

Controls and checks for your security review

Voice translation and virtual office | English customer edition

This edition preserves the earlier 114 questions and adds 29 questions informed by recent data-leakage incidents. Answers on transport, authentication and monitoring reflect the scope currently verified. The question count describes review coverage, not a security score.

Classification	How to read it
Verified	Confirmed in public specifications or policy. This classification does not guarantee deployment in every environment or effectiveness against every attack.
Conditional	Conditions depend on feature, plan, settings, contract or the implementation/test environment. Read the scope of each answer.
Confirm individually	This document alone cannot establish implementation. Confirm required configuration, implementation records and contract terms individually.

Carried forward means the answer comes from the September 8, 2026 edition. Updated and Added identify items revised for this edition. Check the applicable contract and current settings during adoption, including for carried-forward answers.

The October 22 edition retains all 143 questions and adds verified dependency-review and update examples. Each question retains its own review date and response classification.

For security reasons, internal configurations, detection rules and thresholds are not public. This document presents representative controls and checks, not an exhaustive inventory. Contact support for detailed review materials.

Products, features and scope

This document covers VoicePing voice translation and virtual office services. Assess the products/features you will use. Confirm dedicated/on-premises configurations, feature limits and actual settings under the plan and contract.

Product / feature	Use and review scope
Live voice translation	Transcribe/translate in-person or online audio. Check the audio source and recipients of captions/translated speech.
Event translation	Deliver captions/translated speech to attendees. Check listener URLs/QR codes, participation passwords and event-use conditions.
Meeting Bot	A Bot joins supported Zoom, Google Meet or Microsoft Teams meetings. Check admission, optional calendar connections and record sharing.
File transcription/translation	Generate transcripts, translations, subtitles or dubbing from uploaded audio/video. Check handling of both inputs and outputs.
Meeting logs and AI summaries	Review/share conversation records and file-processing results. Check retention, viewers, exports and API/MCP access.
Virtual office	Collaborate through presence, floors/rooms, calls, translation and screen sharing. Check member/guest permissions and sharing scope.
Time tracking	Record projects, work notes and time. Check separate settings for optional desktop/webcam images and input activity.
Mobile offline translation	Transcribe/translate on-device after obtaining models. Check local records, deletion and export separately from cloud features.

Before adoption, check domestic/overseas processing, training use versus external transmission, authentication exceptions and retention/deletion by data type. For presence history and optional image capture, also check explanations to affected people and capture/viewer settings.

Verified update and deployment examples

Update and deployment records and the running MySQL version were checked on October 22, 2026. These are selected examples; affected systems and internal configuration remain private. Versions identify the verified deployment, not a claim that each is always the newest release.

Updated software	Verification
MySQL 8.4.11	Confirmed the completed upgrade and running version through a read-only database connection.
Samlify 2.15.1	Tested signature verification and rejection of reused authentication responses.
Nodemailer 10.1.7	Tested recipient-address parsing after the update.
pgx 5.11.0	Tested malformed-input rejection, database connections and queries.
lib0 0.2.119	Tested that data reads stay within the supplied input bounds.

Advisory scans, publisher/artifact review and behavior tests provide different evidence. Findings limited to unused code, compatibility patches and tool-use restrictions are tracked separately. Official sources appear in the references.

Governance and certification

GOV-01 Are the provider and services identified?

Verified

VoicePing Inc. provides voice translation and virtual office services, including transcription, meeting summaries, file processing, collaboration and time tracking. Identify the products, features and plan in the contract.

Carried forward 2026-09-08 | Earlier PDF and related public guides

GOV-02 Does the provider hold an information security certification?

Verified

Official materials state ISO/IEC 27001:2022 certification, BSI certificate IS 820960. Check the latest certificate for its scope and current validity.

Updated 2026-10-21 | Current public guides and verification records

GOV-03 Can certification scope and validity be verified?

Confirm individually

Confirm the scope and current validity individually using the latest documents.

Carried forward 2026-09-08 | Earlier PDF and related public guides

GOV-04 Can third-party assessments be reviewed?

Confirm individually

Contact us about completed third-party assessments and the materials available.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Governance and certification (continued)

GOV-05 Are SOC 2 reports, PrivacyMark or other materials available?

Confirm individually

Confirm individually whether these reports or certifications are held or available and request current materials.

Carried forward 2026-09-08 | Earlier PDF and related public guides

GOV-06 Are security policy and management responsibilities defined?

Confirm individually

Contact us for details of security policy and management responsibilities.

Carried forward 2026-09-08 | Earlier PDF and related public guides

GOV-07 Are risk assessment and asset management performed?

Confirm individually

Define the required scope and confirm risk assessment and asset management individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

GOV-08 How is employee security awareness managed?

Confirm individually

Contact us for details of employee-related security management.

Carried forward 2026-09-08 | Earlier PDF and related public guides

GOV-09 Can the security management assessment framework be reviewed?

Confirm individually

Contact us about the assessment framework and how it can be verified.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Governance and certification (continued)

GOV-10 Are employees and contractors bound by confidentiality obligations?

Verified

Published policies and contracts set confidentiality obligations for people handling personal data and data-protection obligations for processors. Customer-specific NDAs depend on the plan and contract.

Carried forward 2026-09-08 | Earlier PDF and related public guides

GOV-11 Are custom questionnaires, evidence requests and customer audits supported?

Conditional

Security reviews, documentation, NDAs and customer audits are coordinated according to the plan and contract. Contact us with additional questions and required materials.

Carried forward 2026-09-08 | Earlier PDF and related public guides

GOV-12 Is compliance with every law and standard guaranteed?

Confirm individually

We publish a privacy policy. Assess industry standards, GDPR, healthcare and financial requirements individually for the region and data involved. Certification alone does not establish compliance with all laws or industry standards.

Carried forward 2026-09-08 | Earlier PDF and related public guides

GOV-13 Can the scope of security controls be confirmed?

Confirm individually

Contact us about control scope and detailed supporting materials.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Governance and certification (continued)

GOV-14 Can supplier and processor management be reviewed?

