Offision

ISO 27001:2022 CERTIFIED · SECURITY & COMPLIANCE

Offision Security White Paper

A comprehensive overview of Offision's security architecture, governance, and compliance posture — covering data protection, identity, application security, and the controls that keep customer data safe on Microsoft Azure.

ISO 27001:2022 Certified

Hosted on Microsoft Azure

TLS 1.2+

VERSION

1.0

LAST UPDATED

2026-05-04

PUBLISHED BY

ONES Software Limited

Document Information

Field	Value
Document title	Offision Security White Paper
Product	Offision (Cloud SaaS)
Vendor	ONES Software Limited
Audience	Anyone evaluating Offision's security posture, including end users, prospective customers, security and procurement teams, and the general public
Scope	Offision Cloud SaaS only (Microsoft Azure-hosted). Self-hosted deployments are out of scope.
Version	1.0
Last updated	2026-05-04
Owner	Bernard Chung

Change History

Version	Date	Author	Summary of changes
1.0	2026-05-04	Kit Ngai	Initial public release. Includes Cloud Architecture overview at the top of §5 (Azure hosting, three-data-centre high availability in Japan, per-tenant database isolation, TDE encryption at rest, point-in-time recovery, Azure Firewall, HTTPS) with the Cloud Architecture diagram. Merged §5.1 Logical architecture overview and §5.2 Data flow into a single §5.1 Logical architecture and data flow with the Data flow diagram. Renumbered §5.3 Multi-tenant isolation and §5.4 Hosting and regions to §5.2 and §5.3 respectively. Documented the annual third-party security audit by MSX (latest April 2026) in §7.3. Documented current API rate-limit thresholds (Internal API 100 req/5s per user; External API 1,000 req/5s per token) in §10.9. Renamed the Outlook Add-in surface to **Microsoft Add-in** to reflect its presence inside Microsoft Outlook, Microsoft Teams, and the Microsoft 365 web apps.
1.0 RC2	2026-04-28	Bernard Chung	Expanded prose in §1 and §5–§8 with concrete detail. Wrote prose for previously-stubbed sections: §2 About, §3 Scope and Shared Responsibility, §4 Governance and Compliance, §9 Infrastructure and Cloud Security, §10 Integrations and API Security (10.1–10.9), §11 Logging, Monitoring, and Incident Response, §12 Business Continuity and Disaster Recovery, §13 Privacy and Data Protection (13.1–13.7), §14 Customer Responsibilities, §15 Responsible Disclosure, and §17 Disclaimer.
1.0 RC	2026-04-28	Bernard Chung	Promoted from skeleton draft to release candidate. Wrote prose for §1 Executive Summary, §5 Service Architecture, §6 Identity and Access Management, §7 Application Security, and §8 Data Protection, sourced from the Offision data-flow reference, External API documentation, and Privacy Policy.
0.3	2026-04-27	Bernard Chung	Aligned scope with the Neat Pulse reference white paper. Added §10.8 Outbound webhooks, §10.9 API rate limiting, §13.7 Data Processing Addendum, and §17 Disclaimer. Expanded §8.2 (TLS specifics) and §10.2 (Player enrollment). Tightened §6.4 (external support access into a positive control). Added new bullets to §14 (network egress and webhook receivers).
0.2	2026-04-27	Bernard Chung	Resolved hosting-region open item (Azure Japan East, §5.3, §13.4). Resolved MFA open item (native + IdP-delegated, §6.1).

Version	Date	Author	Summary of changes
0.1	2026-04-26	Bernard Chung	Initial skeleton: TOC, section objectives, and source citations.

Table of Contents

- Document Information
- Change History
- Table of Contents
- 1. Executive Summary
- 2. About Offision and ONES Software
- 3. Scope and Shared Responsibility Model
  - What ONES Software is responsible for
  - What the customer is responsible for
- 4. Security Governance and Compliance
  - 4.1 ISO/IEC 27001:2022 certification
  - 4.2 Underlying cloud certifications
  - 4.3 Policies, standards, and risk management
- 5. Service Architecture
  - Cloud Architecture
  - 5.1 Logical architecture and data flow
  - 5.2 Multi-tenant isolation
  - 5.3 Hosting and regions
- 6. Identity and Access Management
  - 6.1 End-user authentication
  - 6.2 Role-based access control
  - 6.3 Provisioning and deprovisioning
  - 6.4 Administrative access and least privilege
- 7. Application Security
  - 7.1 Secure development lifecycle
  - 7.2 Peer review and quality framework
  - 7.3 Vulnerability assessments
  - 7.4 Release management and staged deployments
- 8. Data Protection
  - 8.1 Data classification
  - 8.2 Encryption in transit
  - 8.3 Encryption at rest
  - 8.4 Password storage and token-based authentication
  - 8.5 Backups, retention, and secure deletion

- 9. Infrastructure and Cloud Security
  - 9.1 Azure data-centre physical security
  - 9.2 Redundancy and availability
  - 9.3 Network architecture and content delivery
  - 9.4 Continuous monitoring and threat detection
- 10. Integrations and API Security
  - 10.1 Internal APIs
  - 10.2 Player APIs and player device enrolment
  - 10.3 External APIs
  - 10.4 SSO interface
  - 10.5 Synchronization jobs
  - 10.6 Notification jobs
  - 10.7 Access-control integrations
    - Room access
    - Visitor access
  - 10.8 Outbound webhooks
  - 10.9 API rate limiting
- 11. Logging, Monitoring, and Incident Response
  - 11.1 Application and audit logging
  - 11.2 Operational monitoring
  - 11.3 Incident response process
- 12. Business Continuity and Disaster Recovery
  - 12.1 Redundancy posture
  - 12.2 Backup strategy and off-site storage
  - 12.3 RPO and RTO targets
- 13. Privacy and Data Protection
  - 13.1 Applicable law
  - 13.2 Personal data categories collected
  - 13.3 Purposes of processing
  - 13.4 Cross-border transfers
  - 13.5 Data subject rights
  - 13.6 Retention and deletion
  - 13.7 Data Processing Addendum and contractual data-protection terms
- 14. Customer Responsibilities
  - Identity and access
  - Integrations

    - Endpoint and credential security
    - Privacy obligations
    - Network egress and webhook receivers
- 15. Responsible Disclosure and Security Contact
- 16. References
- 17. Disclaimer

---

1. Executive Summary

Offision is a cloud-based smart-office management platform operated by ONES Software Limited. The service supports room, desk, and parking booking, visitor management, attendance tracking, event management, service management, ticket management, and digital signage. This white paper describes the security and privacy controls that apply to the Offision Cloud SaaS service, which is hosted on Microsoft Azure.

The document is intended for two audiences. The first is customer security and procurement teams reviewing Offision against an RFP or vendor questionnaire; for them, the paper is structured around control families and cites the public material that supports each statement. The second is any reader — existing customer, end user, or member of the public — who wants a structured account of how the service is operated and how their data is handled.

The remainder of this paper expands each of the following control families. Section references point to the section where the control is described in detail.

