IOT-BASED BUILDING MANAGEMENT

SECURITY PRACTICES

*An overview of 75F's **IoT-Based Building Management System** security protocols.*

INTRODUCTION TO 75F SECURITY PROTOCOLS

Security and privacy are major concerns when it comes to enterprise applications. The 75F platform incorporates protection in all stages of its lifecycle.

75F maintains transparency on all the data it collects from buildings and portfolios by creating, storing, using, and deleting data — and keeping all stakeholders informed on exactly what happens to this data and where it resides. From information protection, data management, and knowledge sharing to secure collaboration, 75F makes the most of your building information in a secure and user-friendly environment.

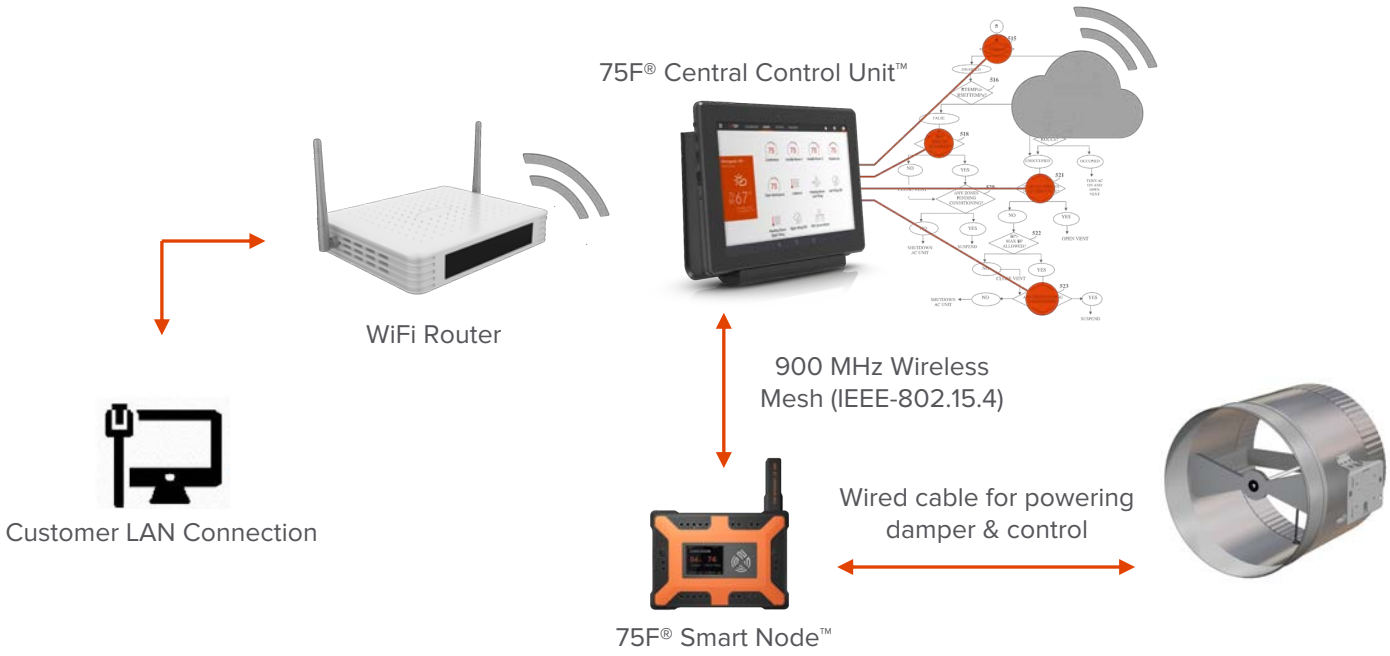
75F provides industry-leading security and privacy standards to its customers using a secure, enterprise-grade platform design for its whole product suite and cloud-based managed data. 75F alleviates security and privacy risks by isolating and protecting enterprise data sources and networks from client applications running on multi-platform devices and their networks.