Confirm individually

Contact us for details of supplier and processor selection and management.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Data protection and privacy

DAT-01 What data is processed?

Verified

Data includes accounts, audio/video, transcripts, translations, summaries, shared content, IP addresses and device information. Virtual office features also handle presence and history, work notes and time, and optional images and input activity. Collection depends on features and settings. See USE-14 for optional capture.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-02 Are purposes and responsibilities for customer data clear?

Verified

Customer content is processed under customer instructions. Accounts, billing, support and security operations have separately defined purposes. See the privacy policy for maintenance, legal compliance and other details.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-03 Which cloud infrastructure and primary storage locations are used?

Verified

Primary infrastructure uses AWS and GCP in Tokyo, Japan, with Cloudflare for delivery. Distinguish the cloud provider's responsibilities from VoicePing's. See DAT-04 for overseas processing and OPS-04 for backup scope and locations.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-04 Is data processed or subcontracted overseas?

Conditional

CDN, AI and notification integrations involve overseas processing. The data-handling table lists purposes, destinations and data by service. Japan-only processing or a ban on overseas access requires individual agreement.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Data protection and privacy (continued)

DAT-05 Is data encrypted in transit?

Verified

Public web/API traffic uses HTTPS, WebSocket uses WSS, and WebRTC audio/video uses mechanisms such as DTLS-SRTP. Not all traffic uses one TLS version. Cloud translation and transcription process content on servers and are distinct from E2EE that prevents servers reading content.

Updated 2026-10-21 | Current public guides and verification records

DAT-06 Is stored data encrypted?

Verified

The public DPA specifies AES-256 for databases and file storage; the privacy policy describes AES-256 for audio. Verify configuration evidence for particular stores when needed. See INF-12 for key management and BYOK/CMK requirements.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-07 Is customer data separated between organizations?

Verified

The design separates organizations' data logically in the database. This does not guarantee a dedicated database or physical separation as a standard feature.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-08 How long is audio retained?

Conditional

Published retention is up to three months depending on plan and settings, followed by deletion. Do not apply audio retention to every data type. Discuss longer retention in advance and export required data before expiry.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Data protection and privacy (continued)

DAT-09 How long are meeting records and summaries retained?

Confirm individually

Meeting documentation states up to one year for paid self-service plans and contract-specific Enterprise retention. The privacy policy states the contract period. Confirm the applicable contract and actual settings; this sheet does not guarantee one year or unlimited retention universally.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-10 How long are video recordings retained?

Conditional

Pricing/storage guidance states deletion of recordings after one month. Distinguish meeting recordings from uploaded video, generated subtitles/dubbing and time-tracking images; confirm retention for each feature.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-11 How are log retention and identifier deletion handled?

Confirm individually

Pricing guidance states 18 months for event, online and work logs on paid plans; the privacy policy states the minimum necessary period for access logs. Confirm actual retention/deletion scope, including images. Personal identifiers are deleted or anonymized within 30 days of a valid deletion request under the published policy.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-12 Is all data automatically erased on cancellation?

Conditional

Published policy retains data after contract termination until an authorized deletion action or request, with deletion within 30 days of a valid request, except legally required retention. Cancellation and deletion requests are separate. See USE-09 for exit tasks and DAT-13 for backups.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Data protection and privacy (continued)

DAT-13 Can complete deletion, including backups, be verified?

Confirm individually

Confirm backup retention, replicas, deletion propagation, legal holds and deletion-certificate scope individually. Deletion through the UI does not guarantee immediate physical erasure of every copy.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-14 Can users request disclosure, correction or deletion?

Verified

We publish contact channels and procedures for identity-verified requests for disclosure, correction, suspension of use and erasure. Requests are handled after checking authority, scope and legal exceptions.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-15 Are media and equipment disposal and reuse controlled?

Confirm individually

Define the relevant scope and confirm disposal and reuse controls individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

DAT-16 Are external document-sharing rules defined?

Confirm individually

Contact us for details of controls on sharing company documents externally.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Authentication and permissions

IAM-01 Are users managed with individual accounts?

Verified

The general model is one account per user. Subtitle listeners using URLs/QR codes and virtual-office guests using the guest web app have different participation methods. See USE-04.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-02 Is two-step authentication supported?

Conditional

Paid plans can require email-token two-step authentication for all workspace users. Google and Apple sign-in have an exception that does not require email verification. Check authentication strength on exception routes and its interaction with SSO during adoption.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-03 Is SSO available?

Conditional

We publish Enterprise SSO setup guides for Microsoft Entra ID and HENNGE One. Confirm the plan, IdP configuration and domains.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-04 Can mandatory SSO and alternative sign-in be controlled?

Conditional

The Entra ID guide requires members to use SSO when enabled, while owners and managers can use other sign-in methods. Confirm protection of administrator exceptions, other IdP behavior and access during IdP outages.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Authentication and permissions (continued)

IAM-05 Can source IP addresses be restricted?

Conditional

IP Restriction is available on paid plans. The guide applies it to managers and members, with an owner exception. Confirm owner protection, guest/API routes and allowed IP/CIDR scope.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-06 Are role permissions checked after authentication?

Verified

The design authorizes requests using role, workspace and sharing settings in addition to authentication. Owners, managers, members and guests have different permissions. Workspace deletion and billing are owner functions. See DAT-07 for tenant separation and IAM-08 for group/feature access.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-07 Can members and their roles be managed?

Verified

Owners and managers can add/remove members and change roles. Ownership must be transferred before removing the current owner.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-08 Can access be configured by group and feature?

Verified

Member access can be configured for groups, floors, projects and features such as translation and virtual office. Apply the minimum permissions needed for your organization.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Authentication and permissions (continued)

IAM-09 Can meeting and file-processing records be shared with the right audience?

Conditional

Meeting-log permissions and sharing settings are managed. Verify viewers according to the source, such as a Bot, virtual office or file processing, and the sharing method. Check floor participation and record sharing separately. See USE-04 for participation and USE-07 for exported copies.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-10 Are session identifiers and cookies protected?