- **Governance and compliance (§4).** ONES Software's Information Security Management System covering the Offision service is certified to ISO/IEC 27001:2022. The service runs on Microsoft Azure infrastructure that holds ISO 27001, ISO 27018, and SOC 1, SOC 2, and SOC 3 attestations maintained by Microsoft.
- **Architecture and tenant isolation (§5, §7).** The service is decomposed into bounded API surfaces (Internal API, Player APIs, External API, SSO Interface) with separate Synchronization and Notification job tiers. Every customer is assigned a dedicated database, preventing cross-tenant data access by design. The hosting region is Microsoft Azure Japan East.
- **Identity and access management (§6).** Local password authentication is supported alongside Single Sign-On via SAML 2.0 and OpenID Connect with Microsoft 365. Multi-factor authentication is supported either natively in Offision or by delegation to the customer's identity provider. Authorization is governed by predefined least-privilege roles (Administrator, Staff, User) backed by granular feature, module, and data permissions.
- **Application security (§7).** A documented secure-development lifecycle gates all changes through peer review, automated and manual vulnerability assessments, and staged deployments through non-production environments before production.
- **Data protection (§8).** All client and integration traffic uses HTTPS, with plain HTTP automatically redirected and unauthenticated API requests rejected with HTTP 401. Customer data is encrypted at rest in the underlying Azure storage. End-user passwords are stored as one-way hashes; sessions and API access use server-issued tokens. Backups run continuously, are stored off-site, and are permanently destroyed at end of retention.
- **Integrations and APIs (§10).** Internal APIs are reachable only by authenticated users; Player APIs only by enrolled Offision Players; the External API is disabled by default and, when enabled, is protected by access tokens with optional source-IP allowlisting and configurable expiry. Outbound channels (notification jobs, workflow webhooks, booking-change subscriptions) are HTTPS-only.
- **Operations (§11, §12).** The production estate is monitored 24/7/365. Offision is deployed redundantly across Microsoft Azure data centres and targets 99.9% availability.

- **Privacy (§13).** Personal-data handling complies with the Personal Data (Privacy) Ordinance (Cap. 486) of Hong Kong. The Offision Privacy Policy sets out collection categories, purposes of processing, retention rules, and the additional rights available to users in the European Economic Area under the GDPR.

---

2. About Offision and ONES Software

Offision is developed and operated by **ONES Software Limited**, a private limited company incorporated under the laws of the Hong Kong Special Administrative Region. The registered office is at Room 804, Premier Centre, No. 20 Cheung Shun Street, Cheung Sha Wan, Kowloon, Hong Kong SAR.

The Offision service is delivered as a connected suite of components:

- A **Management Console** for tenant administration (user lifecycle, role assignment, integration setup, policy configuration).
- A **User App** (web and mobile) for end-user workflows: booking rooms, desks, and parking spaces, attendance check-in, raising service requests, viewing analytics, and similar tasks.
- A **Visitor App** used for visitor registration and check-in flows at front-desk kiosks and on visitor devices.
- A **Microsoft Add-in** that lets end users view and create bookings from inside Microsoft Outlook, Microsoft Teams, and the Microsoft 365 web apps.
- **Offision Players** — physical endpoint devices that include room display panels, desk display panels, e-paper room tags, lockers, and check-in kiosks.
- A back-end service hosted on Microsoft Azure that exposes Internal, External, Player, and SSO API surfaces, together with Synchronization and Notification job tiers, file/object storage, and an ORM-managed database.

Offision integrates with **Microsoft 365**, **Google Workspace**, **Active Directory**, **LDAP**, and **Microsoft Exchange Server** for user-directory and calendar synchronization.

General contact: `hello@offision.com`. Integration support: `support@bookings.one`. Offision's Privacy Policy and product documentation are listed in §16.

3. Scope and Shared Responsibility Model

This white paper covers the **Offision Cloud SaaS** deployment hosted on Microsoft Azure. Self-hosted Offision deployments, customer-operated player hardware beyond the Offision-supplied firmware, and customer-side integrations are out of scope.

Operating Offision securely is a shared responsibility between ONES Software and the customer.

What ONES Software is responsible for

- Operating the Offision application and its infrastructure on Microsoft Azure (compute, database, storage, networking).
- Maintaining the ISMS certified to ISO/IEC 27001:2022 (§4.1).
- Applying the secure-development, vulnerability-management, and release controls described in §7.
- Providing the authentication, authorization, and tenant-isolation mechanisms described in §5–§8.
- Operating the monitoring, backup, and incident-response processes described in §11–§12.
- Honouring the privacy commitments set out in the Offision Privacy Policy (§13).

What the customer is responsible for

- Configuring their identity provider (SAML 2.0 / OIDC) and choosing whether to enforce MFA at Offision or at the IdP (§6.1).
- Maintaining password policy where local authentication is used.
- Assigning roles consistent with each user's job function, performing periodic access reviews, and deprovisioning users that have left the organisation (§6.2, §6.3).
- Generating, scoping, IP-restricting, and rotating External API access tokens (§10.3).
- Maintaining customer-side mappings used by access-control integrations (email-to-card-number; bookable-resource-ID-to-access-control-unit; §10.7).
- Endpoint security and protection of credentials used for the Management Console and User App.
- Notifying their internal users when personal data is shared with Offision, as required by applicable privacy laws (Privacy Policy §1).
- Allowing the network egress required for Offision's hosted endpoints (§14).
- Operating customer-side webhook receivers (HTTPS endpoints with valid TLS certificates, secret confidentiality, signature/timestamp validation where provided, and a 2xx response within the receiver's expected window; §10.8 and §14).

A consolidated customer-responsibility checklist is in §14.

---

4. Security Governance and Compliance

4.1 ISO/IEC 27001:2022 certification

ONES Software's Information Security Management System covering the Offision service is certified to **ISO/IEC 27001:2022**, the current revision of the international standard for information security management systems. Certification is granted on the basis of an independent audit, requires the operation of an ISMS that covers asset and risk management, control selection, monitoring, internal audit, management review, and continuous improvement, and is maintained through periodic surveillance audits and a recertification cycle.

The certificate is issued to ONES Software Limited and is available on request.

4.2 Underlying cloud certifications

Offision is hosted in Microsoft Azure data centres. The physical and platform-level controls of those data centres are independently certified by Microsoft to **ISO 27001**, **ISO 27018**, **SOC 1**, **SOC 2**, and **SOC 3**. Offision relies on those underlying certifications for physical security, environmental controls, and platform-layer attestations; ONES Software does not separately attest to controls that Microsoft operates inside the data centre.

Customers that need to review the Microsoft attestations directly can obtain them through Microsoft's compliance offerings (see §16).

