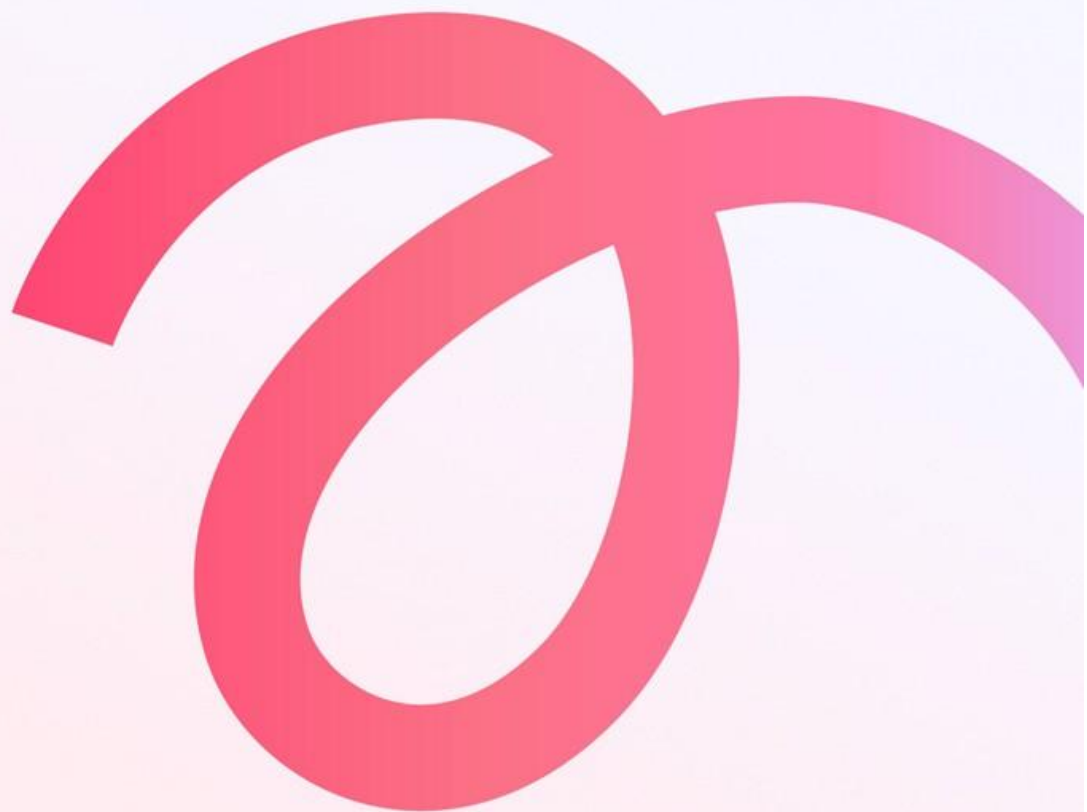


Security description

Systemam Visit (RespaManager)

Confidential

Updated 25.9.2025



Contents

1	System overview	4
1.1	Name, owner, physical location, and contact person	4
1.2	Purpose and principles	4
1.3	Typical solution architecture	5
1.4	Processed data content and data protection level	5
1.5	Security audits.....	5
2	Processing of personal data	5
2.1	Key legislation	5
2.2	Data processing principles	6
3	Administrative security solutions	6
3.1	Risk management	6
3.2	Operating principles.....	7
3.3	Change management process.....	7
3.4	System maintenance	8
3.5	Termination	9
3.6	Data security reporting policies	9
3.7	Sub-processors, partners, and security agreements.....	10
4	Operational security solutions	11
4.1	Personnel security.....	11
4.2	Physical security solutions.....	11
4.3	Usage controls.....	11
4.4	Preparedness and continuity management.....	12
4.5	System documentation.....	12
4.6	Actions in a state of emergency	12
5	Technical security solutions.....	13
5.1	Security architecture	13
5.2	Access and usage authorization management.....	13
5.3	Usage tracking and logs	14
5.4	Data communications security and integrations to other systems	14

- 5.5 Backups 15
- 5.6 Technical platform security 15
- 5.7 Application-level security 15

1 System overview

1.1 Name, owner, physical location, and contact person

System Visit visitor management, owner System Oy.

Service is produced and maintained in Finland.

Contact Person: Anssi Tamminen, CEO, anssi.tamminen@system.io

1.2 Purpose and principles

System Visit visitor management is designed for the management of visitor traffic and for automating visitor reception. It helps to create a user-friendly solution that can be managed both centrally and site-specific.