Conditional

Session information is managed, with attributes such as Secure and SameSite checked for each route. Confirm each attribute, including HttpOnly, for the screen and authentication method. This replaces the earlier blanket cookie-attribute description.

Updated 2026-10-21 | Current public guides and verification records

IAM-11 Can session expiry and revocation be managed?

Conditional

Password-reset links expire and cannot be reused; completing a reset revokes existing sessions. Confirm absolute/idle timeouts, per-device revocation and SSO-linked revocation individually.

Updated 2026-10-21 | Current public guides and verification records

IAM-12 What password strength and storage rules apply?

Confirm individually

Users can change passwords. Verify current length, complexity, hashing and reuse rules against current technical evidence. Contact us before adoption for specific authentication requirements.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Authentication and permissions (continued)

IAM-13 Are login attempts and other requests limited?

Conditional

Request-count and capacity limits depend on IP address, authenticated user and feature. Login, verification-code resends and guest admission have specific controls. Thresholds, exceptions and unblock conditions are private. Reaching a limit alone does not establish malicious intent.

Updated 2026-10-21 | Current public guides and verification records

IAM-14 Is automated provisioning or dormant-account suspension available?

Confirm individually

Confirm SCIM, IdP-linked deletion and automatic dormant-account suspension individually. Standard member management does not guarantee automated integration.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-15 Can customers review their account inventory?

Verified

Administrators can inspect members/roles and export the member list as CSV. Customers should manage removal after transfers/departures and periodic permission reviews.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-16 Is operators' privileged access restricted?

Confirm individually

Confirm operator permission scope, authentication, approvals and activity records individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Authentication and permissions (continued)

IAM-17 Are employee account creation, changes and reviews managed?

Confirm individually

Contact us about employee account creation, changes and permission reviews.

Carried forward 2026-09-08 | Earlier PDF and related public guides

IAM-18 Are access and issued equipment handled on departure?

Confirm individually

Contact us about access termination and return of issued equipment when employees leave.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Infrastructure, endpoints and monitoring

INF-02 Is network access controlled?

Verified

Official materials describe source-IP restrictions for servers and databases using AWS Security Groups. Disclosure of detailed architecture and permitted routes is coordinated individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

INF-03 Is continuous threat detection performed?

Confirm individually

Amazon GuardDuty is one possible cloud threat-detection method. Earlier documentation is not proof of enablement for every service; confirm current scope, settings and alert destinations individually. Threat detection and file antivirus scanning are separate controls.

Updated 2026-10-21 | Current public guides and verification records

INF-04 Does a WAF cover all public services?

Confirm individually

Confirm covered domains/APIs, rules, exceptions and log operations individually. Use of a CDN or DDoS protection does not prove WAF coverage on every route.

Carried forward 2026-09-08 | Earlier PDF and related public guides

INF-05 Are DDoS protections used?

Conditional

Published materials describe Cloudflare for content delivery and DDoS protection. Confirm routes, subscribed services and guarantees for attack scale individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Infrastructure, endpoints and monitoring (continued)

INF-06 What is the antivirus/EDR scope?

Confirm individually

Confirm antivirus and EDR coverage and implementation individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

INF-07 Is system operation monitored?

Conditional

Processes, responses, scheduled jobs, certificates and monitoring-tool health are checked, with anomaly alerts. Confirm CloudWatch/custom-alert coverage per configuration. Automated monitoring does not guarantee continuous staffed response.

Updated 2026-10-21 | Current public guides and verification records

INF-08 Can administrators inspect and export activity history?

Conditional

EventLog shows actor, action, time and source IP, with filtering by period, member and category and export to CSV/PDF. Confirm permissions and plan conditions. See DAT-11 for retention and INF-14 for continuous SIEM export, WORM storage and tamper protection.

Carried forward 2026-09-08 | Earlier PDF and related public guides

INF-10 Are employee endpoints and software managed?

Conditional

A local implementation is being tested on designated operational endpoints to review processes, startup, SSH settings/permissions and monitoring-tool health. This is development for DaaS use, not a guarantee of deployment to all employee/customer devices or EDR-equivalent protection.

Updated 2026-10-21 | Current public guides and verification records

Infrastructure, endpoints and monitoring (continued)

INF-11 Is physical security managed?

Confirm individually

Define the relevant office/data-center scope and confirm physical controls individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

INF-12 How are keys and secrets managed?

Confirm individually

Confirm key/secret management and customer-managed key support against specific requirements.

Carried forward 2026-09-08 | Earlier PDF and related public guides

INF-13 Are unattended screens and desks protected?

Confirm individually

Contact us about employee screen locking and protection of information left on desks.

Carried forward 2026-09-08 | Earlier PDF and related public guides

INF-14 Are logs protected from tampering and unauthorized deletion?

Confirm individually

Confirm tamper/deletion controls, storage methods and integrations with external monitoring systems individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

INF-15 Is there a time-synchronization policy?

Confirm individually

Contact us about time-synchronization scope and management.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Application and development

APP-01 What controls address SQL injection?

Verified

Official materials describe database access using ORMs/placeholders and restricted database privileges. Assessment scope, date and results require separate confirmation.

Carried forward 2026-09-08 | Earlier PDF and related public guides

APP-02 Are OS command-injection risks addressed?

Conditional

Calls to external programs separate commands from arguments and restrict accepted values. This does not guarantee that no process ever uses a shell. Confirm individual call paths and test coverage in technical evidence.

Updated 2026-10-21 | Current public guides and verification records

APP-03 What controls address directory traversal?

Conditional

The design checks destinations and file permissions to prevent arbitrary paths exposing private files. Download URLs are issued after checking access to the original data. Confirm coverage for each upload/download route.

Updated 2026-10-21 | Current public guides and verification records

APP-04 What controls address XSS?

Conditional

Output is handled appropriately and returned data is limited. HTTPS alone is not an XSS defense. Confirm CSP and cookie-attribute coverage for each screen.

Updated 2026-10-21 | Current public guides and verification records

Application and development (continued)

APP-05 What controls address CSRF?