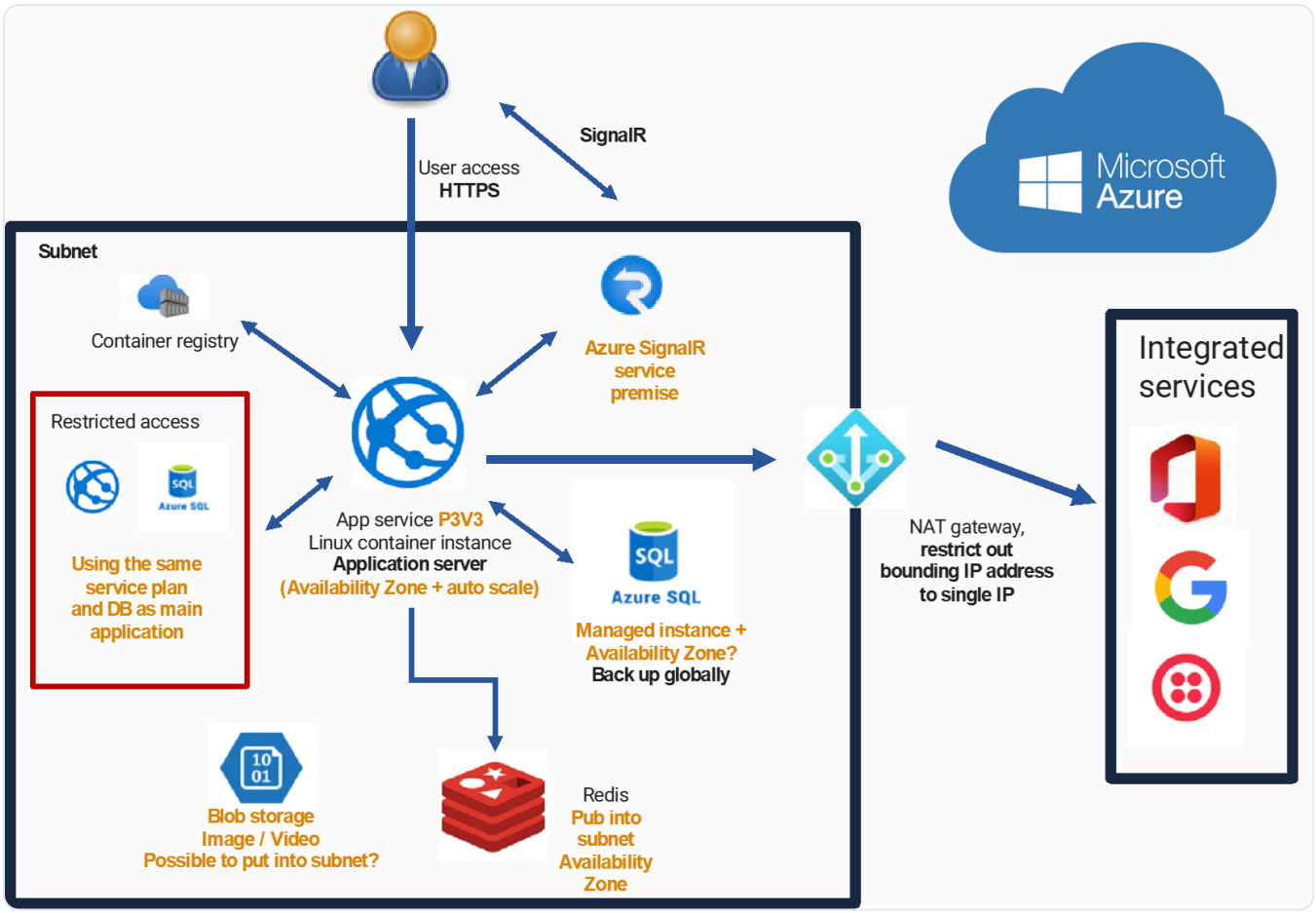
4.3 Policies, standards, and risk management

The ISMS is supported by a set of internal policies covering information security, secure development, access control, vulnerability management, incident response, and related areas. Policy ownership, the review cadence, and the details of the risk-assessment workflow are not publicly disclosed; further detail is available to customers under appropriate confidentiality terms during procurement review.

5. Service Architecture

Cloud Architecture

Offision is delivered as a managed Cloud SaaS service on Microsoft Azure. The architecture is designed for high availability, strict tenant isolation, and protection of customer data both in transit and at rest.



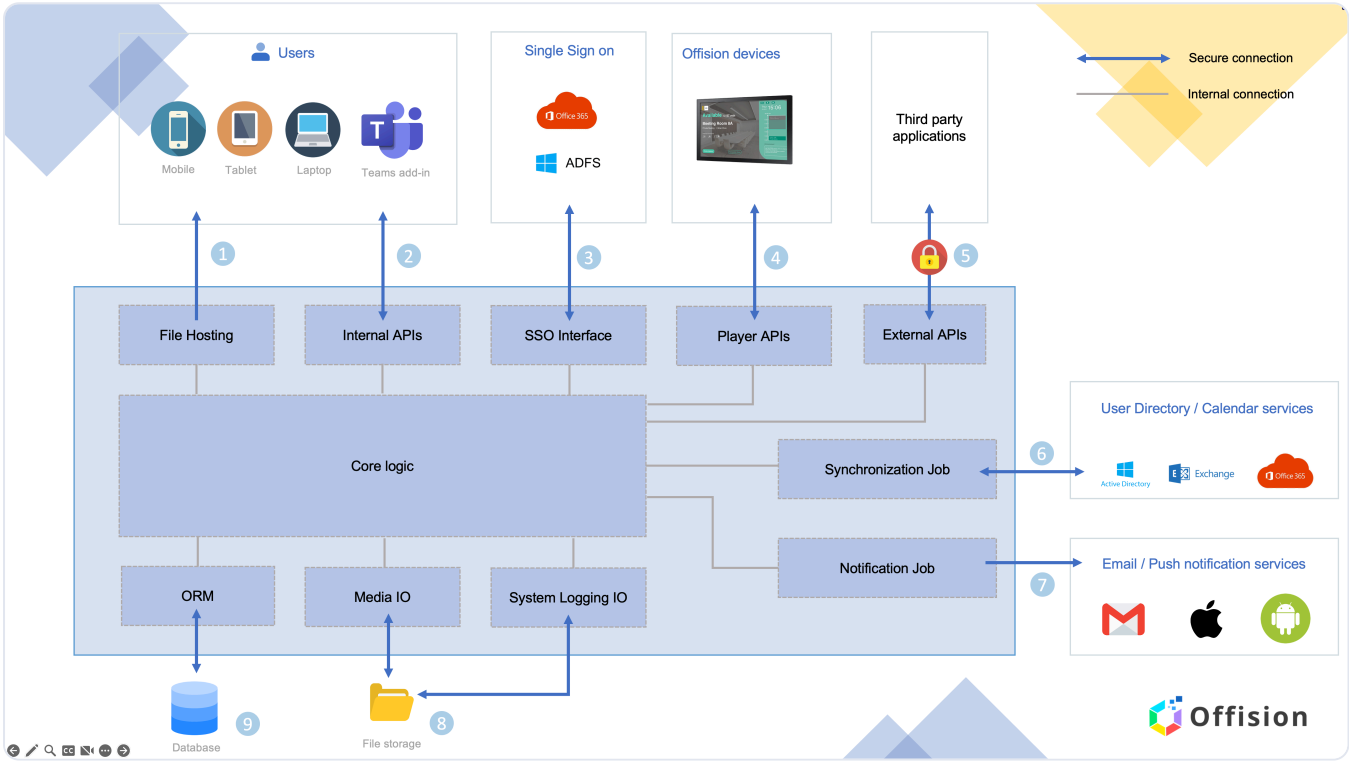
- **Microsoft Azure data centres.** All production compute, database, and storage are hosted in Microsoft Azure (§5.3).
- **High availability across three Japan data centres.** Production workloads run simultaneously across three Microsoft Azure data centres in Japan, eliminating any single point of failure (§9.2).
- **Per-tenant database isolation.** Each customer's data lives in its own logical database; tenants do not share schema or rows, so there is no application path that can return another tenant's data (§5.2).
- **Encryption at rest (TDE).** All databases are protected with Transparent Data Encryption, so the underlying storage is encrypted on disk (§8.3).
- **Point-in-time recovery (PITR).** Databases are continuously backed up so customer data can be restored to any moment within the configured retention window (§8.5).
- **Azure Firewall and network controls.** External network access is gated by Azure Firewall and the Azure platform's network security controls; only intended public surfaces are exposed (§9.3).

