LYYTI

Lyyti Information Security

Maintaining a high level of information security is our top priority. You can be assured of its safety when you entrust your event data to Lyyti. We are 100% committed to upholding stringent security standards through multiple layers of protection.

With Lyyti, you have all the tools necessary to manage your participant data securely.

Lyyti's Information Security Management System (ISMS) aligns with the ISO/IEC 27001 standard and encompasses a comprehensive range of security measures. These measures include controls, policies, guidelines, plans, and procedures, all designed to safeguard every aspect of our operations.

Lyyti processes data exclusively within EU territory, in strict compliance with GDPR (2016/679). Lyyti's premises have been designed and equipped to comply with strict security regulations.

An operations team constantly guards Lyyti's operability. The team is on duty 24/7, every day of the year. We continuously monitor Lyyti environments to identify and promptly address potential vulnerabilities.

All Lyyti subprocessors are carefully selected to meet our stringent security standards. Each subprocessor is audited annually to ensure compliance and a list of these partners is available on the Lyyti website.

Lyyti’s backup system is robust, encompassing four distinct operational levels that are geographically separated to enhance security.

Our personnel security program mandates that all employees complete annual training in data security and data protection, ensuring our team is well-versed in maintaining the highest standards of information safety

Lyyti Security Program

Company security encompasses all aspects of the company's operations. Security operations safeguard Lyyti's core values, including people, data, reputation, property, assets, and the environment. A primary responsibility of corporate security is to enhance the company's competitiveness by ensuring the confidentiality, integrity, and availability of all processed information.

Physical Security

The Lyyti office is equipped with electronic locks, camera surveillance, and modern burglar alarm systems and is monitored 24/7 by an external security company. Each employee is required to use a personal electronic key for office access. All-access events are logged, monitored and can be audited if necessary.

The hosting provider for Lyyti products adheres to several industry-recognised security standards, such as ISO 9001, SOC 1 Type II, SOC 2 Type II, ISO 27001, ISO 22301, and PCI-DSS. A comprehensive list of the hosting provider's certifications can be found here: https://upcloud.com/data-centres.

Data Classification

Lyyti uses a three-tier data classification model. The criteria for classifying data into these levels, along with guidelines for handling each classification level, are described in our policy documentation. Employees receive regular training on these procedures to ensure proper data handling.

Endpoint Security

All user devices accessing company data are company-issued and have been hardened in a documented manner. These devices are protected against various types of attacks by an XDR solution, which is monitored 24/7. Lyyti employs an MDM solution for endpoint policy control and patching, ensuring that all devices are managed and encrypted. Users are obligated to report any anomalies encountered while using the company's devices.

Lyyti's Acceptable Use Policy outlines the acceptance of company IT resources and company-issued assets and includes the policy violation process.

Security Training

All new employees must complete security and privacy training and pass a related exam on their first day of work. The training content is periodically updated, and all staff are required to successfully complete these updates and pass the corresponding exams within the designated time frames, normally at least annually. The outcomes of these exams are carefully monitored and recorded for accountability purposes.

Developers are trained annually for Secure Software Development practices.

Data encryption

All company-issued devices are encrypted, and customer data is always processed in encrypted format, both at rest and in transit.

Company Security Roles

Lyyti's internal company pages describe all security-related roles and substitutes. The company's secure communication channels include contact details for the security role holders.

Policy description

The company's security documentation comprises several controlled policy documents and guidelines, each of which is assigned to a designated owner with primary responsibility for the review process. These documents undergo an annual review process or in the event of any significant modification to the content. This robust system ensures that the policies and guidelines remain current and aligned with the organization's objectives, goals, and statutory requirements.

Security Breaches and Incident Management

Lyyti maintains documented processes and comprehensive plans for incident management, ensuring continuous monitoring of security breaches with sophisticated solutions. All employees are mandated to promptly report any detected or suspected breaches of information security policies, intrusion attempts, data breaches, theft or loss of hardware, or other security-related events and incidents.

The company reviews its incident management documentation regularly and makes it accessible to all users. The documentation describes communication protocols to be followed during incidents, underlining the importance of swift response to safeguard Lyyti's services and data.

Risk management

Risk management is an integral part of Lyyti's strategic process. It helps the company achieve its targets by ensuring that risks are proportional to risk capacity.

Lyyti has identified and documented various risks in its Risk Register. The risks have been classified and analysed, and action plans are made annually to mitigate them. The CTO, along with the CEO and Compliance team, is responsible for formulating the Risk Management policy and Risk assessment. The management team approves the risk management policy and reviews the process annually.

Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

Lyyti has a Business Continuity Policy supported by a comprehensive Disaster Recovery Plan. This plan ensures that all critical business functions can continue, both during and after a disaster. The primary objective of the Plan is to minimise system downtimes and data losses. These documents are regularly reviewed to ensure their effectiveness.

Vulnerability scans and monitoring

All Lyyti infrastructure, including cloud infrastructure, networks, endpoints, and office properties, undergoes 24/7 operational monitoring. Any anomalies found are classified, documented, and handled according to policies and guidelines.

All environments are scanned against vulnerabilities either online, daily, or weekly, depending on the system.

Penetration Testing

An independent external company executes Penetration testing at least once per year. All possible findings are documented in the electronic systems and handled appropriately. A summary of the latest penetration test, executed by Fraktal Oy in March 2024, is available here: LINK.

Patching Process

Lyyti's production hardware and software are continuously monitored for potential vulnerabilities. According to the CVSS v3.0 Severity Rating system, vulnerabilities classified as 'Critical' or 'High' are patched immediately, while those rated 'Medium' or lower are patched within one month of the patch's release.

Employee and Contractor Security Practices

Lyyti is dedicated to upholding the highest levels of security, starting with the hiring and onboarding processes for both employees and contractors. The company hires only dependable and trustworthy individuals; additionally, each contract includes a confidentiality clause to protect sensitive information.

To ensure security, staff and contractors undergo training and pass assessments before being granted system access. Access is strictly regulated based on job roles, allowing only necessary access to sensitive data.

Furthermore, all staff members must adhere to the company's security policies as a requirement of their employment or contractual agreement. This strict dedication to security practices and policies helps Lyyti safeguard its assets, data, and clients' privacy.

Employee offboarding

When an employee leaves the company, a detailed step-by-step offboarding process is followed. This includes, for example, immediately disabling or deleting the user account on all systems used and wiping the endpoint devices used. All company-issued devices are listed in the asset registers and collected and managed according to documented procedures.

Data Location and subprocessing

All data processed by Lyyti, including subprocessing, is handled within the EU Region. A list of subprocessors used by Lyyti is available at https://www.lyyti.com/en/subprocessors, and all subprocessors are reviewed annually.