Conditional

Request origin is checked on routes such as cookie-authenticated requests. HTTP methods or notifications alone are not CSRF defenses. Check authentication, Origin/Referer validation and exceptions for each route.

Updated 2026-10-21 | Current public guides and verification records

APP-06 Are HTTP header-injection risks addressed?

Verified

Published controls use APIs for header output. Confirm input handling and response-splitting test evidence individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

APP-07 Are email header-injection risks addressed?

Confirm individually

Confirm current coverage for email-header validation and newline handling individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

APP-08 What controls address clickjacking?

Confirm individually

Review embedding restrictions such as X-Frame-Options and CSP frame-ancestors per screen/delivery destination. Earlier documentation alone does not establish universal coverage. Check exceptions for features requiring embedding.

Updated 2026-10-21 | Current public guides and verification records

Application and development (continued)

APP-09 How are memory-corruption risks addressed?

Conditional

Official specifications describe Node.js and other runtimes. Runtime characteristics alone do not eliminate vulnerabilities in native or dependency code. See APP-16 for dependency review and update procedures.

Carried forward 2026-09-08 | Earlier PDF and related public guides

APP-11 Are development and change controls defined?

Conditional

The policy reviews scope, diffs, data migrations and recovery procedures, then verifies actual versions, processes, responses and affected features after deployment. Confirm implementation records and approval conditions by product.

Updated 2026-10-21 | Current public guides and verification records

APP-12 Are third-party vulnerability assessments performed?

Confirm individually

Confirm external assessment scope, dates and remediation status individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

APP-13 Are development, testing and production separated?

Confirm individually

Confirm environment separation for the relevant configuration individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Application and development (continued)

APP-14 Is personal information protected in test data?

Confirm individually

Contact us about permitted test-data use and protection of personal information.

Carried forward 2026-09-08 | Earlier PDF and related public guides

APP-15 Does another person review code?

Confirm individually

Contact us about code-review methods and coverage.

Carried forward 2026-09-08 | Earlier PDF and related public guides

APP-16 Are vulnerability information and remediation managed?

Conditional

Records cover direct and indirect dependency inventories, npm/OSV/Go advisory checks and maintainer notices. Work includes artifact review, isolated testing without credentials, remediation and post-deployment checks; examples appear in this document. Scope varies by environment. Some dependencies use compatibility patches and some tools have usage restrictions. This does not guarantee that all dependencies are vulnerability-free.

Updated 2026-10-22 | Current public guides and verification records

APP-17 Can development security tests be reviewed?

Conditional

Records cover authentication/recovery, rejection of cross-organization access, API permissions and meeting communications. Results apply to the tested environment at the time. Distinguish development or undeployed changes from available features.

Updated 2026-10-21 | Current public guides and verification records

Availability, continuity and incident response

OPS-01 What are the service hours?

Conditional

Earlier guidance described availability in principle 24 hours a day, 365 days a year. Confirm current terms, scheduled maintenance, outages and service/contract conditions. Service hours differ from staffed support hours.

Updated 2026-10-21 | Current public guides and verification records

OPS-02 What uptime does the SLA guarantee?

Conditional

The earlier edition described at least 99.9%. Confirm current guarantees, covered services, calculation, planned downtime, exclusions and credits/refunds in the applicable contract. Do not treat historical guidance as a guarantee for every contract.

Updated 2026-10-21 | Current public guides and verification records

OPS-03 Can recent uptime measurements be reviewed?

Confirm individually

Confirm current availability results with a defined measurement period and method. An undated cumulative result is not a measurement of the latest 12 months.

Carried forward 2026-09-08 | Earlier PDF and related public guides

OPS-04 Are backups taken?

Confirm individually

Confirm backup scope, frequency, locations and retention individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Availability, continuity and incident response (continued)

OPS-05 Can business-continuity arrangements be reviewed?

Confirm individually

Contact us about continuity arrangements and available evidence.

Carried forward 2026-09-08 | Earlier PDF and related public guides

OPS-06 Are RTO, RPO and recovery capability guaranteed?

Confirm individually

Confirm recovery time and recovery point objectives individually for the required services and contract.

Carried forward 2026-09-08 | Earlier PDF and related public guides

OPS-07 Are maintenance and specification changes announced?

Conditional

Guidance describes maintenance/change communications. Confirm timing and notice conditions under the service contract.

Carried forward 2026-09-08 | Earlier PDF and related public guides

OPS-08 Which outage-reporting and support channels are available?

Verified

Guidance lists email, in-app chat and inquiry forms. Check business hours and emergency-contact conditions. Normal response estimates are not a fixed response-time SLA.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Availability, continuity and incident response (continued)

OPS-09 Are incident-response procedures defined?

Conditional

The basic policy covers anomaly detection, necessary record preservation, impact assessment, authorized containment, recovery and recurrence prevention. Confirm staffing, communications, approvals and recovery conditions individually.

Updated 2026-10-21 | Current public guides and verification records

OPS-10 Can security events be discussed individually?

Confirm individually

Security-event information is handled individually after agreeing the period and disclosure scope.

Carried forward 2026-09-08 | Earlier PDF and related public guides

OPS-11 Are customer outage-notification targets defined?

Confirm individually

Confirm recipients, channels and notification deadlines under the applicable contract.

Carried forward 2026-09-08 | Earlier PDF and related public guides

OPS-12 Are incident evidence and response records preserved?

Conditional

The policy preserves relevant records and correlates time, configuration changes and processes. Screen records can support investigation in the DaaS development environment. This does not universally guarantee completeness, tamper resistance or legal evidentiary status.

Updated 2026-10-21 | Current public guides and verification records

AI and external integrations

AI-01 Is customer audio or transcription used for AI training?

Verified

Published policy excludes customer audio, transcripts and similar content from AI-model training/development. Check external-service use separately from training use.

Carried forward 2026-09-08 | Earlier PDF and related public guides

AI-02 What data is sent to external AI, and where?

Conditional

Public materials describe OpenAI for meeting summaries/text analysis with processing in the United States. Confirm current models, transmitted data and destinations for the selected feature and processing.