System Visit Visitor Management enables, amongst other things:

- The creation of a standardized and unified operating model for the reception of the estate.
- Improvement of the estate security, service level, brand image, and visitor satisfaction.
- Saving on costs.
- Visitor traffic monitoring and management.
- Generation of pictorial and personalized visitor cards for the visitors.
- A visitor reception in places where it is not possible otherwise.
- Placing reception points at different entrances of the estate and connecting locations and offices.
- Extension of operational times.
- Construction of broader IT concepts with the digital processing of visitor data.

The solution is built and developed following the standards of information security principles.

The service is supplied from a high-security data center located in Finland that also has ISO 27001 certification. The more detailed description of the data center is in separate documents.

1.3 Typical solution architecture

Solution consists of a web service (web UI) and a database, and optional integrations, such as calendar invitation or AD and self-service kiosks.

The data is stored in a secure data center, protected by strong access controls. All technical processing is performed via API interfaces and database queries using the least privilege principle.

Supplying and maintaining a network connection for self-service kiosks is the responsibility of the customer. Data transfer between the self-service kiosk and the data center is always encrypted using the HTTPS protocol. Self-service kiosks do not store personal information.

1.4 Processed data content and data protection level

System Visit is a digital visitor management SaaS solution. Therefore, to ensure the operation of the system, it is necessary to collect information related to a visit event, such as personal data from visitors and hosts.

The processed data includes the host data in the system, data of the visitors, and information related to the visit (such as the date). The collected data and retention times depend on the settings set by the customer.

1.5 Security audits

The security of the solution has been audited by a third party. The report of the audit can be shared with customers.

The solution is possible to be audited by customers when separately agreed upon.

2 Processing of personal data

2.1 Key legislation

System Oy is a Finnish company. The service is produced and maintained in Finland in accordance with Finnish law. Personal data is processed in accordance with the General Data Protection Regulation (GDPR).

2.2 Data processing principles

System has internal guidance for the personnel on the procedures for the processing of data and the consequences of non-compliance with these procedures, as well as the failure to comply with the provisions on confidentiality.

Technical measures for System personnel operating the solution include logging in to services using their own personal identification with the lowest privileges principle. The use of IDs/credentials is automatically logged. The computers used by the personnel are encrypted.

Information security for customer data content in System services and the confidentiality, integrity, and availability of personal data are ensured by the most appropriate technical and administrative measures in accordance with the company's security principles.

Customer information is processed only by persons who are specifically eligible for the processing of the personal data in System. The verification of customer services and the information therein is only permitted where necessary to determine the problematic situation of the customer. Even in this case, the information is accessed regarding the requirement of resolving the problematic situation.

The connection to the data center and client data is produced through secure VPN connections with strong passwords and logging.

Connections to the data center are stored with user-specific logging.

Data transfer between the user and the service, the self-service device, and the service is encrypted via the HTTPS protocol without intermediate storage.

3 Administrative security solutions

3.1 Risk management

The risks to the system are mainly the personal information ending up in the wrong hands, for example, because of the actions of a service user. The risk can be minimized by limiting the user's access rights and the people to whom the access rights are issued, restricting the access to the service by IP limits, using the SSO login, setting the retention time of the data stored on the service, and limiting the data collected. Administrative users of the customer can also maintain several settings regarding the visibility of stored data.

The system automatically logs the use of the service and the actions taken, so that in possible problematic situations it can be used to trace the actions and events that led to the situation. It is a technical action log that does not save personal data. Access to the action logs is only available for the System support personnel.

The system also automatically logs (audit-log) the actions related to the use or reading of personal data, for example, if a customer user (typically a host) opens the detailed visitor information, and error situations (error-log), in which there is no personal data.

3.2 Operating principles

The customer is responsible for the right use of the system and for user management.

Customer administrative users (users with an administration role) have the right to remove users, reset passwords, or alter the roles for other users with lower privileges.

Personnel users can only access the data to which they have rights.

Only administrative users have the right to request information regarding the personal data that is stored in the system from System support.

Any data, including personal data, is primarily transmitted through encrypted data transmission without email. System support personnel do not store any personal information locally.

3.3 Change management process

System constantly develops the solution. These updates might include fixes or new features. All updates are well tested (automated tests and manual tests) before being released in production.

For testing, an identical environment to the production environment is used. Updating takes place over encrypted connections.

Application development at System is managed using GitHub, which ensures that all changes are tracked and that previous versions are preserved. This allows for efficient rollback in case of issues or regressions.

Updating and other changes to applications and services, as well as web-based centralized management tools, are handled via secure remote access. The default remote access to the self-service kiosk is by using the TeamViewer application.

Application updates for self-service kiosks are done remotely through direct connection to the device at a predetermined time, generally after normal office hours. The update will cause a break in use, typically from one to fifteen minutes.

The normal web service update process on the server is fast and only causes a temporary, less than one-minute downtime. Updates are always agreed in advance and are scheduled to take place after office hours.