The company's security protocol is a collection of security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, data, and resource access control, and data privacy protection. This paper describes the security protocol and its features from three perspectives:

APPLICATIONS & COMMUNICATIONS — Communication across all layers aims to protect software application code & application data against any security threats

SECURITY OF PLATFORM SERVICES — Relies on a unified bundle of hardware and software that protect both infrastructure and software-defined hardware, storage, and network components along with the operating systems and applications that reside on those platforms

UNDERLYING CLOUD INFRASTRUCTURE — Procedures and technology that secure cloud computing environments against both external and internal security threats



SECURING THE SOFTWARE PLATFORM

The foundation for comprehensive platform and cloud security rests on four pillars: visibility and compliance; compute-based security; network protections; and identity security.

Securing the application and communication has a two-pronged approach:

1. User Management – Authentication and Authorization
2. Managing access to application functionality, API and data based on user management.

MICROSOFT AZURE AS 75F CLOUD PROVIDER

With Microsoft Azure acting as the 75F cloud provider, all the security aspects provided in Azure have been utilized and integrated into the 75F platform.

APPLICATIONS SECURITY

- SSL / TLS Certificates
- Azure Active directory and other identity services integration
- Secure deployment of code

GOVERNANCE

- Azure policies
- Security policies
- Guest security configuration
- Locks

IDENTITY & ACCESS MANAGEMENT

- Azure resource manager
- Azure Active Directory
- RBAC
- Azure B2B
- Conditional access
- Identity protection
- Privileged identity management
- AD Connect
- Application management
- Azure B2C

MONITORING

- Azure monitor
- Security Center

DATA SECURITY

- Azure SQL database advanced data security
- Azure SQL database always encrypted
- Encryption in transit and rest