Carried forward 2026-09-08 | Earlier PDF and related public guides

AI-03 How long does the external AI provider retain data?

Conditional

Published policy describes zero-data-retention settings for the OpenAI API used by VoicePing. This does not automatically apply to customer-connected AI or consumer services. Confirm current configuration evidence individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

AI-04 Is AI output accuracy guaranteed?

Conditional

Customers should compare translations, transcripts, summaries, subtitles and dubbing with original audio/video/records before important decisions or external use. This is a customer review responsibility, not a promise of 100% accuracy.

Carried forward 2026-09-08 | Earlier PDF and related public guides

AI and external integrations (continued)

AI-05 Can AI features be disabled or models pinned?

Confirm individually

Confirm summary scope, administrator-wide controls, model pinning, change notices and prompt retention individually. Distinguish individual feature settings from organization-wide policy enforcement.

Carried forward 2026-09-08 | Earlier PDF and related public guides

AI-06 Can external AI or APIs access meeting logs?

Conditional

External access supports MCP-compatible AI clients and API keys, with connections managed by administrators. Customers should also assess the destination's retention, training use and access controls.

Carried forward 2026-09-08 | Earlier PDF and related public guides

AI-07 Can API/MCP permissions be limited?

Verified

Scopes distinguish meeting-list search, record-body reading and AI-summary reading. API keys can have allowed-IP restrictions. Grant only the scopes needed for each purpose.

Carried forward 2026-09-08 | Earlier PDF and related public guides

AI-08 Can external connections be disabled, deleted and audited?

Verified

MCP connections and API keys can be disabled, re-enabled or deleted. Issuance, approval and disablement are recorded in event logs. Disable suspected leaked keys and check copies stored at the destination.

Carried forward 2026-09-08 | Earlier PDF and related public guides

AI and external integrations (continued)

AI-09 Can notification content and destinations be managed?

Conditional

Enabled integrations send notification text or meeting summaries. Customers should check recipients, public channels and content. See the data-handling table for Slack, Discord and Chatwork locations/purposes.

Carried forward 2026-09-08 | Earlier PDF and related public guides

AI-10 Can an EU DPA be executed?

Confirm individually

Confirm current DPA availability, representative arrangements and transfer conditions individually. This document does not establish execution of a DPA or GDPR compliance.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Usage and customer responsibilities

USE-01 Can mobile devices process offline?

Conditional

After downloading models, Offline Transcript on iOS/Android transcribes and translates audio on-device. This processing differs from cloud features and web-meeting Bots.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-02 Can offline records be deleted?

Verified

Guidance describes reviewing/deleting offline records in the device's history. Customers also need device controls for loss, OS backups and data export restrictions.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-03 Are PCs and servers fully offline too?

Confirm individually

Distinguish standard cloud features from mobile offline features. Confirm requirements for isolated PC networks, dedicated or on-premises deployments. Mobile support does not mean every product works offline.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-04 Can subtitle listeners and virtual-office guests be controlled?

Conditional

Subtitle listeners use URLs/QR codes; virtual-office guests join an enabled guest web app through invitation URLs. Check audiences and participation settings separately. Define link distribution, passwords, identity checks and plan requirements. External subtitle distribution also requires checking event-use conditions.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Usage and customer responsibilities (continued)

USE-05 Who manages recording/transcription notices and permissions?

Conditional

Customers must verify permissions, participant explanations and required consent for recording/transcription in meetings, events and virtual offices, and for file processing. Requirements depend on applicable law, internal rules and data classification.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-06 May confidential or sensitive data be used?

Confirm individually

Assess data type, purpose, legal basis, destinations and storage conditions before deciding suitability. This is not unconditional authorization to submit highly sensitive information.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-07 How is exported data protected?

Conditional

Customers manage storage, sharing permissions and expiry for downloaded records/audio, subtitles/dubbing, shared files and time reports. Changing service permissions does not retrieve previously downloaded copies.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-08 Which settings should be checked during adoption?

Conditional

Confirm features, plan and actual settings for voice translation and virtual office. See IAM for authentication, IAM-09 for record sharing, AI-06 to AI-08 for integrations, DAT-08 to DAT-11 for retention and USE-10 to USE-15 for feature-specific issues. Customers should check entitlements, administrators and applied settings against requirements.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Usage and customer responsibilities (continued)

USE-09 What data-return and access-removal tasks apply at exit?

Conditional

Customers separately manage exports, integration disablement (AI-08), unnecessary-account removal (IAM-07), cancellation and deletion requests (DAT-12). Cancellation, access removal and personal-data erasure are distinct states.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-10 Can meeting-Bot admission and calendar integration be managed?

Conditional

A visible Bot joins supported web meetings subject to host admission. Google Calendar/Outlook connections are configured when used. Customers should check meetings, connected accounts/permissions, recording notices and record recipients.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-11 Can file-processing inputs and outputs be managed?

Conditional

Uploaded audio/video produces transcripts, translations and supported subtitle/dubbing outputs, reviewed in meeting logs. Check input rights, output sharing/export, supported formats/features and retention/deletion conditions.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-12 Are virtual-office presence and history distinct?

Conditional

Virtual offices display presence and work notes. Online logs can show presence history, distinct from project time tracking. Check explanations to affected users, required displays/history, viewers and retention.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Usage and customer responsibilities (continued)

USE-13 Can sharing scope be checked during virtual-office collaboration?

Conditional

Floors/rooms support screen sharing, text editors and whiteboards. Screen sharing can select a desktop or window. Check participants/guests and shared content, including accidental disclosure through notifications or other windows.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-14 Can optional time-tracking capture and viewer permissions be configured?

Conditional

Time tracking and desktop images, webcam images and input activity are separate per-member settings. Owners/managers see team logs; members see their own. Check capture types, intervals, blurring, user explanations, viewers and retention. Running the timer requires the PC app.

Carried forward 2026-09-08 | Earlier PDF and related public guides

USE-15 Can remote desktop control be managed?

