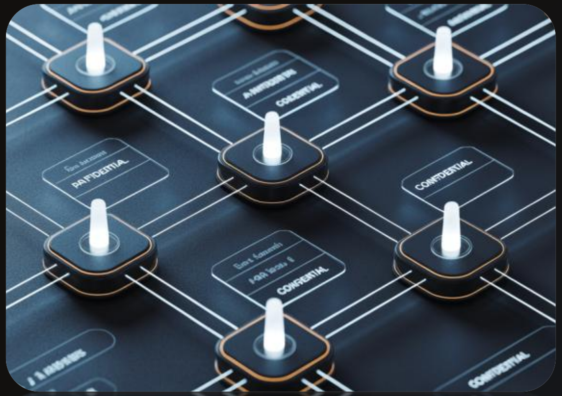
Offision

Connected Workplace Experience

Introduction

Cloud Infrastructure and Security

Secure, scalable, and high-performance infrastructure leveraging cloud technologies to ensure data protection, availability, and compliance.



Data flow

We place the highest priority on ensuring data protection throughout every stage of these integrations.

Cloud Security

Offision runs on a robust, scalable cloud infrastructure, ensuring high performance, availability, and security

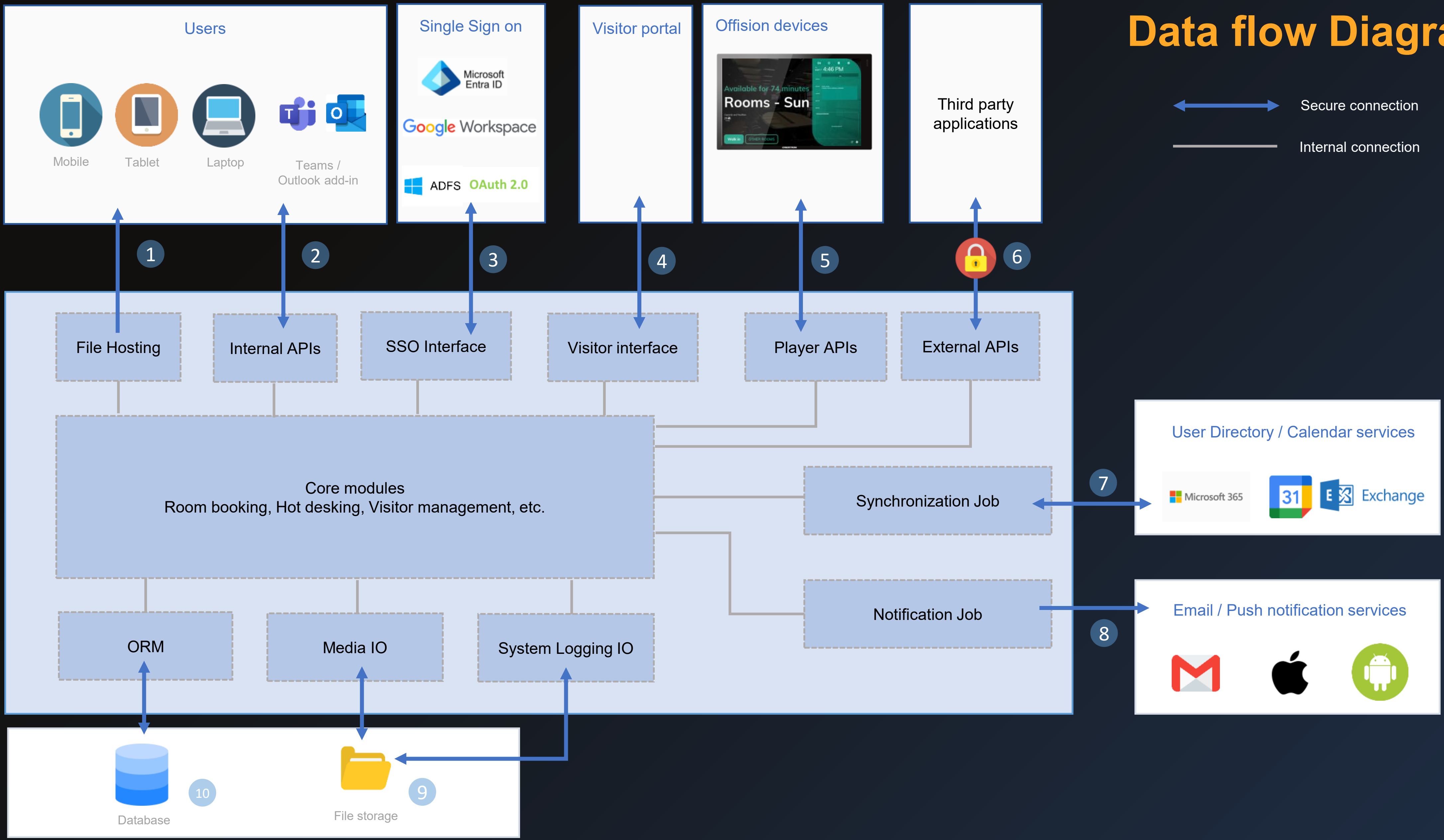
Secure development workflow

A development process that embeds security at every stage to prevent vulnerabilities.

Data flow

Offision are powerful as smart office system and able to integrate with various 3rd-party integration and interfaces, data protection within integration is one of the most important part we highly concern.

Data flow Diagram



CORE COMPONENTS

Secure Data Flow and Integration

1

File Hosting & UI

Hosts static files (HTML, scripts, stylesheets, images) for user-facing facing applications (User portal, User APP, Management Console, Visitor Visitor App, Outlook Add-in). Files are fixed, identical for all users, and and contain no user or booking data.

2

Internal API

Enables data retrieval from the Offision server for UI rendering. Secured by Secured by user authentication and restricted by identity and permissions, permissions, ensuring advanced functionalities are only accessible to accessible to authorized users.

3

SSO Interface

Obtains external user authorization based on pre-configured settings. settings. Verifies data validity and transfers it to Offision with user authentication, subsequently managed by the Internal API.

4