Updates are always aimed at being notified in advance. Updates and any visible changes that may cause will be notified via email. If the changes are significant, they will be given a user manual and, if necessary, separate user training. The service contract may contain terms that are individually agreed upon by the customer.

3.4 System maintenance

System Oy has a fixed number and an email address for the support service. In addition, feedback can be sent via the web service. Tickets also come through an automatic error reporting system.

All messages, errors, and feedback that come to the support service are stored in a ticketing system and are answered through the same system.

Support requests from a customer to System Oy will automatically be logged into the ticketing system. Phone support requests are logged in the same system.

The support requester is informed about the progress of the support request and the changes in status automatically from the ticketing system.

Support requests are monitored, and statistics are compiled to help guide the further development of the support service and improve the features that cause the most support requests in the statistics.

Self-service kiosks are monitored for the online state and for the health of the device. If issues are detected or the device loses network connection, System support is automatically alerted.

3.5 Termination

The customer owns the data stored in their service and may at any time retrieve the collected information from the service.

On the event of terminating the system, all customer information, applications, and settings from the server and backups are removed.

Potentially returning self-service kiosks are cleared from log data and reset to the initial default state.

3.6 Data security reporting policies

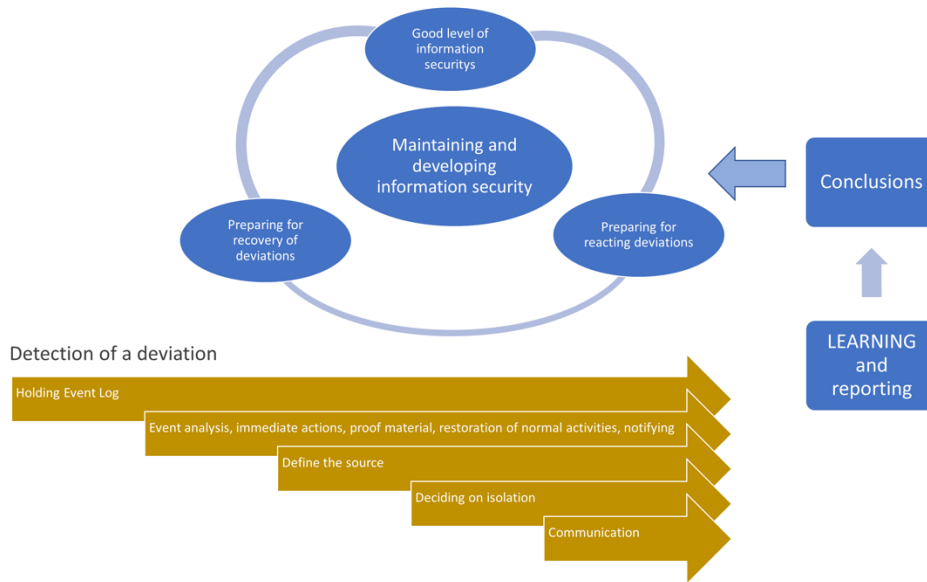
The state of the service is automatically monitored both at the server level and at the system level. In error situations, the system automatically sends an error message along with an information log to the System support, which enables security and data security vulnerabilities to be detected as soon as possible.

The support personnel are informed of suspected security breaches. Even a suspicion launches an investigation. Notifications to customers are immediately made after a serious threat is detected.

When investigating a security breach, all available log data is always saved, and the measures taken are recorded.

If necessary, the production environment can be deactivated during the investigation. The production environment is restored when the deviation is cleared, the event is reported internally, and the customer is informed via a contact person.

The internal development and highlighting the importance of information security



3.7 Sub-processors, partners, and security agreements

System Oy develops and maintains the service. The service is provided through a third-party data center in Finland, where the environment (hardware and network connections) is operated by the service provider. System is responsible for the overall maintenance of the service as well as the processing of personal data.

A list of sub-processors is maintained separately.

4 Operational security solutions

4.1 Personnel security

All employment contracts for System include a confidentiality clause concerning the information of customers and partners, or they have signed a separate sanctioned confidentiality agreement, which is valid even after termination of employment.

Access to information from customers or partners has been granted only to System personnel who require the information to provide services or to maintain and test the system supplied to the customer.

Information is not passed on to third parties and is not used, for example, for marketing purposes. Internal communication within the System personnel regarding customer management is handled through strongly encrypted communication channels.

4.2 Physical security solutions

In standard delivery, the self-service kiosks do not require any connection to the customer's internal network. Self-service kiosks are protected with strong passwords. Self-service kiosks are built robustly.

The premises of System are protected by electronically and mechanically functioning personal access control, which stores log data.

Details about the data center security protection can be requested as a separate document.

4.3 Usage controls

The system has been implemented in accordance with good programming practices, considering, for example, hostile inputs and error handling.