- **HTTPS everywhere.** Every connection to Offision — from user browsers, mobile apps, Players, and third-party integrations — is served over HTTPS with TLS (§8.2).

The remainder of this section describes the logical components, data flow, multi-tenant isolation, and hosting region in detail.

5.1 Logical architecture and data flow

The Offision Cloud SaaS service is a multi-tier application. Users interact with it through several front-end surfaces, each of which reaches a corresponding back-end API surface in the Microsoft Azure-hosted production environment. Offision is a smart office platform that integrates with a wide range of third-party services and interfaces, and protecting data as it crosses these boundaries is a primary design concern. The diagram below shows how Offision routes and protects data across each component, preventing unintended external exposure.



User-facing surfaces:

- **Management Console** — administrator interface for tenant configuration, user lifecycle, role assignment, and integration setup.
- **User App** — end-user application for booking rooms, desks, and parking, raising service requests, and similar workflows. Available as a web application and as mobile applications.
- **Visitor App** — receptionist and visitor flows used at front-desk kiosks and on visitor devices.
- **Microsoft Add-in** — enables end users to view and create bookings from within Microsoft Outlook, Microsoft Teams, and the Microsoft 365 web apps.
- **Offision Players** — physical endpoint devices including room display panels, desk display panels, e-paper room tags, lockers, and check-in kiosks.

Back-end surfaces (described in detail in §10):

- **Internal API** — authenticated user-facing application API consumed by the User App, Management Console, Visitor App, and Microsoft Add-in.
- **Player APIs** — restricted API surface for enrolled Offision Players.
- **External API** — third-party integration API; off by default.
- **SSO Interface** — receives identity-provider assertions and translates them into authenticated sessions for the Internal API.
- **Synchronization Jobs** — read-only ingestion of directory and calendar data from Microsoft 365, Exchange Server, and Active Directory.
- **Notification Jobs** — outbound notifications (SMTP email, web push, mobile pass).
- **File Hosting** — static assets (HTML, scripts, stylesheets, images) used to render the user interfaces; contains no user, booking, or configuration data.
- **File / object storage** — uploaded media and system logs.
- **ORM-managed database** — sole persistence layer for application data.

Two architectural choices are worth highlighting:

- **Static and dynamic content are separated.** The HTML, scripts, stylesheets, and images that render the user interfaces are served from the File Hosting tier, which contains no user, booking, or configuration data. All sensitive data is reached only through authenticated calls to the API tiers (Internal, Player, External) and the SSO Interface.
- **API surfaces are bounded by audience and trust level.** The Internal API is reached only by Offision's own user-facing applications and is gated by per-user authentication and authorization (§10.1). The Player APIs are reached only by enrolled Offision Players (§10.2). The External API is reached only by third-party systems for which an administrator has explicitly enabled the API and provisioned an access token (§10.3). The SSO Interface accepts only assertions issued by configured identity providers (§10.4).

The flow of data through the Offision service follows the nine-component model documented in the Offision data flow reference. Each component has an associated security characteristic.

1. **File Hosting** — serves the static assets used to render the user interface. Contains no user, booking, or configuration data.
2. **Internal API** — accessible only to authenticated users. Per-request authorization is further constrained by the user's identity and assigned permissions, so high-privilege endpoints are unreachable from low-privilege accounts (§10.1).
3. **SSO Interface** — receives the assertion from a configured identity provider, validates it, and hands the resulting authenticated session to the Internal API (§10.4).
4. **Player APIs** — reachable only by enrolled Offision Players under the player security policy (§10.2).
5. **External APIs** — disabled by default. Each customer environment must be explicitly configured by an administrator before any External API calls are accepted. Authentication and access controls are described in §10.3.

6. **Synchronization Jobs** — read-only consumption of directory and calendar data from Microsoft 365, Exchange Server, and Active Directory. Synchronization scope follows the credentials and policies configured in the source system (§10.5).
7. **Notification Jobs** — outbound only (SMTP email, web push, mobile pass). Notification content is restricted to data already visible to the recipient (§10.6).
8. **Media IO / System Logging IO** — uploaded media and system logs are written to the configured object-storage backend (§11.1).
9. **ORM** — the database, accessed exclusively through an object-relational mapper, is the sole persistence layer. The application does not retain operational data outside the database.

5.2 Multi-tenant isolation

Offision is deployed in a multi-tenant configuration with **dedicated-database-per-tenant** isolation. Each customer is assigned its own logical database; tenants do not share schema or rows.

- **No cross-tenant data path.** There is no application path that joins or references a different tenant's database. Even a defective query in the application cannot return rows from another tenant's database, because no such row is reachable from the connection that serves the request.
- **Independent scaling and tuning.** Per-tenant databases can be scaled independently, allowing performance characteristics to be tuned per tenant.
- **Per-tenant export and deletion.** Data export and deletion operate on a single database, which makes tenant offboarding deterministic.
- **Per-tenant backup and restore.** Backups are scoped per database, so a restore operation affects only the tenant being restored. The same applies to retention and secure deletion (§8.5): when a tenant's data is destroyed, its database and the corresponding backups are destroyed without touching any other tenant.

5.3 Hosting and regions

Offision Cloud SaaS production data is hosted on **Microsoft Azure** in the **Japan East** region. Compute, database, and primary storage for each customer environment are deployed within Japan East. Backups are kept in storage operated alongside the primary region (§8.5, §12.2).

The static-asset layer (File Hosting; §5.1) is delivered through a content-delivery configuration optimised for performance. Because the static layer contains no customer data — only the fixed UI bundle that is identical for every user — delivery from globally distributed edges does not change the data-residency posture of the service.

Hosting in a Microsoft Azure data centre brings Microsoft-maintained physical-security and platform attestations under ISO 27001, ISO 27018, and SOC 1, SOC 2, and SOC 3 (§4.2).

The current public-facing Privacy Policy refers to "servers located in Hong Kong"; this wording predates the current hosting arrangement and is scheduled to be updated. The current authoritative statement on the production hosting region is the one in this white paper.

---

6. Identity and Access Management

6.1 End-user authentication

Offision supports the following authentication methods for end users:

- **Local password authentication.** Users authenticate against the Offision identity store with a username and password. Password policy (length, complexity, reuse, lockout) is configurable by the customer's administrator.
- **SAML 2.0 Single Sign-On.** Offision can be registered as a service provider against a customer-operated identity provider (for example, ADFS or other SAML 2.0-compatible IdPs).
- **OpenID Connect with Microsoft 365.** Users sign in with their Microsoft 365 account; Offision consumes the resulting OpenID Connect token via the SSO Interface (§10.4).

Multi-factor authentication is supported in two complementary modes:

- **Native MFA** — for accounts authenticating against the Offision local password store, MFA is enforced by Offision itself.
- **IdP-delegated MFA** — when SAML 2.0 or OpenID Connect is used, MFA is enforced at the customer's identity provider, and the resulting authenticated assertion is consumed by Offision's SSO Interface.

