

Security Schedule

Contractually committed security controls for the Coldbyte service

Provider: Coldbyte AS, org. no. NO 938312133 «Coldbyte»

Customer: End customers legal entity as named in Order Form

Part of: The Coldbyte product terms (Terms of Service, DPA, SLA)

Control reference: ISO/IEC 27002:2022 control numbers are used as a common vocabulary only — see Section 4

Version / date: v1.00 — 31 August 2026

1. Purpose and scope

This Schedule states the security controls Coldbyte commits to maintain for the Service, as contractual obligations. It contains only controls that are in place today; it is deliberately short. This Schedule does not expand Coldbyte's warranties or liability beyond the Terms of Service, and it makes no statement about compliance with any law or regulation. Sector-specific cooperation duties (such as supervisory access, reporting support and exit periods) are governed by the applicable regulatory addendum, not by this Schedule.

Order of precedence. In the event of any conflict or inconsistency between the documents comprising the Agreement, this Schedule ranks below the Order Form, any Regulatory Addendum (e.g. a DORA Addendum, for the matters it governs), the Data Processing Agreement and the Terms of Service— this Schedule ranks lowest among the Agreement documents.

2. Committed controls

Coldbyte maintains the following for the duration of the Customer's subscription. References in the right-hand column are to ISO/IEC 27002:2022 control numbers.

Commitment	In practice	ISO/IEC 27002
Deployment isolation and data locality	The Service runs as an isolated, per-customer instance inside the Customer's own Azure subscription and Microsoft 365 tenant. Service data is stored and processed only there; Coldbyte keeps no copy in its own systems. The technical health signal to Coldbyte carries no personal data (anonymous aggregate user counts only, for billing).	5.14, 8.22

Commitment	In practice	ISO/IEC 27002
Least-privilege access	The continuously running component holds read-only permissions and no content-data permissions (no mail, files, sites or chat access). Write capability is isolated to a separate identity on an on-demand component with no inbound network. Automated tests prevent permission creep.	5.15, 8.2, 8.3
Provider personnel access	Coldbyte's own access to the Customer environment is limited to authorised personnel and used only for provisioning, updates and agreed support. Provider accounts use phishing-resistant multi-factor authentication; provider actions are logged and visible to the Customer; access is revoked on personnel change and reviewed periodically.	5.18, 6.5, 8.5
Network exposure minimisation	Administrative access is restricted to defined source addresses with no password authentication; network security groups limit exposure; service components are hardened and integrity-verified at installation.	8.20, 8.21
Customer-approved change control	No change is made in the Customer's tenant without the Customer's prior approval in the agreed channel: approvals are cryptographically signed, time-bound and bound to the exact code version; one rejection stops the change; employee offboarding requires two independent approvers; person-directed actions select the target from a validated directory lookup, not free text. All requests, votes, executions and rollbacks are written to an append-only event log available to the Customer.	8.32, 8.15
Cryptography and secrets handling	TLS 1.2+ in transit; private storage; key vault with purge protection; encryption-at-host on the service VM; no client secrets (federated identity only); secret rotation on an enforced schedule.	8.24, 5.17
Data minimisation and automated deletion	Collection uses explicit field allowlists on every data source, excluding the most personal-data-dense fields. Bounded retention with automated deletion: raw data 30 days; behavioural baselines 180 days; posture and remediation artifacts 90 days; configuration-drift timeline 90 days; the approval/attestation log 400 days as the accountability record.	8.10, 5.33
Logging and monitoring	Per-deployment logging and monitoring; daily configuration snapshot with drift	8.15, 8.16

Commitment	In practice	ISO/IEC 27002
	detection (fail-safe: a failed read is never reported as a change); a risk-ranked application-identity inventory with an attestation trail; the Customer retains full visibility of resources and logs in its own subscription.	
Vulnerability handling and security updates	Published vulnerability-handling policy with fix targets (critical 72 h, high 7 days, medium 30 days, low 90 days, measured to deployed in every affected environment); a public reporting route; security updates free of charge through the versioned release path; release channels (Stable/Latest) with audited promotion, so the Customer can receive updates only after promotion.	8.8
Secure development and supply chain	CI with automated tests, full-history secret scanning and dependency audit; branch protection and signed commits; pinned, integrity-verified dependencies; a maintained SBOM/component inventory.	8.25, 8.28, 8.29, 5.21
Resilience and backup	Documented business-continuity/disaster-recovery procedure with a tested restore on a quarterly cadence; nightly backup of the assets that cannot be rebuilt from code; the environment is reproducible from code.	5.29, 5.30, 8.13
Recovery objectives	Recovery time and recovery point objectives for the Service are stated in the SLA; the tested restore procedure is exercised against them.	5.30
Incident handling	Incidents affecting the Service are notified to the Customer without undue delay under a documented runbook with a named owner, with status updates until resolution. Timeframes and personal-data incidents follow the SLA and the DPA.	5.24, 5.25, 5.26
Organisation and people	A lightweight information-security management practice with a risk register and an enforced management-review cadence; personnel bound by confidentiality; access revoked on personnel change.	5.1, 6.2, 6.5, 6.6
Physical security	Inherited from Microsoft Azure in the Customer's own subscription; Coldbyte operates no data centres.	7 (inherited)
AI component	The embedded assistant never executes tenant changes; it runs on an AI resource in the Customer's own subscription and region; Customer data is not used for model	8.26, 5.23

Commitment	In practice	ISO/IEC 27002
	training and is not shared with Coldbyte; it has no outbound channel through which content could be exfiltrated.	
Data export and erasure functions	The Service provides export and erasure of an individual's records in the Service's data stores as product functions, executed on the Customer's instruction and logged.	8.10
Termination and offboarding	On termination, the Service instance (VM, storage incl. backups, key vault, AI resources) is deleted from the Customer's subscription per the documented offboarding procedure — or retained by the Customer, since it lives in the Customer's own subscription. Coldbyte's access is revoked and confirmed in writing.	5.11, 8.10

3. Verification

On request, Coldbyte makes available the documentation that evidences the controls above: the Trust Center overview, the CAIQ self-assessment (CSA Cloud Controls Matrix), an ISMS summary, the SBOM/component inventory, the vulnerability-handling policy and a continuity/restore summary. Because the Service runs in the Customer's own subscription, the Customer additionally has direct, continuous visibility of resources, configuration and logs. Audit rights and cadence follow the Terms of Service.

4. Framework references are vocabulary, not conformity claims

ISO/IEC 27002:2022 (and the CSA CCM in the CAIQ) are used in this Schedule as a recognised control vocabulary so the Customer can map Coldbyte's controls into its own frameworks. These references are not a claim of certification or conformity: Coldbyte holds no third-party certification and does not commit to obtaining one, and this Schedule is not a representation that the Service or the Customer's use of it satisfies any legal or regulatory requirement. Any third-party reports or certifications are provided only where and when obtained.

5. Changes

Coldbyte may improve or replace individual controls, but will not materially reduce the overall level of protection described in Section 2 during the Customer's subscription term. Changes that affect the Service's permissions, data categories, retention or data flows follow the change-control process in the DPA.