Technical and Organizational Security Measures

ingenico ePayments

Table of contents

1. Security measures

Scope

The scope of this document covers the following entities: Ingenico eCommerce Solutions' entities (IeCS) and Ingenico Financial Solutions SA/NV (IFS). Both are later referred to in the document as Ingenico.

Organization of Information Security

The objective(s):

Ingenico has an information security office that has been ratified and is supported by senior management and ensures that its information security personnel are competent in information security. Measure(s) include(s):

- Ingenico established an information security office with expertise in the different domains of information security
- Members of the information security office have a full-time responsibility for information security
- The information security office reports directly to an Ingenico senior management member
- Ingenico security office has developed a comprehensive set of information security policies, approved by senior management and disseminated to all Ingenico workers
- Ingenico security policies and procedures are reviewed at least annually and updated when required
- Ingenico workers are given training on information security, compliance and data privacy topics and must take and pass a test on information security at least annually

Information Security Management System

The objective(s):

Ingenico has an ISMS (Information Security Management System) in place to evaluate risks to the security of personal data, to manage the assessment and treatment of these risks and to continually improve its information security. The security controls and activities are implemented in a business as usual approach. Measure(s) include(s):

- Ingenico has deployed an ISMS to manage security professionally and its ISMS has been inspired and based upon industry best practices, frameworks and standards such as the Payment Card Industry Data Security Standard (PCI DSS), ISO/IEC 27001:2013.

Physical Access Security

The objective(s):

Limitation of the physical access to Ingenico systems and data to only authorized Ingenico workers. Measure(s) include(s):

- The payment platform is hosted at a professional, production data center with a defined and protected physical perimeter, strong physical controls including access control mechanisms, controlled delivery and loading areas, surveillance and 24x7x365 guards
- The production data center and its equipment are physically protected against natural disasters, malicious attacks and accidents
- Only authorized representatives have access to the production data center premises, all datacenter accesses are logged
- The data centers are located within European Union
- A camera system (CCTV) monitors all entrances and operational areas within the data center; the recording must use a time synchronization mechanism and be retained for one month
- Desks and workplaces are left clean by Ingenico workers when leaving the office in accordance with the clean desk policy
- Secure printing has been implemented to avoid unauthorized access the print-out on the server.

System Access Security

The objective(s):

Access to Ingenico systems and platforms are only used by authorized, authenticated users. Measure(s) include(s):

- Access to Ingenico production environment is granted only to authorized Ingenico workers (the authorized persons)
- Access are limited as required for those authorized persons to fulfil their function
- Multi-factor authentication is required for access to Ingenico production environment
- All access granted as “user” to Ingenico production environment require a unique and personal identifier (a “user account”)
- Any mobile devices (laptop, USB key,…) must have disk encryption protection in place in order to protect against data leakage when such a device is stolen or lost
- The Ingenico password policy and acceptable usage policy prohibits the sharing of passwords, re-use of personal non-work related password and requires passwords to be changed on a regular basis and default passwords to be altered. All passwords must fulfil defined minimum requirements and are stored in encrypted form.
- Each computer has a password-protected screensaver that is activated upon a specific time of inactivity
- The production environment is equipped with multiple layers of security controls such as firewalls, web application firewall, intrusion detection systems, intrusion prevention systems, file integrity monitoring, etc.
- Network access control must be implemented in order to avoid un-trusted device to connect to the privileged network segment having access to the Ingenico information systems
- All of the production systems (including network equipment) are logging into a central log server
- All Ingenico production systems must be set to log key & critical events. These logs must be centralized, appropriately secured and kept for a minimum of 12 months.
- User lifecycle management procedures have been implemented to assign, deploy user rights in alignment with the specific assign function and revocation user rights and deactivation of user account upon leaving the company.
- Access Authentication to the environment hosting the information systems is based on a two-factor authentication mechanism.
- Ingenico has implemented a formal change management program with a change advisory board (CAB) that evaluates, approves or rejects changes. The CAB is led by a change manager and consists out of members from different departments, such as research & development, security, operations, etc.

