANIZATION]:
>
> - **Availability incident:** Determine whether business operations are affected. Note that heylogin client applications cache credentials locally, so short outages may not affect the ability of employees to log in to systems.
> - **Confidentiality or integrity incident:** Evaluate whether the organization's credentials may be affected. Given the zero-knowledge, end-to-end encrypted architecture, a server-side breach at heylogin does not expose credential content. If the incident involves client-side vulnerabilities or a compromise of the encryption architecture, treat this as a high-severity event and initiate credential rotation.
>
> **Escalation:** If the assessment indicates a material impact on the organization's information security, a security event shall be filed per the organization's standard incident management procedure ([REFERENCE]).
>
> **Data breach:** If heylogin GmbH notifies the organization of a personal data breach, [RESPONSIBLE ROLE] shall immediately evaluate whether a report to the supervisory authority is required under Art. 33 GDPR and notify affected data subjects if required under Art. 34 GDPR.

7 Business Continuity

7.1 Context

The availability of your password manager directly affects employees' ability to access business systems. Your Business Impact Analysis and continuity plans should account for the scenario of a heylogin service disruption.

Relevant ISO 27001:2022 Annex A controls: A.5.29 (Information security during disruption), A.5.30 (ICT readiness for business continuity)

7.2 What heylogin provides

- **Contractual availability:** 99% annual average
- **Demonstrated availability:** ~99.95% annual average
- **Recovery Time Objective (RTO):** 8 hours (defined); < 2 hours (measured)
- **Recovery Point Objective (RPO):** 60 minutes (hourly encrypted backups)
- **Standby server:** Geographically separated data center (Falkenstein); switchover within 30 minutes
- **Client-side caching:** Credentials are cached locally in the browser extension and mobile app
- **Data replication:** Continuous replication to standby server via VPN tunnel

The local caching capability is particularly relevant for business continuity: even during a complete heylogin server outage, employees can continue to access credentials that have been previously synchronized to their devices.

7.3 Template: Business Impact Analysis entry

> - **System:** heylogin (enterprise password management)
> - **Business processes supported:** Authentication to all systems and applications where credentials are managed in heylogin
> - **Impact of unavailability:** `[Assess: e.g., "Employees cannot access new or recently changed credentials. Previously synchronized credentials remain available locally. Impact is moderate for short outages (< 4 hours) and high for extended outages."]`

- **Provider RTO:** < 2 hours (measured), 8 hours (contractual)
- **Provider RPO:** 60 minutes
- **Continuity measures:** heylogin mobile client apps maintain a local credential cache. This mitigates the impact of short service disruptions.

8 Data Protection and GDPR

8.1 Context

The GDPR serves as the foundation for all regulations, especially when it comes to password security. As heylogin processes personal data on behalf of your organization (at minimum, employee email addresses and metadata about credential usage), it must be reflected in your data protection documentation, including the Record of Processing Activities and Data Processing Agreements.

Relevant ISO 27001:2022 Annex A controls: A.5.34 (Privacy and protection of PII)

8.2 What heylogin provides

- **Data Processing Agreement (DPA)** available at heylogin.com/en/dpa; automatically effective on contract signing; bilateral signing available on request.
- **Processing location:** Germany only. No Non-European cloud providers for the core service.
- **Zero-knowledge architecture:** Content data (passwords, credentials) is end-to-end encrypted and inaccessible to heylogin GmbH. The provider processes only encrypted data and limited metadata (e.g., email addresses, organization membership).
- **No trackers.** The heylogin mobile apps are free of advertising or profiling trackers. Crash reporting is pseudonymized, opt-in based, and purpose-bound.
- **Data subject rights:** Users can export their data. Deletion requests are handled organizationally upon request to support.
- **No performance monitoring.** Audit logs are used exclusively for IT security and compliance purposes. Use for performance or behavior monitoring is contractually excluded.
- **Private vault protection.** Administrators have no access to or visibility into employees' private vault data, including metadata.

- **Works council compatibility.** The external privacy review by Projekt 29 GmbH & Co. KG explicitly confirms compatibility with employee data protection and co-determination requirements.

8.3 Template: Record of Processing Activities entry

> - **Processing activity:** Enterprise password management
> - **Purpose:** Secure storage and management of authentication credentials for organizational systems and applications
> - **Legal basis:** Art. 6(1)(f) GDPR (legitimate interest in information security) or Art. 6(1)(b) GDPR (performance of employment contract)
> - **Categories of data subjects:** Employees, contractors
> - **Categories of personal data:** Email address, name, organization membership, encrypted credential data (inaccessible to processor due to E2E encryption)
> - **Recipients:** heylogin GmbH (processor); sub-processors as documented at heylogin.com/en/dpa
> - **Third-country transfers:** None for core service. Optional ancillary services (e.g., billing) secured by adequacy decisions or SCCs where applicable
> - **Retention:** Per contract duration; deletion upon contract termination and request
> - **Technical and organizational measures:** End-to-end encryption (zero-knowledge), ISO 27001-certified provider, data processing in Germany, DPA in place
> - **DPA reference:** `[YOUR reference, e.g., "Signed on DATE, version X"]`
> - **Responsible:** `[NAME / ROLE]`

9 Information Security Awareness and Training

9.1 Context

Organizations must ensure that employees are aware of information security policies and trained in the tools they use. heylogin's design significantly reduces the training burden for password security, but this should be documented explicitly.