Customers can therefore either rely on Offision's built-in MFA or centralise MFA policy at their existing identity provider, depending on their identity strategy.

Authentication outcomes (sign-in success, failure, lockout) are recorded in the application logs (§11.1). Repeated failed authentication attempts against the local password store are subject to throttling and lockout under the configured policy.

6.2 Role-based access control

Offision applies role-based access control (RBAC) backed by a fixed set of predefined roles:

- **Administrator** — full administrative access to the tenant, including user lifecycle, role assignment, and integration configuration.
- **Staff** — operational roles with broader access than end users, used for facilities, HR, and similar functions depending on configuration.
- **User** — end-user access, scoped to the user's own bookings and visible workspace data.

Each role is associated with a set of granular permissions that scope access to features, modules, and data. The model is designed so that role assignment alone is sufficient to deliver least privilege; per-user permission overrides are not required for routine operation.

Permissions are evaluated at every API call (§10.1), so a user who attempts to call a high-privilege endpoint with a low-privilege account is rejected at the API layer, regardless of the path used to reach the endpoint.

6.3 Provisioning and deprovisioning

User provisioning and deprovisioning is supported through two mechanisms:

- **Directory synchronization.** Synchronization Jobs (§5.1 step 6, §10.5) bring user records and calendar data from configured systems (Microsoft 365, Exchange Server, Active Directory) into Offision under the source system's permissions.
- **External API user-management endpoints.** Administrative tooling can manage users through the External API `User` group (§10.3). Available operations include `Invite a new user`, `Invite a new user for an integration client`, `Deactivate user by id`, `Activate user by id`, `Delete user by id`, `Assign a license to a user`, `Unassign a license from a user`, `Set an access card for a user`, and `Remove an access card from a user`. Group memberships are managed through the External API `UserGroup` group.

Either mechanism can be used to keep the Offision user directory aligned with the customer's authoritative source of identity. When a user is deactivated or deleted, their interactive session and any externally issued access tokens scoped to that user lose their authorised state.

6.4 Administrative access and least privilege

ONES Software personnel access to a customer's Offision environment is not automatic or persistent. Such access is granted only when:

- the customer has given explicit consent (for example, in support of a troubleshooting case), or
- access is required to maintain the integrity of the production system,

and is restricted, audited, and time-bounded for the duration of the activity. The default state is that no internal personnel hold standing access to a customer environment.

Where access is granted, it is recorded against the consenting customer ticket or the system-integrity event that authorised it, expires when the activity completes, and is reviewed under the ISMS.

---

7. Application Security

7.1 Secure development lifecycle

Offision is developed under a documented secure-development lifecycle. Security activities are integrated into the engineering workflow rather than applied as a separate audit at the end of a release. The lifecycle covers:

- **Requirements review** — security input on changes that touch authentication, authorization, data classification, or external interfaces.
- **Internal secure-coding standards** — applied across the engineering team and reinforced through peer review (§7.2).
- **Security training** — engineers receive training on common application risks and on Offision-specific patterns.
- **Pipeline-integrated security checks** — automated scans run as part of the development pipeline (§7.3) and gate code changes through environment promotion (§7.4).

7.2 Peer review and quality framework

Code changes are reviewed by at least one peer engineer before they are merged. The review covers:

- **Correctness** — does the change implement what was intended?
- **Security implications** — input validation, authentication checks, authorization checks, secrets handling, error handling, and data exposure.
- **Adherence to internal coding standards.**

Review and merge activity is recorded in the source-control system, providing an audit trail of who approved what.

A quality framework with automated tests gates code changes through environment promotion. Releases progress through development and pre-production environments before reaching production; a change that fails the quality framework cannot be promoted.

7.3 Vulnerability assessments

Offision is subject to both automated and manual vulnerability assessment activity:

- **Automated scanning** — the application and its third-party dependencies are scanned as part of the development pipeline. Findings are surfaced into the engineering backlog.
- **Manual review** — peer code review (§7.2) acts as a manual layer; it is supplemented by periodic deeper security assessments.
- **Annual third-party security audit.** Offision commissions an independent third-party security audit on an annual cadence, conducted by **MSX**. The most recent audit was completed in **April 2026**. Findings from each audit are tracked to remediation under the ISMS (§4).

Identified vulnerabilities are prioritised and tracked through to remediation under the ISMS (§4). The categories tracked typically follow the OWASP application-security risk taxonomy (broken access control, injection, cryptographic failures, security misconfiguration, vulnerable and outdated components, identification and authentication failures, etc.) together with vulnerabilities reported in third-party dependencies.

7.4 Release management and staged deployments

Releases are produced on a regular cadence covering both security and functional changes. Each release is validated in non-production environments before deployment to production; the deployment workflow is designed to support **rollback** if a release surfaces a regression.

For changes that are scoped narrowly enough, deployments may be progressive (only a subset of the production estate is updated in the first wave) so that any regression can be detected before the change is applied everywhere.

---

8. Data Protection

8.1 Data classification

The data Offision processes falls into the following categories:

- **Configuration data** — tenant-level configuration, including policies, role definitions, building/floor/resource definitions, and integration settings.
- **User-directory data** — user records (identity, contact details, employer/position when accessed via a Company Subscription, optional access-card mappings).
- **Booking and calendar data** — bookings, meeting metadata, attendees, and resource appointments.
- **Visitor records** — visitor identity, host details, and visit status (including QR-code-based identifiers used for visitor access; §10.7).
- **Uploaded media** — files uploaded by users (for example, attached to bookings or service requests).
- **Application and system logs** — operational logs written by the service for monitoring, audit, and troubleshooting.

The protection level applied to each category is described in §8.2 (in transit), §8.3 (at rest), §8.4 (passwords and tokens), and §8.5 (backups, retention, and deletion).

8.2 Encryption in transit

All client-to-service and integration traffic is carried over HTTPS. Plain HTTP requests are automatically redirected to HTTPS. API requests that arrive without authentication are rejected with HTTP 401.

This applies to:

- Browser, mobile, and Microsoft Add-in traffic between user agents and the Offision service.
- External API calls from third-party integrations (§10.3).
- Player API traffic from enrolled Offision Players (§10.2).
- Outbound traffic from Offision to customer-configured destinations: Notification Jobs (§10.6) and outbound webhooks (§10.8).

Within the Microsoft Azure environment, traffic between Offision's own service tiers traverses the Azure platform's network. Outbound TLS connections (Notification Jobs and webhooks) require the receiving system to be addressable over HTTPS with a valid certificate.

8.3 Encryption at rest

Customer data is encrypted at rest using the platform-level encryption applied by the underlying Microsoft Azure storage services. Encryption applies to:

- The relational database that holds tenant data via the ORM (§5.1 step 9).

- Object storage used for uploaded media and system logs (§5.1 step 8).
- Backup copies (§8.5).

Encryption is transparent to the application: data is encrypted when written and decrypted when read, with key material managed by the Microsoft Azure platform.

8.4 Password storage and token-based authentication

End-user passwords are stored as **one-way hashes** rather than in reversible form. Plain-text passwords are not retained anywhere in the service.