Visitor Interface APIs

Used by Offision Visitor Interfaces for displaying relevant visitor data. data. Protected by a security policy ensuring access only by official Offision official Offision visitor interface devices.

Offision

CORE COMPONENTS

Secure Data Flow and Integration

5

Player APIs

These APIs are provided for the Offision Players (including Booking panel, Signage, etc...) to show the related information. These API are protected by player security policy, which only Offision's official players can access to these APIs.

6

External APIs

External APIs are the APIs made for third party application, which allow allow them to access data from Offision, or upload data to Offision such as Offision such as IoT Sensor data. These API are closed by default, and will and will only be enable based on administrator configuration.

7

Synchronization Jobs

Offision has integration with multiple user directory and calendar service, service, such as active directory and Microsoft Office. These jobs are are integrated with the interfaces based on external security policy. Offision policy. Offision only collects user data / calendar data.

8

Notification Jobs

Offision pushes the notification and information data to user through through common services, e.g. SMTP email server, web push notification notification and mobile pass. Only visible data will be sent out.

CORE COMPONENTS

Secure Data Flow and Integration

9

Media IO / System Logging IO

Offision will save the user uploaded media file / system logging file to the file to the file storage. Currently Offision support multiple type of file file storage. The file storage configuration will be based on customer customer installation setting of Offision server .