HOST SECURITY

- VM endpoint protection
- Update management solution
- Azure disk encryption

NETWORK SECURITY

- VM endpoint protection
- Update management solution
- Azure disk encryption

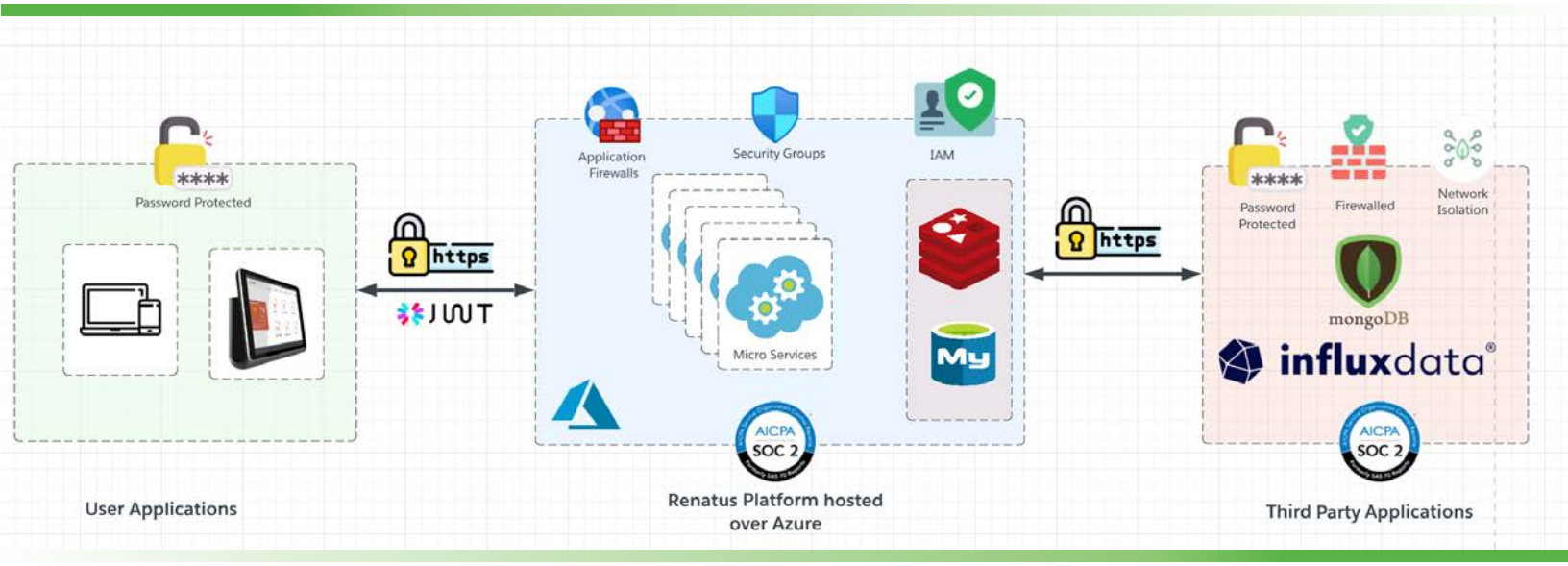
STORAGE SECURITY

- Storage firewall
- Access keys & SAS keys

SECURING THE SOFTWARE PLATFORM

APPLICATION CONNECTIVITY

75F applications connect with various services hosted in Azure. Each of the hosted services are available over https protocol. 75F's user platform, Facilisight, supports four different types of user roles: support, facility managers, organizational managers, and installers. Each of these roles have a range of permissions.

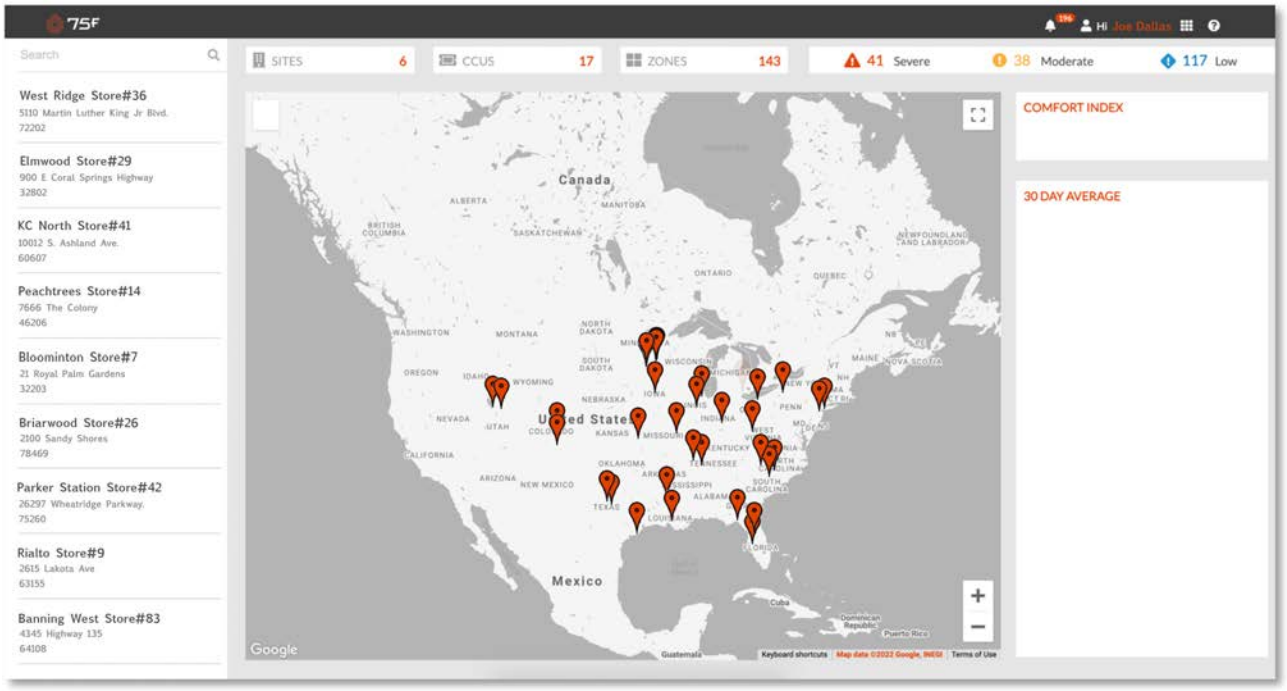


APPLICATION COMMUNICATIONS

All the communication between application is over TLS/SSL:

- CCU to Renatus Micro Services over Azure Cloud
- Mobile Applications to Renatus Micro Services over Azure Cloud
-
- Web applications to Renatus Micro Services over Azure Cloud
- Renatus Micro Services with Databases
- Renatus APIs for third-party use

SECURING THE SOFTWARE PLATFORM — USER ROLES



An example snapshot of 75F's user portal, Facilisight. Users register for Facilisight under varying roles with their own set of pre-defined permissions.

The Facilisight platform supports four different types of user roles: support, facility managers, organizational managers, and installers. Each of these roles have a range of permissions:

SUPPORT USERS

Support users are 75F employees with broad access to all portfolios and sites in order to assist customers. These role types may assign or revoke site access to all other user types and adjust building settings..

PRIMARY & SECONDARY FACILITY MANAGERS

Primary facility manager users have access to assigned sites. They may add or remove secondary managers or installers, manage notifications, transfer site ownership to another primary manager, and adjust building settings. Secondary facility manager users have similar permissions, although they may not add other primary or secondary managers.

ORGANIZATIONAL MANAGERS

Organizational manager users have access to all company building sites. Organization managers can perform all the operations as a facility manager and may manage multiple organizations.

SECURING THE SOFTWARE PLATFORM — USER ROLES

	Support User	Facility Manager Primary	Facility Manager Secondary	Organization Manager
Assign Sites to Users	X			
Transfer Site Ownership		X		
Add/Remove Primary Manager & Installers	X			
Add/Remove Secondary Managers	X	X	X	X
Add/Remove Secondary Installers	X	X		
Add/Remove Organization Manager	X			
Add Organizations to Organization Manager	X			
Site Energy Configuration	X			
Change Site Configuration	X	X	X	X
Notification Management	X	X	X	X
Alert Insight and Configuration	X			
Tuners	X	X	X	X
Adhoc Visualizer and Table Viewer	X			
Facilisight Assist	X			
Access to Website and Apps	X	X	X	X
Haystacker	X			
Domain Modeler	X			

USER ONBOARDING

75F does not support self-service registration in Facilisight to prevent unsolicited accounts in the system. All users in the system are added by existing users with a role that gives them permission to add a new user.

User onboarding for support users and facility managers is a two-step process:

- The new user receives an email confirming their addition to the platform
- The new user receives a one-time password for the first login to confirm their email, and the user then sets their password. The user may also complete the signup using Microsoft login if Microsoft is the email authentication provider

The following describes what user types may add new members to the system:

- Support — A support user may only be added by other support users
- Primary Facility Managers — This user type may only be added by a support user
- Secondary Facility Managers — This user type may be onboarded by support users or primary facility managers

USER AUTHENTICATION

User authentication depends on whether the user is onboarded with a Microsoft Authentication provider or a username-password authentication provider:

- Microsoft Login Authentication — 75F supports Microsoft Authentication for third-party logins for accounts that are onboarded on Microsoft AD
- Username-Password Authentication — The user's password is hashed with salt, generated with multiple iterations, encrypted, and then stored in the database. Authentication includes verified user existence, plus a password that matches the record stored in the database