Data Access

The objective(s)

Persons entitled to use data processing systems gain access only to the data that they are authorized to access. The authorized persons need to be trustworthy and need to handle the data in accordance with their classification. Measure(s) include(s):

- Data access is granted by the “Need-To-Know and Need-to-Use” principles in alignment with the job function/role.
- The production environment is separate from the development, integration and testing environment.
- Ingenico employs data minimization principle and where appropriate and practical, pseudonymizing is used to reduce the likelihood of inappropriate access to personal data.
- Information is disposed of in accordance to its classification level and by following the established procedure(s)
- Ingenico will perform background verification on all employees. Ingenico shall be required to perform the following background verification checks on all employees recruited/hired with access to any assets before they start work activities]:
    - Proof of legal right to work;
    - Proof of legal address;
    - Identity verification (passport or similar document);
    - Confirmation of claimed academic and professional qualifications;
    - Verification (for completeness and accuracy) of the applicant’s curriculum vitae;
    - Criminal record or review;
    - Certificate of Good Conduct or an equivalent certificate depending on the country, from the relevant police authority

Data Transmission

The objective(s):

Prevent data from being read, copied, altered or deleted by unauthorized parties during transfer. Measure(s) include(s):

- Customer access to the payment platform and end customer (card holder) payment request are protected through strong encryption protocols and ciphers; e.g. HTTPS with Transport Layer Security (TLS)
- The strength of the TLS is closely monitored, so that no weak ciphers and protocols are allowed.
- Data is exchanged based on secure protocols agreed between Ingenico and the Financial Institutions.

Vulnerability Management

The objective(s):

Prevent systems from being compromised by reducing the attack surface using vulnerability detection and timely system patching.

Measure(s) include(s):

- Ingenico will establish and maintain up-to-date protection against malicious code.
- The Ingenico systems must be patched on monthly basis. A risk-based approach can be used with high risk security patch being installed within a month and medium risk security patch within three months.
- Where updates cannot be applied to a system, Ingenico deploys appropriate security countermeasures to protect the vulnerable systems.
- The Ingenico systems have a firewall enabled and configured according to standards.
- Ingenico has controls in place to ensure that the ability to use USBs or portable media is restricted. Monitoring controls must be in place to detect and block (where appropriate) the use of USBs or portable media.
- Ingenico performs internal network vulnerability scans on a regular basis.
- Penetration tests are performed on a regular basis.

Secure Development Life Cycle

The objective(s):

Prevent against unauthorized, malicious code and ensure robust and secure applications through implementing a secure development life cycle (SDLC). Measure(s) include(s):

- Ingenico will develop software and systems upon Secure Software Development Lifecycle (SDLC) guidelines. The guidelines are based on industry standards and/or best practices, and include (but are not limited to):
  - No production data (Live PANs) is used during testing and development.
  - All source code must be reviewed prior to release.
  - Change control processes and procedures will be followed for all changes to software and systems.
  - Test and development environment will be separate and appropriate access controls will be enforced.
- Code reviews are performed by someone other than the developer of the code to allow for an independent and objective review.
- Code reviews ensure code is developed according to secure coding guidelines and PCI DSS requirements.
- Developers must be trained in secure coding best practices and frameworks.
- All code changes are documented and monitored and can be linked to the developer that initiated the code changes.

Incident Management

The objective(s):In the event of any security breach of personal data, the effect of the breach is minimized and the stakeholders are promptly informed. Measure(s) include(s):

- Ingenico maintains an up-to-date incident response plan that includes responsibilities, how information security events are assessed and classified as incidents and response plans and procedures.
- Ingenico logs administrator and user activities at the production data center to provide evidence in the event of an incident.
- The clocks of all systems at the production data center are synchronized to a reference time source to support time tracking of activities and logs in the event of an incident.
- Ingenico regularly tests its incident response plan and learns from tests and potential incidents to improve the plan.
- In the event of a security breach, Ingenico will notify the impacted stakeholders within an acceptable time after becoming aware of the security breach.

Compliance

The objective(s):

Provide a service in alignment with industry rules and regulations. Measure(s) include(s):

- Ingenico conducts regular internal and external audits of its security
- Ingenico takes reasonable steps to ensure that Ingenico workers are aware of and comply with the technical and organizational measures set forth in this document.
- Ingenico provides awareness training for Ingenico workers to educate them on different topics such as compliance, security, PCI DSS, etc.
- Ingenico conducts at least quarterly application vulnerability scan penetration tests on the payment platform.
- Ingenico will maintain its security certification such as PCI DSS.

Business Continuity

The objective(s):

Ensure a high-available service to the customers and reduce platform outages and/or downtime. Measure(s) include(s):

- Ingenico uses a high level of availability at the production data centers so that a failure of a single system or component is unlikely to impact general availability.
- The production platform is deployed over multiple data centers within Europe.
- The production data center has multiple power supplies, generators on-site and with battery back-up to safeguard power availability to the data center.
- The production data center has multiple access points to the Internet to safeguard connectivity.
- The production data center is monitored 24x7x365 for power, network, environmental and technical issues.
- Ingenico has a business continuity plan (BCP) and a disaster recovery plan (DRP) which are tested at least annually.