Interactive sessions and API access use **token-based authentication**:

- Interactive user sessions are bound to a server-issued session token, which is invalidated on sign-out and on session timeout.
- External API access is bound to an access token issued from the Management Console (see §10.3); each token can be expired, IP-restricted, and rotated independently.

The session token is bound to the user's authenticated session and does not by itself contain sensitive personal data. External API tokens are scoped per administrator-issued credential.

8.5 Backups, retention, and secure deletion

Offision runs **continuously automated backups**. Backups are written to secure off-site storage operated alongside the primary Azure region; backup access is controlled and backups themselves are encrypted at rest in line with §8.3. When the retention window expires, backups are permanently destroyed.

In line with the Offision Privacy Policy, personal data associated with a customer Subscription is deleted or anonymised within two months of the expiry or termination of the Subscription, except where a legal, statutory, regulatory, or accounting obligation requires longer retention. When a tenant is deleted, the corresponding database and its backups are destroyed; because tenants are isolated in dedicated databases (§5.2), the destruction does not affect any other tenant.

9. Infrastructure and Cloud Security

9.1 Azure data-centre physical security

Physical security controls for the data centres that host Offision are operated by Microsoft as part of the Microsoft Azure platform. They cover access control to the facility, video surveillance, intrusion detection, fire suppression, environmental controls (power, cooling), and the destruction of decommissioned media. The control set is independently certified to ISO 27001, ISO 27018, and SOC 1, SOC 2, and SOC 3, and is described in Microsoft's published compliance material (see §16).

ONES Software does not operate any of its own data centres for the Offision Cloud SaaS service.

9.2 Redundancy and availability

Offision is deployed across **multiple Microsoft Azure data centres** in a triple-redundant configuration. The redundant configuration removes the data centre as a single point of failure: the loss of one data centre does not, on its own, take the service down.

The service targets **99.9% availability**, supported by 24/7/365 monitoring (§11.2). Recovery point and recovery time targets, and the cadence of disaster-recovery exercises, are described in §12.

9.3 Network architecture and content delivery

Offision separates content delivery from data access:

- **Static front-end assets** (HTML, scripts, stylesheets, images) are delivered through a content-delivery configuration optimised for performance. These assets are identical for every user and contain no customer data (§5.1, §5.3).
- **Dynamic data access** is handled by the Internal, Player, and External APIs and the SSO Interface — all of which are gated by authentication and authorization (§10).

Within Azure, the API tier and the data tier (database and object storage) are segmented so that data-tier resources are not directly exposed to public networks. A request from a client reaches the database only by passing through the application's authorization-checked code path.

9.4 Continuous monitoring and threat detection

Offision's production estate is monitored continuously. Monitoring activities include availability and performance telemetry, application and platform-level logs (§11.1), and threat-detection signals from the Microsoft Azure platform. Maintenance is scheduled to address vulnerabilities that surface from internal scanning (§7.3) and from external advisories.

10. Integrations and API Security

10.1 Internal APIs

The Internal API is the application API consumed by Offision's own user-facing surfaces (User App, Management Console, Visitor App, Microsoft Add-in).

- **Authentication.** Internal API calls require a valid session token issued at sign-in (§6.1) — either through the local password store or via the SSO Interface (§10.4).
- **Authorization.** In addition to authentication, every call is authorised against the user's identity and assigned permissions (§6.2). Endpoints that require an Administrator or Staff permission cannot be reached from a User-role account, regardless of how the call is constructed.
- **Transport.** All Internal API traffic is HTTPS-only (§8.2).

10.2 Player APIs and player device enrolment

Player APIs serve Offision's physical endpoint devices — room display panels, desk display panels, e-paper room tags, lockers, and check-in kiosks. They are a distinct API surface, separate from the Internal and External APIs, and are reachable only by Offision's official Players.

- **Endpoint segregation.** Other API surfaces (Internal API, External API, SSO Interface) cannot accept Player API calls, and vice versa.
- **Enrolment.** Players are bound to a tenant through an enrolment process initiated from the Management Console.
- **Ongoing authentication.** Once enrolled, a Player presents its issued credential on every API request, allowing only the registered device to send and receive data.
- **Transport.** All Player API traffic is HTTPS-only (§8.2).

10.3 External APIs

The Offision External API is the surface used by third-party systems for integration scenarios such as IoT-sensor ingest, access-control integration, and analytics. The External API is **off by default** in every customer environment; an administrator must explicitly enable and configure it before any calls are accepted.

- **Transport.** All API requests must be made over HTTPS. Plain HTTP is auto-redirected to HTTPS. Requests without authentication return HTTP 401.
- **Authentication.** Authentication uses an **API access token** issued from the Management Console under `Integration → API authentication`. The access token is presented either as the username in HTTP Basic Auth (the password field is left empty) or as a Bearer token in the `Authorization` header.
- **Token issuance and storage.** Access tokens are shown **once at generation** and are not retrievable afterwards. If the token is lost, a replacement token must be generated.

- **Per-application tokens.** When a customer integrates more than one application, ONES Software recommends issuing a **separate token per application** rather than reusing a single token across applications. This way tokens can be rotated independently and revocation has a smaller blast radius.
- **Source-IP allowlisting.** Each token can be restricted to a list of allowed source IP addresses. Supported formats include single addresses (e.g., `225.154.33.1`), inclusive ranges (`225.154.33.1–100`), comma-separated lists (`225.154.33.3, 225.154.33.100`), and CIDR notation (`225.154.33.0/24`).
- **Configurable expiry.** Each token can be configured with an expiry, after which it stops being accepted.

The External API exposes endpoints across functional groups including `Analyze`, `BookableResource`, `BookableResourceAccessKey`, `BookableResourcePlayerContent`, `Booking`, `Building`, `Dashboard`, `EnvironmentSensor`, `EPaperController`, `Locker`, `OccupancySensor`, `ServiceItem`, `System`, `User`, `UserGroup`, `VisitingAppointment`, `VisitorManagement`, and `WorkflowWebhook`. The full list is documented in the External API reference.

10.4 SSO interface

The SSO Interface is the entry point used by SAML 2.0 and OpenID Connect sign-in flows (§6.1). Its responsibility is to receive the assertion or token issued by the customer's identity provider, validate it (signature, audience, expiry, replay, issuer), and produce an authenticated session that is then handed to the Internal API.

The SSO Interface does not consume credentials directly; it consumes only IdP-issued artefacts. It does not sign in users that are unknown to the Offision tenant — the user must already exist in the tenant's directory (provisioned via Synchronization Jobs or via the External API user-management endpoints; §6.3).

10.5 Synchronization jobs

Synchronization Jobs are background read-only consumers that bring user, group, and calendar data into Offision from external systems. Supported sources are:

- **Microsoft 365** (user accounts, calendars).
- **Microsoft Exchange Server** (calendars, including on-premises configurations).
- **Active Directory** (user accounts, groups).

Synchronization is scoped by the credentials and policies configured on the source system: Offision can only read what the source system permits the synchronization principal to read. Offision does not write back to the source system; if a customer wants to make changes in the source system based on Offision activity, that is a customer-side integration.

10.6 Notification jobs

Notification Jobs are background outbound producers that deliver event notifications to users. Supported channels are:

- **SMTP email** (booking confirmations, visitor invitations, service-request updates, reminders, and similar).
- **Web push** (browser-based push notifications to subscribed users).
- **Mobile pass** (notifications via the Offision mobile applications).

