Always secure
with Fellow Digitals

fellow digitals

Succeeding together

Table of contents

Security in good hands
with Fellow Digitals

In the age of GDPR, data security is essential. Our customers trust that the security of their data and information is always our top priority. In this brochure, you can read how Fellow Digitals meets the highest possible security standards. This way, everyone can work safely no matter where they are.

Concerning security, we do not make any compromises. Since 1997, our customers expect that they can work in a safe and reliable environment. Also when connecting or integrating other platforms or when inviting external users. Our servers are monitored 24/7 by a Dutch hosting provider to ensure that everyone's security remains unaffected.

ISO 27001 is an internationally recognized security standard that specifies requirements for setting up, implementing, maintaining, and continuously improving information security management systems. It is important to know that Fellow Digitals has the NEN 7510 certificate in addition to this, which focusses on information security in the healthcare sector.

Fellow Digitals has also been ISO 27701 certified since 2022. The international standard ISO 27701 provides guidelines for privacy protection, how organizations should manage personal information and it helps with privacy compliance worldwide.

Security, **compliance, and certification**

At Fellow Digitals, the security of your company data is always key. Our servers are hosted in the Netherlands and under 24/7 monitoring. We comply with the EU General Data Protection Regulation (GDPR). This commitment is supported by our ISO/IEC 27001, ISO/IEC 27701, and NEN 7510 certifications.

General Data Protection Regulation

Fellow Digitals' products are hosted in the Netherlands. Our security standards meet the requirements of the EU General Data Protection Regulation (GDPR) and apply to employee, stakeholder, and customer data.

We continuously improve our security measures. In 2022, we achieved ISO/IEC 27701 certification, an extension to ISO/IEC 27001 focused on managing and protecting personal data.

Our employees receive regular training on current data protection regulations, so they have up-to-date knowledge to help safeguard your data.

Fellow Digitals certificates

ISO 27001

Fellow Digitals is ISO 27001 certified. This means that we meet the highest requirements regarding data and information security. Users can use Fellow Digitals' products without worrying about security. With the ISO 27001 certificate, Fellow Digitals presents the following:

- Careful handling of data at all levels
- Compliance with legislation and regulations
- To be a credible and professional company
- Reducing the possibility of risks and incidents

ISO 27701

The ISO 27701 standard is an extension of the ISO 27001 standard for information security and the European data protection regulation (GDPR). It provides specific guidelines for privacy protection and management measures for privacy sensitive data.

This standard provides assurance that Fellow Digitals complies with international requirements for comprehensive personal data protection.

NEN 7510

Where the ISO 27001 standard focuses on 'general' data and information security, the NEN 7510 certificate specifically addresses the protection of medical personal data. The NEN 7510 quality mark is a very relevant certificate for various clients of Fellow Digitals in the healthcare sector.

Security of
hosting and data centres

Personal data, documents, and company information. These are just a few examples of data that can be placed in the Fellow Digitals platforms. This data is stored in a physical location that meets the highest possible security requirements. This reduces the chance of incidents or theft to a minimum.

The servers of Fellow Digitals are hosted and managed by Exonet. Exonet is ISO 27001, ISO 9001, and NEN 7510 certified and therefore meets the highest security standards. The servers are located in BIT's data centre in Ede (the Netherlands). Backups are secured in a second (fallback) data centre: Smartdc in Rotterdam (the Netherlands).

Our servers are equipped with the latest security patches as standard. The servers are behind a firewall, making them inaccessible to hackers and other invaders.

Properties of Exonet (Managed Hosting)

- ISO 27001, ISO 9001, and NEN 7510 certified managed hosting
- Customer focus, customer satisfaction, complaint management
- Service processes, product development
- Quality audits
- Integration of products and open standards
- Service Level Agreement (SLA)
- Uptime of at least 99.9%.
- Hosting and maintenance of the systems
- Test systems, test procedures, and incidents

Properties of BIT and Smartdc (data centre)

- ISO 27001
- NEN 7510
- Fallback location

Fallback location

We are not assuming, but what if one or multiple servers fails due to a calamity? At Fellow Digitals we do not take any risks. That is why we offer a fallback location since 2021. This is a server environment that is identical to the environment in our primary data centre and is also managed by our hosting provider Exonet. In this way, you can access your data at lightning speed.