Relevant ISO 27001:2022 Annex A controls: A.6.03 (Information security awareness, education and training)

9.2 What heylogin provides

- **No master password training required.** Unlike traditional password managers, heylogin does not use a master password. Employees do not need training on choosing, protecting, or rotating a master password.
- **Security by design.** Two-factor authentication is inherent to the architecture, not an optional configuration. Employees do not need to enable or configure MFA separately.
- **Phishing resistance.** heylogin's autofill is domain-bound and replaces the login process in the browser, reducing the risk of credential entry on phishing sites.
- **Simple user experience.** The "Swipe to Login" interaction model requires minimal training.

9.3 Template: Training plan addition

> **Password management training**
>
> All employees receive an introduction to the organization's password management tool (heylogin) during onboarding. The training covers:
>
> - How to set up and pair heylogin (smartphone / security key + browser extension)
> - How to save, retrieve, and generate credentials
> - How to use heylogin teams for shared credentials
> - The obligation to store all work credentials exclusively in heylogin
> - What to do if a device is lost
>
> Recurring training on password security topics (e.g., master password hygiene, manual MFA setup) is **not required**, as heylogin enforces strong, unique, hardware-protected credentials by design. Awareness training shall instead focus on recognizing social engineering and reporting security events.
>
> **Responsible:** `[ROLE]`
>
> **Frequency:** During onboarding; refresher as part of `[YOUR annual awareness program]`

Appendix A: ISO 27001:2022 Annex A Control Mapping

The following table maps heylogin capabilities to specific controls from ISO/IEC 27001:2022 Annex A (derived from ISO/IEC 27002:2022). This can serve as a reference when completing your Statement of Applicability or assessing control implementation.

Control	Title	heylogin contribution
A.5.15	Access control	Central enforcement of credential policies; team-based access with admin control
A.5.16	Identity management	Visibility into shared identities; approval and revocation of access; audit log
A.5.17	Authentication information	Automatic generation of unique strong passwords; encrypted storage and transmission; no clear-text handling
A.5.19	Information security in supplier relationships	heylogin is ISO 27001:2022 certified; DPA available; sub-processors documented
A.5.23	Information security for use of cloud services	Zero-knowledge architecture; data processing in Germany; client-side encryption
A.5.24–28	Incident management	Public status page; defined incident classification and response; vulnerability disclosure program
A.5.29–30	Business continuity	Local credential caching; RTO < 2h; RPO 60min; geo-redundant infrastructure
A.5.34	Privacy and protection of PII	DPA available; GDPR-compliant; private vault separation; no performance monitoring; external privacy review

Control	Title	heylogin contribution
A.6.03	Awareness, education and training	Reduces training burden (no master password, MFA by design); domain-bound autofill reduces phishing risk
A.6.05	Responsibilities after termination	Account disabling; team removal; credential rotation guidance
A.8.02	Privileged access rights	Privileged credentials managed in heylogin with same protections; admin visibility without content access
A.8.05	Secure authentication	Hardware-backed 2FA by design for all credentials; biometrics/PIN required for every access
A.8.24	Use of cryptography	E2E encryption (XSalsa20+Poly1305, Curve25519); hardware key storage; TLS 1.3/1.2 transport

Appendix B: TISAX (VDA ISA) Control Mapping

For organizations subject to TISAX assessments, the following table maps heylogin capabilities to relevant criteria from the VDA ISA catalog v5.0.

VDA ISA	Criterion	heylogin contribution
3.1.4	Handling of mobile IT devices	heylogin uses smartphones as authenticators; display lock with biometrics/PIN is mandatory
4.1.2	User access to network services, IT systems, and IT applications	2FA via smartphone integrated into the login process for all managed credentials
4.1.3	Secure management of user accounts and login information	Unique personal accounts; E2E encryption prevents provider access; easy employee offboarding; admin control over shared accounts
4.2.1	Assignment and management of access rights	Passwords known only to the user due to E2E encryption; team-based sharing with admin control
5.1.1	Management of cryptographic procedures	XSalsa20+Poly1305 and Curve25519; documented in publicly available Security Whitepaper
5.1.2	Protection of information during transport	End-to-end encryption ensures only sender and recipient can access data; TLS for transport layer

Appendix C: Key References and Contact Points

Resource	Location
Security Whitepaper	heylogin.com/en/trust-center

Resource	Location
Compliance Whitepaper	heylogin.com/en/trust-center
Data Processing Agreement (DPA)	heylogin.com/en/dpa
Privacy policy (product)	heylogin.com/en/privacy
Sub-processor list	heylogin.com/en/dpa
ISO 27001 certificate	heylogin.com/en/trust-center
Service status	status.heylogin.com
Vulnerability disclosure	heylogin.com/security
Security contact	security@heylogin.com
Legal contact	legal@heylogin.com
General support	support@heylogin.com