Notification content is restricted to data that is already visible to the recipient. Offision does not include data in notifications that the recipient is not entitled to see in the application itself.

10.7 Access-control integrations

Offision supports two integration patterns with physical access-control systems.

Room access

Room access is driven by booking events:

- The customer's access-control middleware **subscribes to booking changes** via the External API (`POST` to the `Subscribe resource appointment change` endpoint), supplying a callback URL that Offision will call when a booking is created, updated, or cancelled.
- The middleware is responsible for two customer-maintained mappings:
  - **Bookable resource ID → access-control unit** — so that a booking change can be translated into the right physical door, gate, or boom barrier.
  - **User email → access-card number** — so that the access-control side can identify the user when the user presents their card.
- When a booking change is signalled, the middleware updates the access-control unit's accessibility for the relevant time window and, if needed, fetches the daily booking list (`Get bookable resource daily booking list`) for the resource.

For richer access-key scenarios, three additional subscription channels are available:

- `Subscribe to daily access key changes` — daily-grain access keys.
- `Subscribe to one-time access key changes` — single-use keys.
- `Subscribe to player content changes` — for Player-mediated workflows (kiosks, panels) that depend on access-key state.

Visitor access

Visitor access is driven by **QR-code verification**:

- When a visitor is registered, Offision issues a QR code as part of the visitor badge or invitation email.
- At the access-control point (gate, reception turnstile), a scanner reads the QR code and queries the External API's `VisitorManagement` endpoints to retrieve visitor information and current visiting status (checked-in, checked-out, etc.).
- The access-control side allows or denies entry based on that status.

10.8 Outbound webhooks

Two channels exist for Offision to send outbound HTTP callbacks to customer-supplied URLs.

- `WorkflowWebhook` — workflow triggers fired via a webhook key. Supports `POST`, `GET`, `PUT`, and `DELETE` methods.
- **Booking change subscriptions** — the access-control subscription pattern described in §10.7: `Subscribe resource appointment change`, `Subscribe to daily access key changes`, `Subscribe to one-time access key changes`, and `Subscribe to player content changes`.

Common controls:

- **Transport.** Outbound calls are made over HTTPS. The customer-supplied URL must be reachable over HTTPS with a valid TLS certificate.
- **Endpoint configuration.** The customer-side URL is configured in the External API call that creates the subscription, or in the Management Console for `WorkflowWebhook` keys.
- **Customer responsibilities.** The receiving endpoint must respond with a 2xx status code in the receiver's expected window. Where Offision provides a signing scheme or shared secret, the customer is responsible for keeping that secret confidential, validating the signature on every received call, and validating any timestamp header against a sensible tolerance window. See §14 for the customer-responsibility checklist.

10.9 API rate limiting

External and Internal API consumption is subject to rate limits to protect service availability and prevent abuse. Limits are applied at multiple levels (per token, per endpoint, per tenant). When a limit is exceeded, the response indicates the limit condition; clients should respect the response and back off accordingly.

The current default thresholds are:

Surface	Limit
Internal API (per user)	100 requests / 5 seconds
External API (per integration token)	1,000 requests / 5 seconds

Thresholds may be tuned over time. Integrators that need adjusted limits or finer-grained quotas can request them through the API support channel (`hello@offision.com`).

11. Logging, Monitoring, and Incident Response

11.1 Application and audit logging

Offision writes logs covering several categories:

- **Application logs** — operational events emitted by the application during normal operation (request handling, integration calls, scheduled jobs).
- **System logs** — platform-level events (startup, shutdown, recurring jobs, configuration changes).
- **Audit-relevant events** — authentication outcomes (sign-in success, failure, lockout), changes to roles and permissions, External API token issuance, and similar privileged operations.
- **Media-IO logs** — events associated with file uploads and downloads (§5.1 step 8).

Logs are written to the configured storage backend (§5.1 step 8). The exact list of audited event types, the log-retention period, and customer access to audit logs are made available to enterprise customers through contract review.

11.2 Operational monitoring

The Offision production estate is monitored 24/7/365. Availability and performance telemetry, error-rate metrics, and platform-level signals are consolidated into operational dashboards. Anomalies and threshold breaches surface alerts that route to the on-call team. Monitoring runs continuously, including outside business hours.

11.3 Incident response process

Offision operates a security incident-response process under the ISMS. The process covers:

- **Detection** — alerts from the monitoring stack (§11.2), customer reports, internal staff reports, and threat-intelligence signals.
- **Triage** — initial assessment of severity and scope.
- **Containment** — actions to limit the spread or impact of the incident.
- **Eradication** — removal of the root cause.
- **Recovery** — restoration of normal service.
- **Lessons learned** — post-incident review and updates to controls and processes.

Where an incident affects customer data, the affected customers are notified in line with applicable contractual and regulatory obligations. Notification timelines, regulatory-notification commitments, and the post-incident report format are made available to enterprise customers through contract review.

12. Business Continuity and Disaster Recovery

12.1 Redundancy posture

Offision is deployed redundantly across Microsoft Azure data centres (§9.2). The redundant configuration removes the data centre as a single point of failure: the loss of one data centre does not, on its own, take the service down.

12.2 Backup strategy and off-site storage

Backups run continuously rather than on a daily schedule. They are written to off-site secure storage with controlled access, are encrypted at rest in line with §8.3, and are integrity-protected. When the retention window expires, backups are permanently destroyed (§8.5).

12.3 RPO and RTO targets

Recovery-point and recovery-time targets, the cadence of disaster-recovery exercises, and the date of the most recent exercise are made available to enterprise customers through contract review.

13. Privacy and Data Protection

13.1 Applicable law

ONES Software is established in the Hong Kong Special Administrative Region. Personal-data processing complies with the **Personal Data (Privacy) Ordinance (Cap. 486)** of the laws of Hong Kong.

For users in the **European Economic Area**, the Privacy Policy provides additional rights under the General Data Protection Regulation (GDPR), including erasure, objection, portability, restriction of processing, withdrawal of consent, and the right to lodge a complaint with a national supervisory authority. The lawful bases used are Contract Performance, Legitimate Interests, Consent, and Legal Obligation, as set out in §15 of the Privacy Policy.

Alignment with other regulatory regimes (for example, the U.S. CCPA, Brazil's LGPD, or industry-specific regimes such as HIPAA) is made available to enterprise customers through contract review.

13.2 Personal data categories collected

As set out in the Offision Privacy Policy §1, Offision may collect the following categories of personal data:

- **Identity and contact details** — title, name (first and last), mobile phone number, email address.
- **Employer-related data** — when the user accesses Offision through a Company Subscription, the user's employer/company and position.
- **Credentials** — username and password.
- **Payment information** — credit-card information, billing address, particulars of any third-party payment account; financial information may also be collected from payment-gateway providers.
- **Technical metadata** — IP address, MAC address, mobile-carrier-related information, browser settings, and other internet log-on information from the user's device.
- **Real-time location data** — only for location-enabled functions, only on the user's consent, and revocable by disabling the relevant function.
- **Usage analytics** — date and time of access, frequently used services, browsing records, referring websites.
- **Communication preferences** — opt-in choices for marketing material.

