fastroi
— Caring together —

Fastroi - ISO 27001 White Paper

White Paper

Published 16 April 2020

fastroi

Table of contents

Disclaimer

The purpose of this white paper is to introduce the key concepts of the ISO 27001 standard and offer materials to support Fastroi's Clients in their efforts determining Fastroi's compliance.

Bear in mind that nothing on this document is intended to provide you with, or should be used as a substitute for legal advice. You should also seek independent legal advice relating to your status and obligations under applicable Information Security and Privacy legislation, as only a lawyer can provide you with legal advice specifically tailored to your situation.

Any questions you may have about this ISO 27001 White Paper or Fastroi's ISO 27001 standard compliance, you can contact our Information Security & Privacy Team at privacy@fastroi.com

1 Introduction to the Fastroi's ISO 27001 certification

Fastroi Oy (later Fastroi in the text) was ISO 27001 certified in November of 2019. This means that Fastroi now complies with the international standard in information security.

Fastroi as a Company, comprehends Information Security and Privacy Management as an essential part of best practices in IT management, which in turn are cornerstones in Company governance.

To Fastroi, information Security and Privacy are key factors of success that enable us to provide the best possible services to our Clients. Fastroi's Information Security Management System (ISMS) is built to fulfill the criteria of ISO 27001 standard requirements:

- Risk Management
- Asset Management
- Human Resource Security
- Access Control Management and Securing physical areas
- Software development and maintenance
- Information Security and Privacy Incident Management
- Communications Management
- Operations Management
- Supplier Information Security Management
- Business Continuity Management
- Disaster Recovery
- Compliance

Fastroi has defined Information Security Policy documentation that is available to our Clients upon request.

You are also able to read more on our certification journey at our website blog.

fastroi

2 The ISO 27001:2013 Certificate

ISO 27001:2013 is an Information Security Management Standard that specifies security management best practices and comprehensive security controls that follow the best practice guidance. This is a widely recognized international security standard, in which Fastroi's Clients have shown a significant interest in.

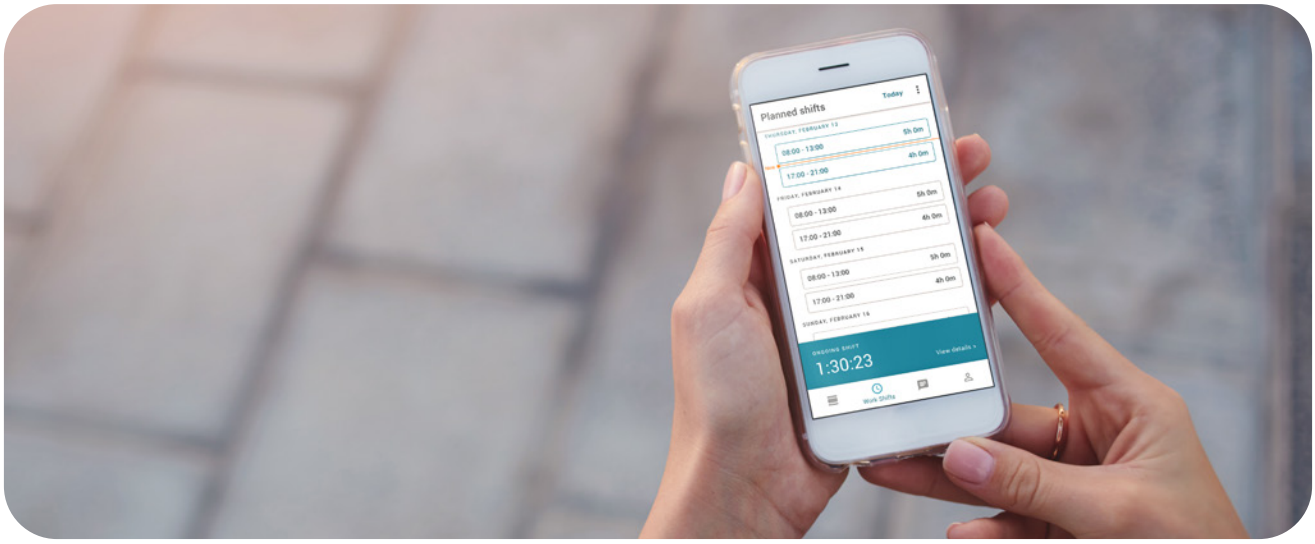
Certification in the standard requires us to continually:

- Systematically evaluate our information security risks, taking into account the impact of the Company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address Company and architecture security risks
- Adopt an overarching Management Process to ensure that the information security controls meet our information security needs on an ongoing basis

The key to certification under this standard was and is the effective management of a rigorous security program. The Information Security Management System (ISMS) required under this standard defines how we continually manage security in a holistic, comprehensive way.

The ISO 27001 certification is specifically focused on the ISMS and measures how our internal processes follow the ISO standard. Certification means a third party accredited independent auditor (DNV GL) has performed an assessment of our Processes and Controls and continually confirms we are operating in alignment with the comprehensive ISO 27001 certification Standard.

It is also worthwhile to mention, that in contrast to the previous editions of the ISO 27001 Standard, the 2013 edition supplements the business-focussed approach with a greater emphasis on demonstrating clear management leadership and support of the ISMS, the application of robust and repeatable risk management and the evaluation and improvement of ISMS effectiveness.



3 The Cornerstones of the Fastroi ISMS

3.1 Product Security

To us, making sure that our Software Products are safe and secure for our Clients is of paramount importance. This means that securing our Software Products and their use are our first priority. Within development, we perform both external and internal testing on our software during the entire development process. Our rigorous internal testing takes place in multiple phases, and to make sure nothing is missed within the development, the testing is taken further with external penetration tests.

3.2 Data Privacy

Fastroi treats the privacy of our Clients' data as a top priority. Due to varying global privacy regulations, our approach is to protect to the most stringent level. We protect the data from workstation to destination using a Transport Layer Security (TLS 1.2) encryption. We have also executed a comprehensive privacy program for our GDPR readiness from which you can read more here.

3.3 Physical Security

The information and IT assets in general are never located in the middle of nowhere. They need security and adequate operating conditions. Softwares have backdoors and many times IT security features are built on "old" and sometimes obsolete physical security principles and solutions. Without proper physical security controls, the information assets are at risk. The ISO 27001 sets out intransigent security controls for the physical environment that must meet the security expectations. Setting up these controls in physical access management, surroundings, and perimeters and borders at Fastroi, happened through providing the adequate level of strength as defined by the risk management activities to each of its elements.

fastroi

4 The Confluence of GDPR and ISO 27001

The European Union General Data Protection Regulation (2016/679), hereinafter "GDPR", was enforced on May the 25th, 2018. The new Data Privacy legislation proposed a new set of obligations to both Data Controllers and Processors. In our privacy program for our GDPR readiness, we took an internationally used accountability framework as the basis of our privacy program work. This has many overlapping areas with the ISO 27001 Standard, so the ISO 27001 certification helped us also to be GDPR Compliant, of which some areas are listed below.

4.1 Risk assessment

The high fines that will be enforced by the new regulations (up to €20 million or up to 4% of annual worldwide turnover of the parent company) could have a major financial impact on any organization. The ISO 27001 Standard requires us to conduct a risk assessment on our information assets, which should consider the increased risk to personal information and potential financial implications. The risk assessment is done periodically and helps us in minimizing the risk and their impacts on our operations.

4.2 Compliance

The GDPR was enforced on late May of 2018 before which all organisations had to review their obligations. The ISO 27001 mandates that we have a list of and comply with relevant legislative, statutory, regulatory and contractual requirements.

