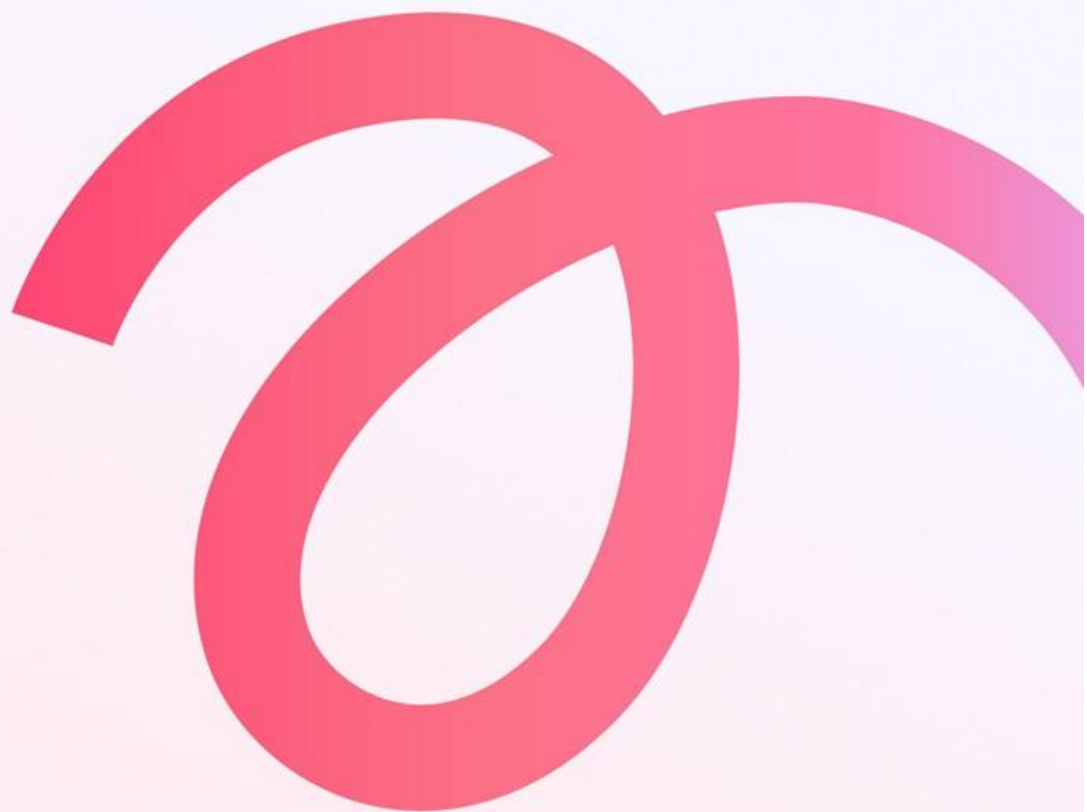


Security description

System Pass

Confidential

Updated 23.9.2025



Contents

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

5.5 Backups 12

5.6 Technical platform security 12

5.7 Application-level security 13

1 System overview

1.1 Name, owner, physical location, and contact persons

System Pass safety Inductions, 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 Pass is a documenting online service for certified safety inductions. Pass sends invitations, carries out training, and documents performance, regardless of device, anywhere, and anytime.

The service:

- Improves induction quality
- Reduces costs
- Improves security and verifiability

System Pass ensures that induction and training have been verifiably completed, ensuring the desired level of quality. Easy editing of the material ensures up-to-date material. The service is efficient and affordable in practice – time spent on induction no longer ties the person to the site, provided the training is carried out in advance.

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

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

1.3 Typical solution architecture

Solution consists of Pass (web UI) and database and optional integrations.

The data is stored in the data center.

User uses the solution by web browser. All connections are encrypted by HTTPS protocol.

Technically data processing is done by using API interface and database queries using the lowest possible rights.

1.4 Processed data content and data protection level

System Pass is a system for managing online inductions. Therefore, to ensure the operation of the system, it is necessary to collect information related to induction performers, such as personal data.

The processed data includes the data of the performers and information related to the induction (such as the timestamp and content).

1.5 Security audits

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

2 Processing of personal data

2.1 Key legislation

System Oy is a Finnish company located in Finland. 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 guidance for the personnel on the procedures for the processing of data and the sanction consequences of non-compliance with these procedures, as well as the failure to comply with the provisions on confidentiality.