USER REVOCATION

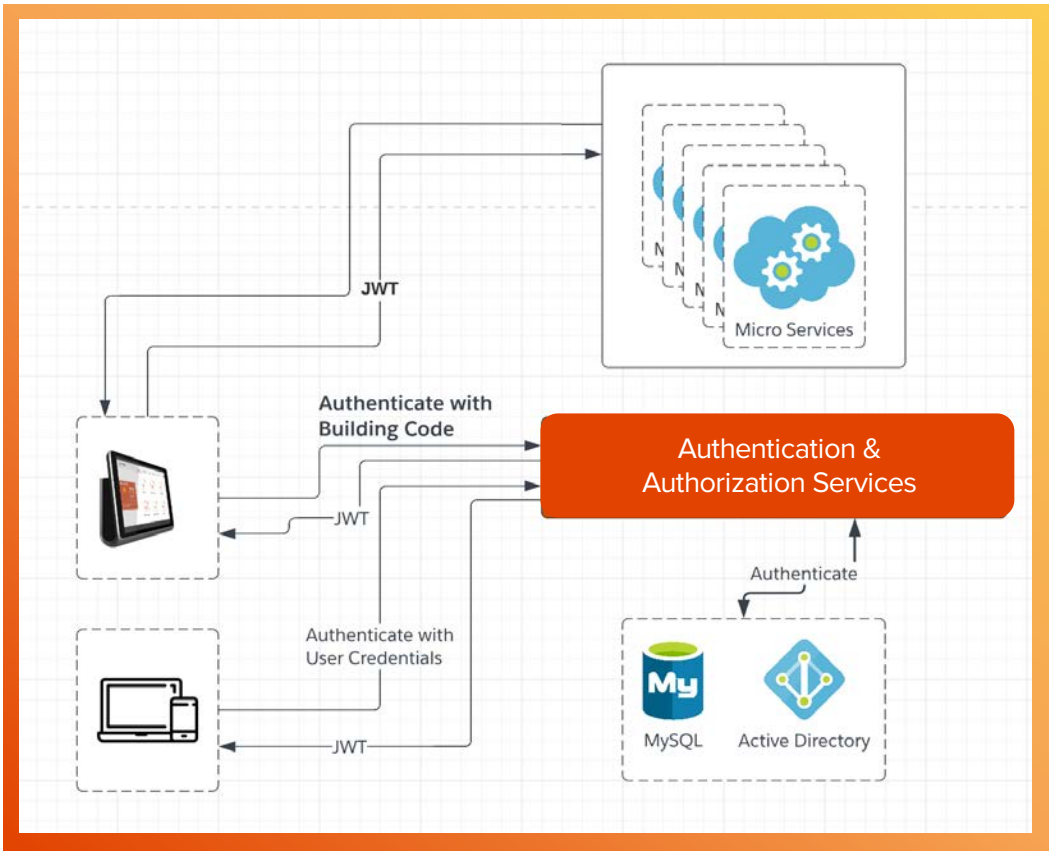
Users may be revoked of site access, and any user who has no sites becomes an unassigned user and may be removed from the system. However, if a user is a primary facility manager, then all of their sites must be transferred to another primary manager before they may be removed from the system. This ensures every site will always have a primary facility manager.

DEVICE AUTHENTICATION

The CCU needs to be authenticated for any communication with the 75F platform. This happens at various stages during the lifecycle of the CCU.

A passcode unique to the building is generated during each of the below mentioned operations:

1. To register a site to the CCU
2. Adding additional CCUs to a site
3. Replacing the CCU
4. Communicating with the 75F platform for data access
5. Reestablishing communication with the platform after a long period of network unavailability



USER INFORMATION

User information is stored in the MySQL database and access to the database is available only to the connected services. Direct access for the database is provided only on request and for the requested IP address only. SSL connection is enforced for all connections to MySQL.

PASSWORDS

User passwords are hashed with salt, generated with multiple iterations, encrypted, and stored in a database.

ENERGY CONFIGURATIONS

Energy configurations are stored in a password protected, user access restricted database.

SENSOR INFORMATION AT THE SITE

Sensor information is stored in password-protected InfluxDb and all communications with the InfluxDb happen over https.

FLOOR PLANS

Floorplans are kept in secure Azure blob storage with direct access to content available only to the subscription root users. The secure transfer option in Azure blob storage enhances the security of storage account by only allowing requests to the storage account by secure connection. For example, when calling REST APIs to access the storage accounts, it is possible to connect using https. Any request using http will be rejected. Site access is verified by application for users before a floor plan is shared.