Offision **does not** collect personal data on **children** and **does not** collect special categories of personal data, including data on race or ethnicity, religious or philosophical beliefs, trade-union membership, sex life, sexual orientation, political opinions, health, genetic and biometric data, or criminal convictions.

13.3 Purposes of processing

Personal data is processed for the purposes set out in the Privacy Policy §4, which include:

- Creating and administering user accounts.

- Verifying user identity.
- Providing the service.
- Identifying and auditing users' use of the service.
- Processing billing and payment.
- Service-job alerts and notifications.
- In-app chat between designated parties.
- Backup and retrieval of user data.
- Two-factor authentication.
- Customer support and communication.
- Service analytics and improvement.
- Notifying users of changes to terms or policies.
- Marketing materials (only on consent; revocable at any time).
- Maintaining records.
- Detecting, investigating, and preventing fraud and other illegal activities.
- Meeting legal, regulatory, and compliance requirements.

Where personal data is to be used for a purpose unrelated to those set out above, the user is notified and consent is obtained.

13.4 Cross-border transfers

Offision Cloud SaaS production data is processed and stored in **Microsoft Azure's Japan East region** (§5.3).

ONES Software's support, engineering, and other operational teams that support the service are located in multiple jurisdictions, and may access customer data from those locations as necessary to provide the service. Where ONES Software shares personal data with service providers (sub-processors) in support of the purposes set out in §13.3, those service providers are bound by confidentiality obligations and are authorised only to use the data as necessary to perform services on ONES Software's behalf.

For users in the EEA, additional safeguards (such as contractual clauses) are applied to transfers that leave the EEA, as set out in the Privacy Policy §15.B.

The current public-facing Privacy Policy refers to "servers located in Hong Kong"; this wording predates the current Azure Japan East hosting arrangement and is scheduled to be updated. The current authoritative statement on the production hosting region is the one in this white paper.

13.5 Data subject rights

Under the Personal Data (Privacy) Ordinance, every user has the right to:

- **Access** the personal data that Offision holds about them.
- **Correct** personal data that is inaccurate or incomplete.

Users in the EEA have additional rights under the GDPR (Privacy Policy §15.D), including:

- **Erasure** of their personal data where there is no good reason for continued processing.
- **Objection** to processing based on legitimate interests.
- **Portability** in a structured, commonly used, machine-readable format.
- **Restriction** of processing in defined circumstances.
- **Withdrawal of consent** for any processing based on consent.
- Reconsideration of automated decisions, where applicable.
- Lodging a complaint with a national supervisory authority.

Requests are made to the **Data Privacy Officer** at `hello@ones.software`. Identity verification is required before requests are processed. Standard EEA requests are handled within 30 days.

13.6 Retention and deletion

Personal data is retained for as long as necessary to fulfil the purposes set out in §13.3. Subject to legal, statutory, regulatory, or accounting obligations that mandate longer retention, Offision endeavours to **delete or anonymise personal data within two months** of the expiry or termination of a Subscription (Privacy Policy §7).

When the retention window expires, the underlying data is removed from the database and the corresponding backups (§8.5).

13.7 Data Processing Addendum and contractual data-protection terms

Customers that require formal data-processing terms beyond the Privacy Policy can request:

- A **Data Processing Addendum** that incorporates the controller-to-processor framing already implicit in the Privacy Policy.
- The **cross-border-transfer mechanisms** appropriate to the customer's jurisdiction (for example, the EU/UK Standard Contractual Clauses for EEA data flows).
- **Sub-processor change notification** when ONES Software adds, replaces, or removes a sub-processor that processes their data.

The exact wording, signing process, and notification cadence are made available to enterprise customers through contract review.

14. Customer Responsibilities

This section consolidates the controls that remain the customer's responsibility under the shared-responsibility model described in §3.

Identity and access

- Configure the identity provider (SAML 2.0 / OpenID Connect) used for SSO and decide whether MFA is enforced at the IdP or natively in Offision (§6.1).
- Maintain password policy where local authentication is in use.
- Assign roles consistent with each user's job function; periodically review role assignments and remove standing access that is no longer needed.
- Deprovision users promptly when they leave the organisation, either through directory synchronization or through the External API user-management endpoints (§6.3).

Integrations

- Generate External API access tokens with the smallest scope appropriate to the use case; restrict each token by source IP where the integration's network position allows; set a configurable expiry; rotate tokens periodically (§10.3).
- Use a **separate token per integrating application** rather than reusing one token across applications.
- Maintain customer-side mappings used by access-control integrations: email-to-card-number and bookable-resource-ID-to-access-control-unit (§10.7).
- For visitor access, ensure that QR-code scanners at access-control points have appropriate connectivity to the External API `VisitorManagement` endpoints (§10.7).

Endpoint and credential security

- Treat the Management Console and User App credentials with the same care as other administrative and end-user credentials. Where MFA is delegated to the IdP, ensure MFA is actually enforced for the relevant population.
- Maintain endpoint security on the devices used to access Offision (browsers, mobile devices, the Microsoft Add-in host).

Privacy obligations

- Notify internal users when personal data is shared with Offision, as required by applicable privacy laws (Privacy Policy §1).
- For EEA users, ensure that the lawful bases set out in the Privacy Policy §15.C apply to the customer's planned use of the service.

Network egress and webhook receivers

- Allow outbound HTTPS from end-user devices, Management Console clients, the Microsoft Add-in, the Visitor App, and Offision Players to the Offision service hostnames and IP ranges.

- For customer-operated webhook receivers (`WorkflowWebhook` or booking-change subscriptions): publish HTTPS endpoints with valid TLS certificates; keep any shared secrets confidential and rotate them periodically; validate signatures and timestamps where Offision provides them; respond promptly with a 2xx status code (§10.8).

---

15. Responsible Disclosure and Security Contact

Security inquiries and vulnerability reports can be sent to ONES Software through the public contact channels below.

- **General contact:** `hello@offision.com`.
- **Integration support:** `support@bookings.one`.

Security researchers and customers who believe they have found a vulnerability in Offision are asked to send a description of the issue, the steps to reproduce it, and any supporting material (logs, screenshots, network captures) to the contact channels above. ONES Software acknowledges responsible-disclosure reports and tracks them through to remediation under the ISMS (§4, §7.3, §11.3).

The full responsible-disclosure programme details — including any safe-harbour terms, scope, and acknowledgement timelines — are made available on request.

---

16. References

- Offision External API — https://offision.com/help/external-api/
- Offision Privacy Policy — https://www.offision.com/privacy

17. Disclaimer

This document is provided for informational purposes only. It describes Offision's security and privacy controls as of the publication date and may be used by recipients for internal reference and procurement review.

The information in this document is believed to be accurate but is presented without warranty of any kind, express or implied. ONES Software Limited makes no representation or warranty regarding the suitability of the information described here for a particular purpose. The product specifications, capabilities, and the controls described are subject to change without notice; the version, date, and authoritative source of every statement are reflected in the Change History at the top of this document and the source citations within each section.

This document does not convey any legal rights to any intellectual property of ONES Software Limited or its licensors, and does not create or modify any contractual obligation between ONES Software and any reader. Where a contract or addendum (for example, a Master Subscription Agreement, a Data Processing Addendum, or a Service Level Agreement) covers a topic also discussed here, that contract or addendum prevails.