10

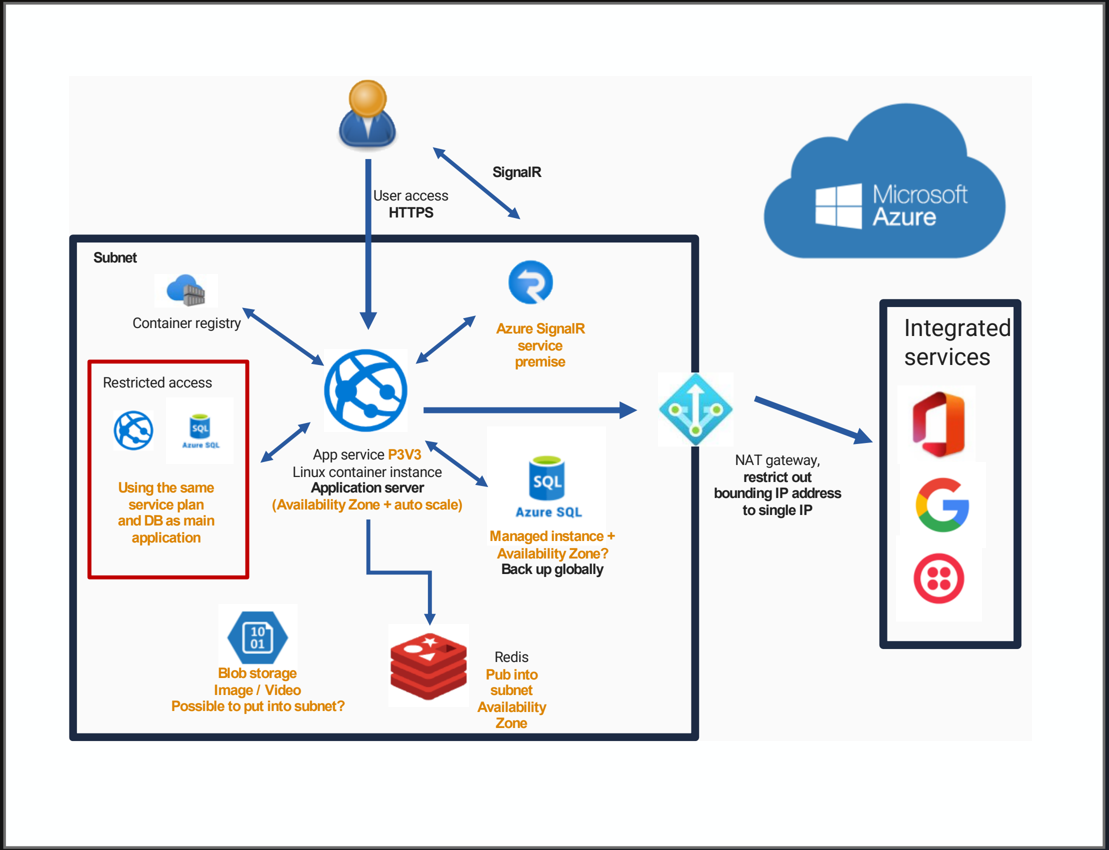
ORM

Offision will save all data to the database through ORM. No data will be will be kept within the Offision application. The protection and backup for backup for database are important for data security.

Cloud Security

Offision leverages a robust and scalable cloud infrastructure to deliver its smart office solutions. Our architecture is built to ensure high availability, performance, and top-tier security for all our services.

By utilizing leading cloud providers, we benefit from cutting-edge technology, global reach, and continuous innovation in security and operational efficiency.



Key features

- ✓ **Hosted in Microsoft Azure's Data Centers**
- ✓ **Complete Data Isolation**
- ✓ **Encrypted Data Storage**
- ✓ **Real-Time Backup & Recovery**
- ✓ **Protected from External Threats**
- ✓ **Secure Connections Only**

Multi-Tenant Architecture and Data Isolation

Offision's cloud infrastructure is designed with a robust multi-tenant architecture, ensuring the ensuring the highest level of data isolation and security for each client.

Dedicated Databases

Each client operates within their own isolated database instance, ensuring complete data complete data separation and privacy.

Enhanced Security

This architecture inherently prevents cross-tenant data access, significantly mitigating risks mitigating risks and enhancing overall data security.

Performance and Scalability

Resource allocation is optimized for each tenant, ensuring consistent performance and performance and independent scalability tailored to individual needs.

Offision

Cloud Data center security

Microsoft Azure Data Centers

Leveraging enterprise-class infrastructure with ISO 27001, ISO 27018, SOC 1/2/3, and other top-tier certifications.

Triple Redundancy

Simultaneous execution across three separate data centers eliminates single points of failure and ensures continuous operation.