4.3 Data classification

Personal data must be processed in a manner that ensures appropriate security. The ISO 27001 requires us to ensure that information always receives an appropriate level of protection in accordance with its importance to the organization.

4.4 Reporting breach notification

Under the GDPR companies have to notify data authorities within 72 hours after a breach of personal data has been discovered. The ISO 27001 requires an incident management process to be put into place with information security events reported through appropriate management channels as quickly as possible.

4.5 Cooperation with authorities

Under the GDPR, organisations must cooperate with the authorities e.g. privacy or data protection regulators. The ISO 27001 requires that "Appropriate contacts with relevant authorities shall be maintained". Within the ISO 27001 certification process, this was included in the Information Security Roles and responsibilities within our organisation.

4.6 Asset management

The GDPR requires companies to understand what personal data they collect, how it is obtained, where it's stored, how long it's kept for and who has access. The ISO 27001 mandates us to identify our organisational assets and define appropriate protection responsibilities. We have completed an inventory of assets with asset owners and defined the acceptable use and retirement processes of those assets.

4.7 Privacy by Design

The adoption of Privacy by Design (PbD) is another GDPR requirement. The ISO 27001 ensures that information security is designed and implemented as an integral part of the entire development and lifecycle of information systems. Within the certification process we utilized an entire set of guidelines of Secure Software Development for our Products' Development Processes.

4.8 Supplier and Service chain relationships

The GDPR applies also to suppliers processing personal data on behalf of others; it requires controls and restrictions to be included in formal agreements. The ISO 27001 standard requires the protection of the organization's assets that are accessible by suppliers and for organizations to monitor the service delivery of suppliers against information security requirements. To make sure our entire Supplier and Service chain is secured, we implemented a set of controls we demand our Suppliers to use in the services they provide to us.

4.9 Documentation

Under EU GDPR, controllers must maintain documentation concerning privacy e.g. for the purposes for which personal information is gathered and processed, "categories"of data subjects and personal data. The ISO 27001 requires documentation to be kept based on the complexity of processes and their interactions.

5 ISO 27001 offers strategic governance

Information Security extends beyond the protection of personal information of our Client's Customers and end-users. The adoption of an ISMS at Fastroi was a strategic decision as the design of the system took into account the other information of value to the Company, such as Company records, the intellectual property of Products and Designs, and sensitive commercial information.

Going forward, the ISO 27001 allows Fastroi to manage the information assets in an organized way, facilitating continuous improvement and adaptation to the changing goals. The standard is about creating and maintaining a structured and comprehensive framework for identifying and assessing security risks, selecting and applying applicable controls and measuring and improving their effectiveness. It helps us to maintain and enhance the Client, Business Partner and Stakeholder confidence in the mature governance of the Company and the resilience of the Business.

6 Other things above and beyond ISO 27001

The ISO 27001 Standard is a great framework in demonstrating that we are committed to Information Security and Privacy.

ISO/IEC 27001 is the international standard that describes the specifications for establishing, implementing, maintaining and continually improving an information security management system. ISO/IEC 27001 applies a risk management approach to securing information and is part of and integrated with the organization's processes and management structure. With its extensive controls, ISO/IEC 27001 helps organizations address the three components of a secure program: people, process and technology.

A holistic approach to information security, ISO/IEC 27001 allows organizations to manage the confidentiality, integrity, and availability of their information assets. Organizations are able to design an "Implement Once, Comply Many" security program, which can aid in protecting, measuring, monitoring, and improving the security across the enterprise and can encompass compliance to the requirements and regulations of a variety of industry-specific security protocols, under one internationally-recognized umbrella.

7 Summary

We want to give our software users all over the world the assurance that their data is securely handled and stored. Information security and privacy are the most important things to us: they have always been among our top priorities both in our operations and in the design of our products. Now we are able to confirm this to you with us obtaining the official ISO 27001 certification. By obtaining the certificate, Fastroi has now proved our compliance with a recognised international security standard.

fastroi

— Caring together —