Conditional

Collaboration guidance describes requesting control of a shared screen and the sharer's ability to revoke it. Customers manage whether it is allowed, counterpart identity, device/screen scope and revocation when finished. Confirm detailed restrictions and activity-record requirements individually.

Carried forward 2026-09-08 | Earlier PDF and related public guides

Additional checks informed by leakage patterns

These VoicePing review questions draw on official JPCERT/CC, IPA, FBI/CISA and partner materials [R1-R4], rather than reproducing their text. They do not indicate that these attacks occurred at VoicePing or that every control is implemented.

LEAK-01 Are organization, role and data permissions checked for direct API calls?

Conditional

Servers separate authentication from authorization and check organization, role, ownership and visibility. Records include tests rejecting cross-organization retrieval and unauthorized administration. Confirm full endpoint assessment scope and dates individually.

Added 2026-10-21 | Public API authorization | JPCERT/CC [R1]

LEAK-02 Can missing/malformed tokens or header differences bypass authentication?

Confirm individually

Credentials are validated on the server by design. Confirm API-specific tests/results for missing headers, malformed or expired tokens, invalid signatures and changed methods.

Added 2026-10-21 | Public API authorization | JPCERT/CC [R1]

LEAK-03 Are administrative secrets absent from distributed apps, public repositories and logs?

Confirm individually

Confirm review scope for API keys, private keys and long-lived tokens in artifacts/logs. Server-side authentication/authorization is needed rather than relying only on obfuscation or in-app signing. Distinguish public identifiers from secrets; confirm detection history and reviewed artifacts individually.

Added 2026-10-21 | Exposed secrets | JPCERT/CC [R1 / R4]

LEAK-04 Can leaked API keys and integrations be restricted and revoked?

Conditional

Check API scopes/allowed IPs, MCP OAuth authorization, current membership and data permissions. Connections/keys can be disabled or deleted. Distinguish personal and organization-shared keys; investigate affected connections and destination copies after suspected leakage.

Added 2026-10-21 | Stolen API keys | JPCERT/CC [R1]

Additional checks informed by leakage patterns (continued)

LEAK-05 Are administrative APIs, databases and origin servers protected from unintended routes?

Conditional

Public entry points and administrative connections are separated, with cloud/host source restrictions. Records show rejection of direct connections and testing of allowed paths. Confirm coverage of every configuration individually.

Added 2026-10-21 | Exposed administration | JPCERT/CC [R1]

LEAK-06 Are configuration files, debug output and backups inaccessible from public areas?

Confirm individually

Review web roots, storage visibility, CDN caches and test files. Confirm configuration evidence and external retrieval tests for all stores individually.

Added 2026-10-21 | Exposed files and backups | JPCERT/CC [R1]

LEAK-07 Are SQL/NoSQL queries protected from malicious input?

Conditional

SQL uses ORMs or parameterized queries, with input-format and target checks. Separately confirm technology inventory, including NoSQL, and negative tests for each route. SQL controls alone do not establish coverage of every query type.

Added 2026-10-21 | Injection and invalid input | JPCERT/CC [R1]

LEAK-08 Are known vulnerabilities and missed updates identified?

Conditional

Dependencies are inventoried and checked against advisories. Review versions, exploitation status, impact and deployed fixes/mitigations. Confirm deadlines and all-asset coverage individually.

Added 2026-10-21 | Known vulnerabilities | JPCERT/CC [R1] / IPA [R2]

Additional checks informed by leakage patterns (continued)

LEAK-09 Are IP/user/feature limits checked for impact on legitimate use?

Conditional

Login, recovery and guest admission have request/capacity limits, considering shared IPs and legitimate users. Confirm bulk-extraction detection and alert operations separately; rate limits alone do not prevent exfiltration.

Added 2026-10-21 | Bulk extraction and attempts | JPCERT/CC [R1]

LEAK-10 Are unauthorized remote-control tools or startup additions detected?

Conditional

A local implementation tests process, startup and access-permission changes on designated operational endpoints. Remote access requires checking user, scope and revocation at completion. Confirm application control and EDR coverage for all endpoints separately.

Added 2026-10-21 | Remote-control abuse | FBI / CISA and others [R3]

LEAK-11 Could someone trick support into resetting passwords or MFA?

Confirm individually

Review identity checks, callbacks to known contacts, approvals and records during recovery, credential changes and device registration. Protected email links alone do not guarantee the security of human-assisted support.

Added 2026-10-21 | Impersonation and recovery | FBI / CISA and others [R3]

LEAK-12 Are MFA methods and exception routes evaluated against credential theft?

Confirm individually

See IAM-02 to IAM-04 for email checks, SSO and external authentication. Separately verify enforced phishing-resistant MFA and coverage of administrator exceptions/recovery routes.

Added 2026-10-21 | Phishing and MFA | FBI / CISA and others [R3]

Additional checks informed by leakage patterns (continued)

LEAK-13 Do stolen sessions or integrations survive password changes?

Conditional

Existing-session revocation after password reset has been verified. Check API keys, MCP connections and IdP sessions separately for disablement/revocation scope. One change does not invalidate every credential.

Added 2026-10-21 | Session theft | FBI / CISA and others [R3]

LEAK-14 Can integration permissions and transmitted data be limited after a supplier/AI compromise?

Conditional

Review integration permissions/disablement, transmitted data and purposes. Separately assess subprocessors, retention/deletion, incident notification and services independently connected by customers.

Added 2026-10-21 | Suppliers and integrations | IPA [R2]

LEAK-15 Are meeting records, subtitle URLs and files shared only with intended recipients?

Conditional

Check organization, role, visibility, invitation validity and meeting permissions. Link renewal and removal of admitted guests are separate actions. This does not guarantee retrieval of downloaded copies or automatic prevention of all mistaken sharing.

Added 2026-10-21 | Sharing and misdelivery | Operational review informed by IPA [R2]

LEAK-16 Are accounts, SSH keys, shared keys and integration permissions reviewed after departures?