Isolated Database Architecture

Complete separation of company account databases with Transparent Data Encryption (TDE) and Point-in-Time Recovery (PITR) backups.

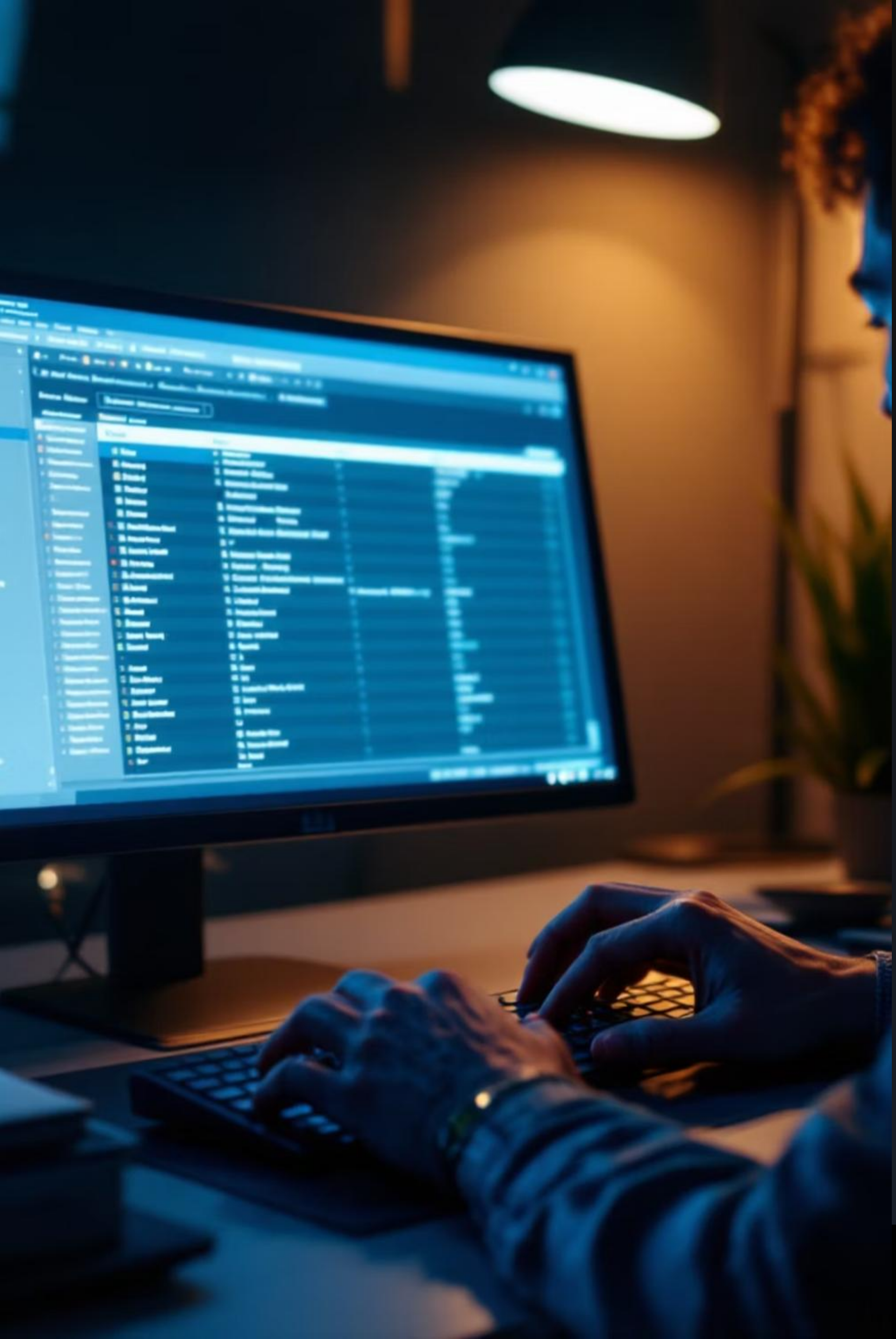
Azure Firewall Protection

External access blocked by enterprise-grade firewall solutions with strictly controlled network traffic network traffic limited to essential services.