System personnel log in to services using their own personal identification. 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 a 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 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, as a result 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, and limiting the data to be collected.

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 the actions related to the use of the service and errors that occur.

3.2 Operating principles

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

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

Lower-level 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.

System uses internal version control for application development, so that all previous versions of the application are stored and can be easily restored in any problem situations.

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

Minor updates are always aimed to be notified in advance, depending on the impact they have in the service. Updates that will cause visible changes to the service will be notified via email. If the changes are significant and alter the way the service is used, they will be included in an updated user guide and delivered to the customer. If necessary, separate user training can be organized. 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. The support service follows the ITIL v3 framework.

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. Reaction to the support request happens during the same day.

The support requester is informed about the progress of the support request and the changes in the 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.

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.

3.6 Data security reporting policies

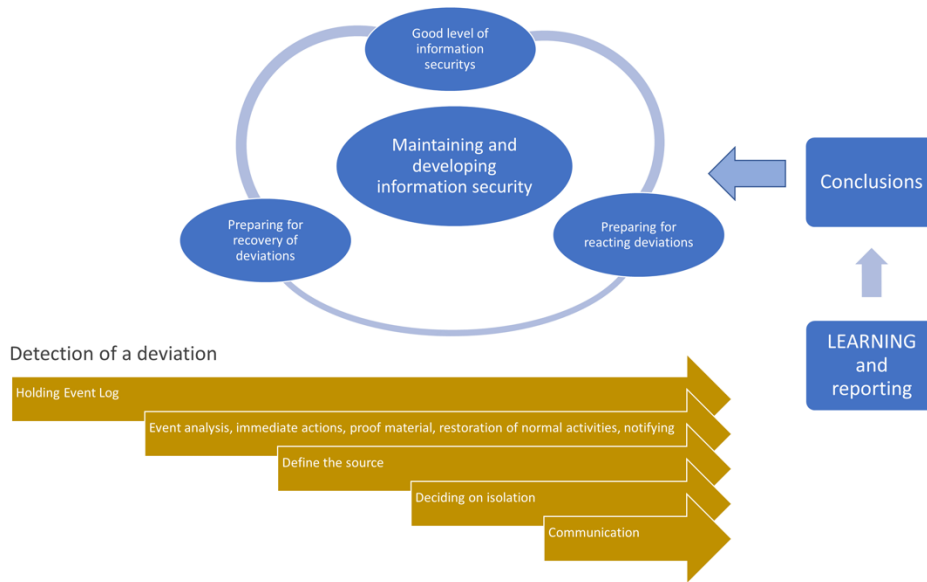
The state of the service is automatically monitored both at the server level and at the system level. In error situations, the system automatically sends an error message along with an information log to the System support, which enables security and data security vulnerabilities to be detected as soon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

The support personnel are informed of suspected security breaches. Even a suspicion launches an investigation. Notification to customers is 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-processing, 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 Systemat personnel regarding customer management is handled through strongly encrypted communication channels.

The customer can request a complete list of people who have access to their service. The list also shows the duties of these persons in Systemat and the reason for granting access.

4.2 Physical security solutions

The premises of Systemat 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. 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

Systemat Pass is one of the core products of Systemat, and the whole personnel is trained to maintain and develop this system.

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

Information on how to handle the matter is thus passed on to the desired contact person.

Systemat constantly improves the customer support service. Systemat 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.

4.5 System documentation

System maintains and updates technical documentation, user guides, and manuals for the solution. Answers to the most common questions can be found in our knowledge base.

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 to the 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

Databases (and their passwords) are separated 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 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.

User manages 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. System cannot resolve passwords.

5.3 Usage tracking and logs

Solution stores access log of sign-ins to the web service and actions that cause communications (email/sms) to persons performing inductions.

A system-level log is maintained from all the connections to the webservice. Access to the technical logs is only available to System support personnel

5.4 Data communications security and integrations to other systems

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

As an SSL certificate, a 2048-bit RSA certificate is used. TLS version 1.2 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 (7) days, unless otherwise agreed.

5.6 Technical platform security

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

Protection means of the data center provider can be provided on request in a separate document.

5.7 Application-level security

The application has been developed using good practices of the industry, such as internal ways of blocking SQL injection attacks.