Conditional

Member/role management and administrative SSH-key inventory/revocation checks are performed. Operational review must cover shared keys and integrations as well as personal accounts. Confirm automated offboarding and all-asset enforcement separately.

Added 2026-10-21 | Excess access and departures | IPA [R2]

Additional checks informed by leakage patterns (continued)

LEAK-17 Can misuse of normal permissions or bulk exports be investigated?

Confirm individually

Review activity logs and data permissions. Confirm bulk-exfiltration detection, approvals, alerts, DLP and tracking of stored copies separately. This does not imply automatic classification of every authorized action as legitimate or abusive.

Added 2026-10-21 | Insider abuse and exports | IPA [R2]

LEAK-18 Are new packages/extensions reviewed before execution?

Conditional

Policy reviews source, artifacts, dependencies, signatures/integrity and scripts, with first execution tested in credential-free isolation. Insufficient evidence holds the change. Confirm application, exceptions and records individually.

Added 2026-10-21 | Supply chain | IPA [R2]

LEAK-19 Are confidential AI inputs and tool-execution permissions restricted?

Conditional

MCP checks OAuth/PKCE, scopes, membership and data permissions. Customers must also evaluate retention, training use and execution approval for connected AI. This does not guarantee prompt-injection protection on every route.

Added 2026-10-21 | Generative AI and automation | Integration review informed by IPA [R2]

LEAK-20 Can process, startup and key changes be compared with records?

Conditional

Designated endpoints detect changes and alert operators, who compare work records. Remote PCs/servers also receive operation and administrative-connection checks. Coverage varies by environment; an alert alone does not establish malware.

Added 2026-10-21 | Suspicious execution | FBI / CISA and others [R3]

Additional checks informed by leakage patterns (continued)

LEAK-21 Are purpose, scope and viewers restricted for screen review?

Conditional

Periodic screen capture and time-based review are tested in the DaaS development environment. Capture pauses while idle, locked or asleep by design. Confirm user explanations, viewers, retention and deletion before adoption. Distinguish this from a generally available DaaS feature.

Added 2026-10-21 | Work records and human error | VoicePing operational review

LEAK-22 Can screen records, alerts or investigation logs expose secrets?

Conditional

The reviewed recorder stores images locally and does not itself transmit images over the network. Alerts exclude images, private-key contents, raw command arguments and keystrokes. Separately confirm storage encryption, endpoint protection and identifying information in alerts.

Added 2026-10-21 | Leakage through records | VoicePing operational review

LEAK-23 Are stopped monitors, lost permissions or full disks detected?

Conditional

Monitoring-tool health and recording errors are checked in the designated environment. Limits include deletion while stopped, recording gaps, short-lived processes and actions not shown on screen. These records are not a substitute for immutable logs or EDR.

Added 2026-10-21 | Monitoring and evidence gaps | VoicePing operational review

LEAK-24 Are backups protected from attackers and restore-tested?

Confirm individually

Check privilege separation, offline/immutable copies, restore tests and RTO/RPO per environment. Current coverage/evidence requires individual confirmation. Treat application rollback and data restoration separately.

Added 2026-10-21 | Ransomware and recovery | FBI / CISA and others [R3] / IPA [R2]

Additional checks informed by leakage patterns (continued)

LEAK-25 Can records be preserved and access stopped after a suspected incident?

Conditional

Policy stops further suspicious execution, preserves necessary records and assesses impact. Blocking, revocation and credential changes require checking authority and impact. Confirm staffing and specific response times individually.

Added 2026-10-21 | Investigation and containment | FBI / CISA and others [R3]

LEAK-26 Is compromise checked across endpoints, environments and shared credentials?

Confirm individually

Correlate accounts, shared keys, destinations and execution history. Worker-assignment checks alone cannot fully isolate the impact of shared-credential leakage. Confirm cross-environment investigation scope and available records.

Added 2026-10-21 | Persistence and lateral movement | FBI / CISA and others [R3]

LEAK-27 Are customer communications and reporting scope defined for suspected leakage?

Confirm individually

Confirm contacts, affected periods/data, contractual notification conditions and legally required procedures. Normal support response estimates differ from incident notification deadlines and recovery guarantees.

Added 2026-10-21 | Notification and explanation | Operational review informed by IPA [R2]

LEAK-28 Are legitimate use and recurrence prevention checked after blocking/unblocking or fixes?

Conditional

Review the proposed change, prior unblock records and user impact, then act within granted authority. Verify actual operation and affected features afterward. This differs from ordinary account cancellation or personal-data deletion.

Added 2026-10-21 | Recurrence and manual changes | VoicePing operational review

Additional checks informed by leakage patterns (continued)

LEAK-29 Can URL-fetch features reach internal networks or unintended destinations?

Confirm individually

Review restrictions for URL previews, file retrieval and integrations, including redirect destinations. Confirm implementation/tests for internal and cloud-metadata addresses, post-resolution destinations, response sizes and timeouts per feature. This is not a statement that every route has complete protection.

Added 2026-10-21 | External URL fetching and SSRF | JPCERT/CC [R4]

Data handling and external processing

This retains the earlier processing-destination information. Check data, locations, retention and deletion for the selected feature against current privacy policy and contracts. The table includes customer-connected services and offline devices, so not every entry is a subprocessor.

Provider / destination	Purpose	Location	Data and review points
AWS	Cloud infrastructure, storage, monitoring	Tokyo, Japan	Customer content, account and operational data. Confirm backup replication locations separately.
Google Cloud	Databases, static hosting	Tokyo, Japan	Database information and static content. Confirm the relevant service configuration.
Cloudflare	CDN and DDoS protection	Global	IP addresses, request information and caches. Processing is not restricted entirely to Japan.
OpenAI	Meeting summaries, text analysis	United States	Transcripts/text for applicable features. This is not an exhaustive list of speech-recognition processors.
Slack / Discord	Summary and other notifications	United States	Notification content and meeting summaries, depending on enabled integrations.
Chatwork	Summary and other notifications	Japan	Notification content and meeting summaries, depending on enabled integrations.
Customer-connected AI / systems	API/MCP retrieval	Depends on destination	Records/summaries within authorized scopes. Customers review retention, training use, contracts and permissions.
Customer-connected meetings / calendars	Meeting Bot, calendar integration	Depends on service/ settings	Meeting links, events, audio/video. Check permissions and retention for Zoom, Google Meet, Teams, Google Calendar, Outlook and other connections.
Mobile device (offline)	On-device transcription/ translation	On the device	Offline audio/text. Requires prior model download and customer device management.