Data Protection Mechanisms

Encryption Strategies

- **Transit Encryption:** SSL/TLS 1.2+ for all connections with third-party validated certificates
- **Storage Encryption:** Data encrypted at rest using advanced key key management systems
- **Password Protection:** One-way hashing and salting prevent credential exposure even during unauthorized access
- **Controlled Port Access:** TCP 443 for web applications and API communications, TCP 587 for secure email services.
- **Whitelisted IP Management:** For on-premise integrations, specific whitelisting available (e.g., 20.210.228.197)



Role-Based Permission Management

Defined Roles

Pre-defined roles (e.g., Administrator, User, Staff) with specific access levels to Offision features and data.

Granular Permissions

Control access to specific functionalities, modules, and data based on the assigned role, ensuring least privilege.

Simplified Management

Streamlined user provisioning and de-provisioning by assigning roles instead of individual permissions.

Enhanced Security

Reduces risk of unauthorized access and ensures compliance by enforcing consistent security policies across all users.

Offision's role-based permission management provides a robust and flexible framework for controlling who can access and manage and manage resources within your smart office environment, ensuring data integrity and operational security.

Authentication and Development Security

Authentication Methods

- **Password Authentication:** Default option with weak password restrictions restrictions
- **Single Sign-On:** Support for ADFS via SAML 2.0
- **OpenID Integration:** Seamless authentication with Microsoft 365
- **Multi-factor Options:** Additional security layers available

Development Practices

- **Circular Release Cycle:** Regular security updates and enhancements enhancements
- **Code Quality Framework:** Rigorous standards for security compliance compliance
- **Peer Review Process:** All code changes require approvals
- **Staged Deployment:** Multi-environment testing before production release

Offision

Authentication and Development Security Security

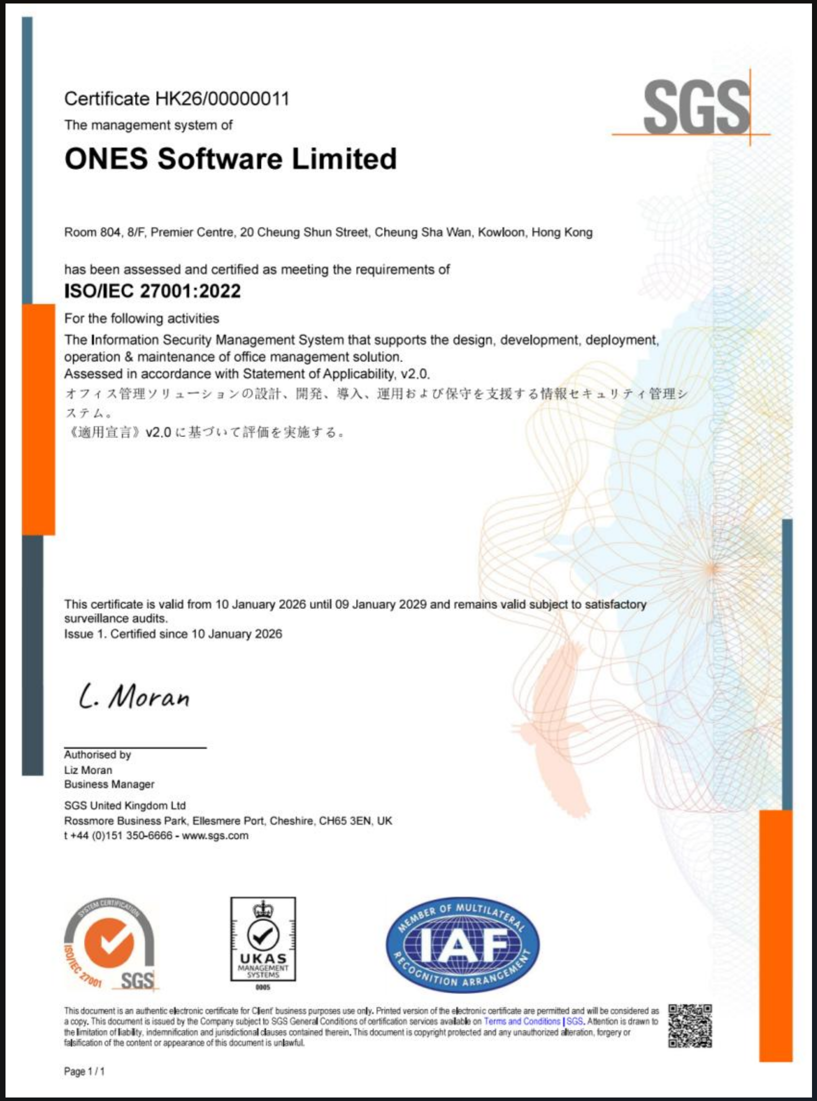
Offision is committed to maintaining the highest level of security through continuous and proactive vulnerability management. Regular and rigorous testing ensures that our systems are resilient against evolving threats and potential exploits.