Physical server protection

- 24/7 occupancy of the Operation Centre
- 24/7 security patrols
- Permanent CCVTV-security
- Security against unauthorised access and alarm protection on site and in the building
- Access to the building and site only via security locks and barriers
- VEB certified protection class 4
- Alternative recovery location

Critical Environment Management

- Experienced management team
- (Thermal) climate control
- Continuous monitoring of building management systems (BMS)
- International recognized Critical Environment Program

Power supply

- Power supply: 50 kV
- Uninterrupted power supply – up to 48 hours at full capacity
- 1,500 W/m2 (possible to increase)

Patch management

Security updates and operating system patches are installed on a daily basis. Urgent hotfixes are carried out on request (emergency maintenance). For each version of Fellow Intranet or Fellow LMS, the code dependencies are updated. To check the patch management process, a third party (i.e. Securify) carries out regular checks. You can read more about this in the section “External audits.”

Digital protection

- SSL/HTTPS-encryption
- Firewalls
- Regular security patches
- Penetration tests
- Year round 24/7 server monitoring
- Management via separate VPN network
- Server virtualization
- Central logging
- Off site backup
- Ecrypted Data Storage

Building and fire protection

- Smoke and fire detectors throughout the building
- Inergen gas (fire extinguisher) in technical departments
- Concrete walls and roof

Server location in the data centre

- Hardware in customized racks in the local data centre in Ede (NL)
- Virtual hardware for increased availability and scalability
- Hardware duplicated

Secure by design software development

Fellow Digitals develops its software according to the secure by design principle. Security and protection of (personal) data form the starting point when designing new functionalities and improvements. In doing so, we follow, among other things, the following guidelines:

- ✓ OWASP Top 10
- ✓ IT security guidelines for web applications of the National Cyber Security Centre

Branch protection

Fellow Digitals makes use of branch protection, which means that adjustments to the software code are always checked according to the four-eye principle before they go into production.

Automated testing

Fellow Digitals uses Selemium automated testing. By continuously performing regression tests, possible errors are detected and corrected at an early stage.

Code reviews

The external agency Securify regularly carries out penetration tests and white box code reviews. With the help of Securify, we proactively detect problems in our software. And we keep up to date with the latest developments in information security.

In addition to regular internal security audits and penetration tests, Fellow Digitals is also happy to help clients with their own tests and penetration tests.

DDoS protection and anti-virus

Denial of service attacks (DDoS) are unfortunately a well-known phenomenon on the internet. However, Fellow Digitals has an intrusion detection system that allows these types of attacks to be quickly detected and contained. In the event of a DDoS attack, traffic is diverted via the Dutch National Wasstraat (NaWas) and delivered “clean.”

Fellow Digitals uses daily updated virus scanners to minimize danger from outside.

Application specific **precaution measures**

Our products Fellow Intranet and Fellow LMS meet the highest security requirements. Both products are equipped with modern technologies to guarantee safe use of the software.

Single sign-on

The Fellow Digitals products offer the possibility to log in with Single sign-on (SSO). Users only need to log in once, after which they can safely and easily switch between the linked systems. Fellow Digitals supports SAML or OpenID Connect to integrate Active Directory, among others.

Two-factor authentication

Fellow Intranet and Fellow LMS support two-factor authentication (2FA). This adds an extra step to the login process. When 2FA is activated, participants are required to enter a temporary PIN code in addition to the username and password, using the Google Authenticator app.

User permissions and roles

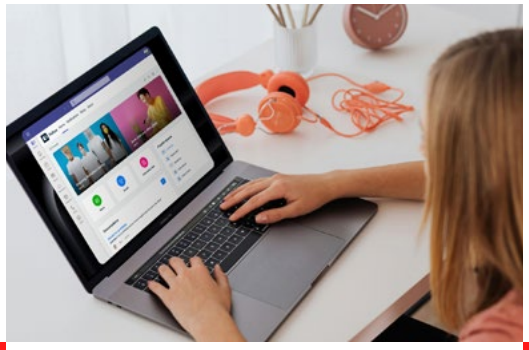
Within Fellow Intranet and Fellow LMS, you have the possibility to set permissions for each user. Our software has a sophisticated authentication model, in which different rights and roles are distinguished.

Single sign-on in practice

On average, an end user uses up to 9 different login codes for all kinds of applications. This leads to situations where employees use the same passwords and store them in poorly secured locations. This is something you want to avoid.

Single sign-on offers a solution to this problem. Thanks to open standards, a secure connection can be established between Fellow Intranet or Fellow LMS with Active Directory, so that you only have to log in once with the same data. This is not only more secure, but also more user-friendly.

This makes it possible to quickly switch between Fellow Intranet, Fellow LMS, and other linked applications such as Office 365.



User permissions in practice

Fellow Intranet and Fellow LMS/LMS+ apply the following levels of rights.