Example floor plan in 75F's user portal, Facilisight.

SECURING THE SOFTWARE PLATFORM — DATA ACCESS CONTROLS & AUDIT TRAIL

DATA ACCESS CONTROLS

The 75F platform creates and manages role-based access rules for data. 75F sets permissions at Site, Zone level to define which users can access what data and how. Access control can be set in the internal portal by the support users.

Access controls are applicable for the:

- Azure platform — Access to the Azure platform is controlled by permissions given to groups. Groups have roles assigned, which the users are enabled for. Group creation and role assignments are possible only by the account administrator
- MySQL — Access restrictions as applicable for the Azure platform are also applicable for MySQL. MySQL can be configured to be provided access from a specific address only
- MongoDB — This has access control restrictions available at network and user level. Access to the portal is only based on invite
- InfluxDB — Access to the portal is based on invite and controlled based on assigned role

AUDIT TRAIL

Audit trail of operations happening at the platform and the application are logged and made available as required.

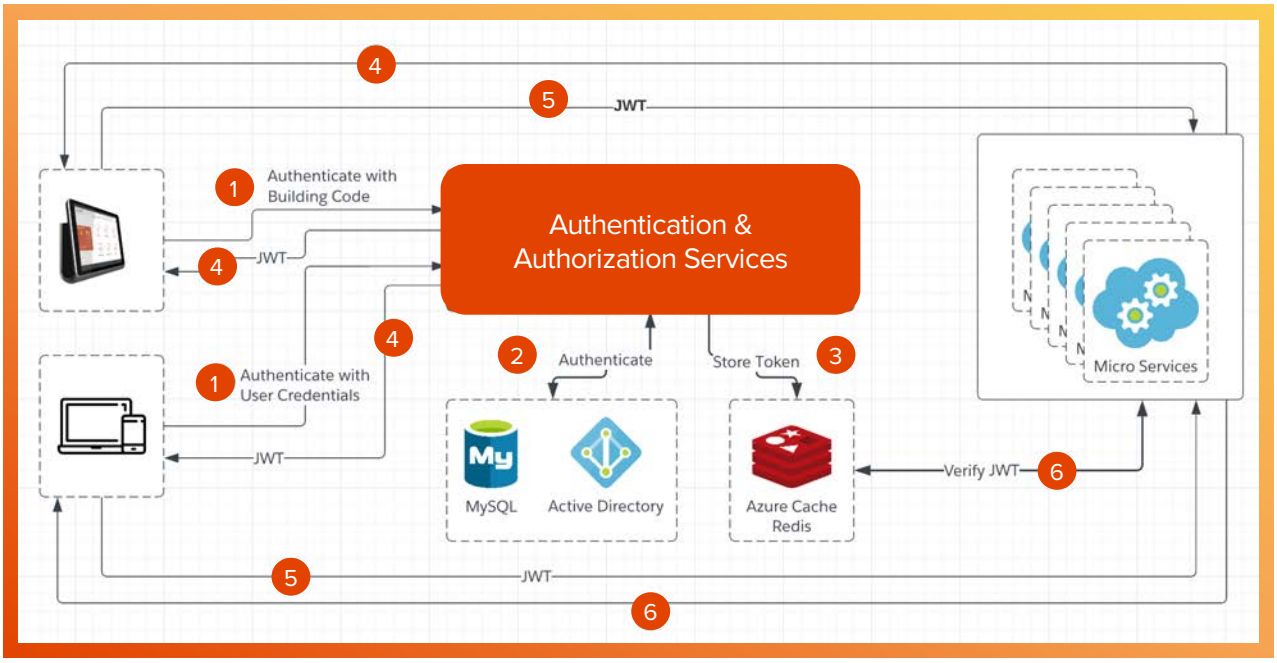
- Azure platform — All changes made to the Azure platform such as configuration changes, deployments, service lifecycle changes, and security are logged by the Azure platform. Such details can be observed under “Activity Log” sections under each service deployed on the platform. Azure also provides a wide array of configurable security auditing and logging options to help identify gaps in your security policies and mechanisms. Further details on security logging and auditing, plus an overview of Azure platform logs
- 75F platform — All activity is tracked and made available to the support users under an audit trail. Tuner configurations, user intents, schedules and alerts are all captured under the audit trail, along with details of change trigger sources. 75F’s audit trail also captures information on previous and changed information to more easily identify performed changes