Vulnerability Assessments

We conduct regular, automated, and manual vulnerability scans across our infrastructure and applications to identify potential weaknesses and misconfigurations. These assessments help us proactively address security flaws before they can be exploited.

Internal Penetration Testing

Independent security experts perform internal penetration tests to simulate real-world attacks. This internal testing helps uncover exploitable vulnerabilities that might be missed by automated scans and validates the effectiveness of our security controls from an insider perspective.



Certificate HK26/00000011

The management system of

ONES Software Limited

Room 804, 8/F, Premier Centre, 20 Cheung Shun Street, Cheung Sha Wan, Kowloon, Hong Kong

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2022

For the following activities

The Information Security Management System that supports the design, development, deployment, operation & maintenance of office management solution.
Assessed in accordance with Statement of Applicability, v2.0.
オフィス管理ソリューションの設計、開発、導入、運用および保守を支援する情報セキュリティ管理システム。
《適用宣言》v2.0 に基づいて評価を実施する。

This certificate is valid from 10 January 2026 until 09 January 2029 and remains valid subject to satisfactory surveillance audits.
Issue 1. Certified since 10 January 2026

L. Moran

Authorised by
Liz Moran
Business Manager

SGS United Kingdom Ltd
Rossmore Business Park, Ellesmere Port, Cheshire, CH65 3EN, UK
t +44 (0)151 350-6666 - www.sgs.com

This document is an authentic electronic certificate for Client' business purposes use only. Printed version of the electronic certificate are permitted and will be considered as a copy. This document is issued by the Company subject to SGS General Conditions of certification services available on Terms and Conditions | SGS. Attention is drawn to the limitation of liability, indemnification and jurisdictional clauses contained therein. This document is copyright protected and any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful.

Page 1 / 1

Click here to DOWNLOAD

ISO 27001 Certification

ONES Software has officially achieved ISO/IEC 27001:2022 certification.
This internationally recognized standard, awarded following a rigorous independent audit by SGS, confirms that our Information Security Management System (ISMS) meets the highest global benchmarks.

Certified ISMS

Our Information Security Management System (ISMS) is independently audited and audited and certified, demonstrating our structured approach to managing sensitive sensitive information.

Risk-Based Security

We employ a proactive, risk-based approach to identify, assess, and mitigate information security risks, safeguarding against potential threats.

Continuous Improvement

Regular reviews, internal audits, and external assessments ensure our security controls security controls are continuously improved and remain effective against evolving evolving threats.

"Achieving ISO/IEC 27001 certification demonstrates our unwavering commitment to safeguarding customer data and delivering secure, innovative solutions," says **Kit Ngai, Founder of ONES Software Limited**. *"This milestone reflects our dedication to excellence and trust in every aspect of our operations."*

Offision

Connected Workplace Experience

Start the new workspace experience

Click to start NOW!

30-days **Free trial**

Homepage

https://offision.com

Sales

Email

hello@offision.com

Technical support

Email

support@offision.com