The service stores a log from server connections and error situations. Self-service kiosks feature an action log that stores technical information about the use and operation of the self-service kiosk, not customer or visitor-specific information. The web service and background processes in the data center have log functions that store technical usage information, not personal information.

The data center service provider has its own measures against prohibited connection attempts.

4.4 Preparedness and continuity management

Visitor management is the core product of System, and the whole personnel is trained to maintain and develop this system.

Error situations are categorized in three stages: disadvantage, problem, or critical failure.

Support connections generated through automatic error reporting by the self-service kiosk or otherwise through the vendor processes are logged in to the same ticketing system as the support requests from the customer. Information on how to handle the matter is thus passed on to the desired contact person.

Software-related issues in self-service kiosks are primarily resolved through secure remote access. For hardware-related issues, we maintain a comprehensive spare parts inventory to ensure quick replacement.

System constantly improves its customer support service. System maintains statistics and analyses connections to the support service (automatic error-reporting, phone calls, email) to improve the overall solution quality and to find concurring problems. Statistics also include the time it has taken to solve the problems.

System automatically keeps an up-to-date backup of each solution, ensuring that data and customer-specific settings can be restored immediately. Even in the event of a complete device failure (e.g., vandalism), reception functionality can be quickly recovered using a replacement device with restored configurations.

4.5 System documentation

System maintains and updates technical documentation, user guides, and manuals for the solution. User guides and quick guides are maintained for each user level.

4.6 Actions in a state of emergency

System support operates during office hours (08-16 EET) if not otherwise agreed with the Customer. Support service is organized in a ring to ensure the maximum availability for all support calls.

In significant disruptions in service (for example, general availability of the service), the whole personnel is automatically informed and alerted.

Procedure in the case of serious error/state of emergency:

- 1 Announcement to the entire System support team
- 2 First essential measures
- 3 Information on customer contact
- 4 Ticketing the error situation
- 5 Creation of potential permanent corrective actions
- 6 Construction of monitoring
- 7 Reporting

5 Technical security solutions

5.1 Security architecture

Applications, databases (and their passwords), and subdomains are separate for different customers in the data center.

5.2 Access and usage authorization management

Access to the web service can be limited to the IP addresses that are used only by the customer.

Technical access to the system environment is only available to designated persons in System.

Logging in to the service can be done either by single sign-on using organizational usernames or by creating and using a personal account.

At the beginning of the customer relationship, the customer's administrator hosts data and roles are created by System Oy. Administrator, then creates a personal account and sets their own password.

Users manage their own profile and password.

All passwords are encrypted in the system. The customer manages the passwords themselves and is responsible for using a sufficiently strong password. Users can reset their own passwords themselves. System cannot resolve passwords.

The administrator has permission to manage accounts. Administrator privileges allow you to change the visitor management system settings and mass delete data.

- **Administrator role:** The account can be used to manage settings for the entire system, including user accounts
- **Lobby service person:** The account meant for the reception officer in the lobby has the broadest possibilities for managing and tracking visitor traffic. Only the lobby service person's account can sign in visitors. When signing in, it is possible to print a visitor card and send an arrival notification to the visit host via SMS and email.
- **Assistant (Power User):** In addition to the basic functions, the possibility to monitor the visitor traffic and browse the visitor database.
- **Personnel account:** Basic functions to preannounce own visitors and see own visitor data.

5.3 Usage tracking and logs

Solution stores read access logs of those who have seen their personal data. Also, sign in to the web service, and password changes are logged. Users can see the basic log through their own profile.

A system-level log is maintained from all the connections to the webservice. Also, the self-service kiosk maintains a system-level log. Logs are technical action logs that do not contain personal information. Access to the technical logs is only available to Systemam support personnel.

5.4 Data communications security and integrations to other systems

Data communications security is done using an HTTPS-encrypted connection. TLS encryption takes place on the server, and the decryption takes place within the client terminal.

As a TLS certificate, a 2048-bit RSA certificate is used. TLS version 1.3 is used by the system.

Certificates are not customer-specific.

5.5 Backups

Full backups are made daily on application servers, database servers, logs, and data. Backups are retained according to the convention for seven (14) days, unless otherwise agreed. Self-service kiosks' action logs are not backed up.

5.6 Technical platform security

Cloud service is produced in a data center that is built to tolerate faults and to detect and block attacks. The visitor management server has the latest operating system updates, antivirus protection, and strict practices and limitations for establishing a connection.

Self-service kiosks can, if separately agreed, be equipped with customer-specific security software and practices. Protection means of the data center provider can be provided on request in a separate document.

5.7 Application-level security

The application is developed following industry-standard secure coding practices. It includes internal mechanisms to prevent common threats such as SQL injection and other input-based attacks.