SECURING THE SOFTWARE PLATFORM — ACCESS TO ENTERPRISE DATA

Access to enterprise data follows the authentication and authorization provided by the identity management system that is integrated with the application. All APIs that make requests to enterprise data are required to include an authorization token (JWT) issued by the authentication module. The authentication token clearly indicates the roles supported for the user requesting enterprise data and is validated at every stage before the response is issued. User is authorized against the sites assigned to the user before any information related to the site is processed thereby protecting the system from unauthorized site information access.

Token issued has expiry set as detailed below:

- 24 hours for web and mobile applications
- 60 days for on-premise CCU



SECURING THE INFRASTRUCTURE PLATFORM

75F runs on cloud infrastructure provided by Microsoft Azure. Microsoft Azure regularly undergoes rigorous security audits and have completed the requirements of major security certifications. This section covers physical and compliance features of Azure including physical security, data compliance and certifications, and incident management.

PHYSICAL SECURITY

Microsoft designs, builds, and operates data centers in a way that strictly controls physical access to the areas where the data is stored. Microsoft has an entire division devoted to designing, building, and operating the physical facilities supporting Azure. This team is invested in maintaining state-of-the-art physical security.

Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Data centers managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Layers of physical security are:

- Access request and approval — Access requests must be raised prior to arriving at the datacenter and a valid business justification is required for the visit, such as compliance or auditing purposes. Individuals only has access to the discrete area of the datacenters required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire.

- Facility's perimeter — Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the datacenters, with a security team always monitoring their videos.

- Building entrance — The data-center entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the datacenter and always monitor the videos of cameras inside the datacenter.

- Inside Building — It is required to pass two-factor authentication with biometrics to continue moving through the datacenter and it is possible to enter only the portion of the datacentre that have approved access to.

- Datacenter floor — Permission is allowed onto the approved floor only. Any person entering the datacenter is required to pass a full body metal detection screening. Additionally, video cameras monitor the front and back of every server rack.

DATA COMPLIANCE & CERTIFICATIONS

- Microsoft — Designs and manages the Azure infrastructure to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. It also meets country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

- InfluxData — SOC 2® Type 2 certified

- MongoDB Atlas — SOC 2® Type 2 certified, HIPAA Compliant, ISO/IEC 27017:2015 certified

INCIDENT MANAGEMENT

75F's system is configured to monitor any anomalies in the service. As part of this health check dashboard and alerts have been setup at the application level and the infrastructure level.

In case of unavoidable incidents causing a data-loss, the platform has enough capabilities to be restored to its original functional state. To ensure this the platform is configured for regular backups of the databases.

Renatus Software uses three databases:

- MySQL : Azure Database for MySQL takes backups of the data files and the transaction log. These backups allow you to restore a server to any point-in-time within the configured backup retention period. The default backup retention period is seven days. All backups are encrypted using AES 256-bit encryption. A full database snapshot is performed daily. Azure maintains copies data synchronously three times within a single physical location in the primary region

- MongoDB: Backup is taken for MongoDB every 6 hours and the backups are retained for 7 days. MongoDB also supports Just-In-time restore which allows us to restore to any point in time in the last 7 days. Weekly snapshots are taken every week and retained for 4 weeks. Monthly snapshots are taken every month and retained for 12 months

- InfluxDB: Influx DB hosted on the cloud automatically keeps three days of hourly backups