References and support

Additional questions draw on the official sources below. IPA selected its 2026 list based on 2025 incidents and other evidence. These sources do not establish attack frequency or VoicePing incident history. Official sources were reviewed on October 21, 2026.

Official security documentation | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/security>

Public encryption, authentication, access-control and monitoring information.

Privacy policy | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/privacy-policy>

Purposes, processors, locations, retention and deletion.

Public GDPR DPA | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/gdpr-dpa>

Personal-data processing and international-transfer terms. Check the current applicable version.

Member roles and permissions | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/member-roles>

Workspace roles and permissions.

Member management | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/member-management>

Member administration and list exports.

Microsoft Entra ID SSO | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/sso-entra-id>

SSO setup using Microsoft Entra ID.

HENNGE One SSO | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/sso-henнге-one>

SSO setup using HENNGE One.

IP Restriction | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/ip-whitelist>

Source-IP access restrictions.

References and support (continued)

EventLog | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/event-log>

Activity history, filtering and export.

Meeting records and AI summaries | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/meeting-minutes>

Meeting records, sharing and AI summaries.

Mobile offline translation | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/mobile-offline-translation>

On-device processing and history management.

External access | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/external-access>

API and MCP connection management.

Pricing and data storage | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/pricing>

Plans and storage guidance.

VoicePing official website | Earlier reference 2026-09-08

<https://voiceping.net/en/>

Services and enterprise features.

Invitations and two-step authentication | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/invite-members>

Member invitations and email verification.

Virtual office product | Earlier reference 2026-09-08

<https://voiceping.net/en/products/virtual-office/>

Presence, collaboration, floors and guest access.

Time tracking product | Earlier reference 2026-09-08

<https://voiceping.net/en/products/time-tracking/>

Work time, optional capture, viewer permissions and export.

References and support (continued)

Meeting Bot product | Earlier reference 2026-09-08

<https://voiceping.net/en/products/meeting-bot/>

Meeting admission, calendar connections and records.

File transcription product | Earlier reference 2026-09-08

<https://voiceping.net/en/products/video-translation/>

Uploads, translation, subtitles, dubbing and exports.

Time tracking management | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/time-tracking-management>

Per-member capture settings, intervals and blurring.

External floor guest invitations | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/guest-invitation>

Guest web app and invitation links.

Collaboration tools | Earlier reference 2026-09-08

<https://manual.voiceping.net/en/collaboration-tools>

Screen sharing, editors, whiteboards and remote control.

[R1] JPCERT/CC unauthorized-access advisory (Japanese) | Updated 2026-10-09

<https://www.jpcert.or.jp/at/2026/at260030.html>

Review points for APIs, credentials and configuration.

[R2] IPA Information Security Top 10 Threats 2026 (Japanese) | Published 2026-01-29

<https://www.ipa.go.jp/security/10threats/10threats2026.html>

Selected based on incidents in 2025 and other evidence; organizational review topics.

[R3] FBI, CISA and partners: Scattered Spider | Updated 2025-07-29

<https://www.ic3.gov/CSA/2025/250729.pdf>

Impersonation, authentication, remote control and recovery review points.

Application security | This edition 2026-10-21

<https://manual.voiceping.net/en/security-application>

Authentication, authorization, APIs and web-attack defenses.

References and support (continued)

Infrastructure security | This edition 2026-10-21

<https://manual.voiceping.net/en/security-infrastructure>

Transport, connections, detection and backups.

Endpoint monitoring and security operations | This edition 2026-10-21

<https://manual.voiceping.net/en/security-operations>

DaaS development, manual checks, human error and software review.

Official BSI certification information | Checked 2026-10-21

<https://voice-ping.com/products/meeting-bot/>

ISO/IEC 27001:2022, IS 820960.

Earlier security questionnaire | Issued 2026-09-08

<https://voiceping.net/pdf/security-checksheet-en-2026-09-08.pdf>

Earlier 114-question edition. Current corrections in this edition take precedence.

Security review and support | This edition 2026-10-21

<https://voiceping.net/en/support/>

Describe required materials and features without sending secrets.

[R4] JPCERT/CC research into successive unauthorized-access incidents (Japanese) | Published 2026-10-15

https://blogs.jpcert.or.jp/ja/2026/10/web_api_attacks.html

Review points for secrets in distributed apps, server-side authorization and SSRF.

MySQL 8.4 release notes | Checked 2026-10-22

<https://dev.mysql.com/doc/relnotes/mysql/8.4/en/>

Official sources used to verify library updates and versions

npm audit | Checked 2026-10-22

<https://docs.npmjs.com/cli/v11/commands/npm-audit/>

Official sources used to verify library updates and versions

OSV | Checked 2026-10-22

<https://osv.dev/>

Official sources used to verify library updates and versions

References and support (continued)

Go Vulnerability Database | Checked 2026-10-22

<https://pkg.go.dev/vuln/>

Official sources used to verify library updates and versions

Samlify security advisory | Checked 2026-10-22

<https://github.com/tngan/samlify/security/advisories/GHSA-w8r9-gp23-wcxp>

Official sources used to verify library updates and versions

Nodemailer 10.1.7 | Checked 2026-10-22

<https://github.com/nodemailer/nodemailer/releases/tag/v10.1.7>

Official sources used to verify library updates and versions

pgx 5.11.0 | Checked 2026-10-22

<https://github.com/jackc/pgx/releases/tag/v5.11.0>

Official sources used to verify library updates and versions

lib0 security advisory | Checked 2026-10-22

<https://github.com/dmonad/lib0/security/advisories/GHSA-g75x-89c3-rvmr>

Official sources used to verify library updates and versions