Fellow Intranet

Read- Read documents
Comment - Read and comment on documents
Add - Add documents to the platform
Edit - Edit the content of documents
Manage - All management functions of the platform

Fellow LMS/LMS+

Participant - Participate as learner
Assistant - User and registration management
Author - Content creation and management functions
Auditor - Reviewing content and results
Trainer - Review and provide feedback
Manager - All the above rights plus administration of the academy

Strong password policy

When a participant creates an account with Fellow Intranet or Fellow LMS, it must meet a number of requirements. Such as the length and use of special characters. This makes the account less hack-sensitive.

Automatic account blocking

Our system will automatically block a user account when the maximum number of incorrect login attempts has been reached.

User provisioning API

Via an API connection, it is possible to use user provisioning. This means that participants can be added and removed from the platform in a simple but secure way.

Audit trail logging

The log files of activities are kept on a central server and are thus secure for audits and possible forensic investigations.

Multi-tenant architecture

In a multi-tenant architecture, multiple instances of an application work in a shared environment. This technique ensures that customers can safely use the platform at the same time.

External **audits**

In order to ensure that the security measures taken have the desired effect, Fellow Digitals is regularly monitored by external parties.

Code reviews and Penetration tests

The Netherlands-based company Securify carries out various types of tests several times a year. The security and reliability of the platform is verified. Errors are reported so that they are corrected in time.

- ✓ Penetration test (quarterly)
- ✓ White box code review (annualy)

ISO and NEN

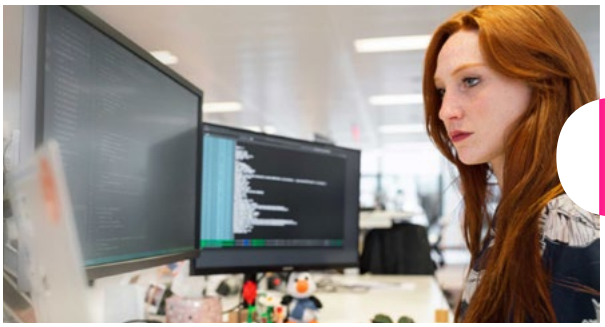
Kiwa is a Dutch organization for testing, inspecting, and certifying products, systems, and processes. This organization is responsible for the annual audits and certification of Fellow Digitals.

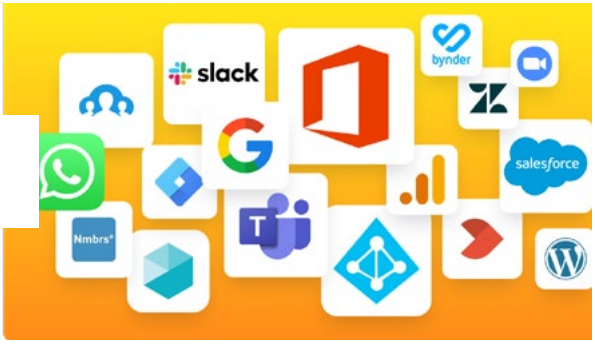
- ✓ ISO 27001
- ✓ ISO 27701
- ✓ NEN 7510

Other **guarantees**

SLA with 99.9% uptime

Fellow Digitals provides its services with a Service Level Agreement (SLA). In this SLA, agreements are made about the quality of our services. We guarantee an uptime of 99.9%, which means that your platform is (almost) always available online.





REST-API

With the industry standard REST-API from Fellow Intranet and Fellow LMS other applications can be easily integrated. In this way, your platform becomes the heart of the digital workplace for all business or learning management processes.

Do you have any **questions?**

We are happy to **help you**

Contact us via info@fellowdigitals.com
or call +31 (0)20 305 76 60

Fellow Digitals bv

Amsterdam Office
Weesperplein 4A
1018 XA Amsterdam
The Netherlands

T: +31 (0)20 305 76 60
www.fellowdigitals.com
info@fellowdigitals.com

Fellow Digitals GmbH

Cologne Office
Brüsseler Str. 25
50674 Cologne
Germany

T: +49 (0)221 828 293 64
www.fellowdigitals.de
info@fellowdigitals.de

Bayern Office
Hauptstrasse 48
83684 Tegernsee
Germany

+49 (0)221 828 293 64
www.fellowdigitals.de
info@fellowdigitals.de

Fellow Digitals Pte. Ltd.

Singapore Office
1 Paya Lebar Link #04-01,
Paya Lebar Quarter
408533 Singapore

T: +65 9155 4446
www.fellowdigitals.com
info@fellowdigitals.com

Succeeding together

fellow digitals