

Information security for our customers

Formcentric is ISO 27001-certified and also has a C5 certificate. In this article, we explain what this means for you and your partnership with Formcentric.

What is ISO 27001 certification?

Corporate information security not only includes protection against cyberattacks or data leaks, for example, but also the handling of security incidents, safeguarding operational security and aspects related to data security. In accordance with the ISO 27001 standard, Formcentric set up an information security management system (ISMS), developed this as part of a continuous improvement process (PDCA cycle) and then commissioned experts from TÜV NORD to perform a corresponding audit. Our ISO 27001 status is regularly recertified and renewed.

What is C5?

C5 (Cloud Computing Compliance Criteria Catalogue) is a set of criteria developed by the German Federal Office for Information Security (BSI) for the purpose of auditing information security for cloud services. The criteria define requirements for the security, transparency and auditability of cloud services. C5 is aimed at cloud service providers, their customers and auditors, and is based on established standards like ISO/IEC 27001, supplemented with specific cloud risks and German compliance requirements (e.g. EU GDPR, IT-Grundschutz from the BSI).

What are the four basic principles of information security?

The primary security objectives for information security are the confidentiality, integrity, availability and authenticity of information.

Confidentiality

Data should only be accessed or modified by authorised users. This principle applies both to accessing stored data and during data transmission.

Integrity

Important data must not be changed 'silently', i.e. all changes must be clearly documented and traceable.

Availability

Access to data must be provided within an agreed period of time.

Authenticity

Information must be authentic and must have clear provenance.

How do you benefit from ISO certification as a customer?

Information security not only prevents financial losses but also protects an organisation's reputation and public image. Our ISO 27001-certified ISMS protects us – and you, as our customer – from IT security incidents (such as cyberattacks) and safeguards the integrity of all of the systems involved. Our certification means we can guarantee our customers first-class information security.

How does our C5 certificate enhance your security?

The C5 certificate from the German BSI supplements ISO 27001 certification by including specific requirements for cloud services. These include transparency obligations, clear rules on the geographical location of data, technical and organisational measures (TOMs), and the handling of security incidents. For you as our customer, this means an additional layer of protection thanks to audited

cloud security according to a recognised national standard, which includes documented test reports and records of compliance with legal requirements – such as the provisions of the EU GDPR.

Detailed benefits for you as a customer include the following:

- All accounts are subject to our access control policy.
We are careful to ensure that we only create accounts that are actually needed. We also conduct regular checks to identify system accounts not being used and to confirm such accounts are still in active use.
- For information transfer, our information transfer policy then comes into play.
Sensitive documents are provided only via a cloud solution that we operate ourselves, with password protection and encrypted data transfer.
- From planning to implementation, our projects comply with our policy for secure software development.
This policy defines how projects are to be initiated, which information is required, how project quality can be assured and how all of the project processes can be represented as transparently as possible.
- We use the PDCA cycle to drive the continuous improvement of our ISMS. This protects our company and yours in equal measure. We live in a fast-paced world and must respond to new challenges as quickly as possible. Our ISMS is a dynamic system and adapts to changing conditions.
- Thanks to our backup strategy, we can restore our systems rapidly in an emergency. Nor do we merely make routine backups and call it a day – we also test these backups regularly.
- We make every effort to ensure that our service providers take information security seriously and have ISO 27001 or similar certification.
We also classify partners and service providers according to their security risk exposure. Those who receive a 'very high' rating must undergo an annual information security audit.
- If a successful cyberattack is made, the contingency planning in our business continuity management system takes effect. This system defines the actions we need to take to secure or restore our business processes. We also provide our customers and partners with regular updates on our current status.
We take regular preventive action that is aimed at preventing a successful cyberattack. As one example, we run pen tests against our systems and have them audited by external experts. We also maintain regular contact with crime agencies and insurers.
- Our non-technical staff complete training programmes several times a year to keep them aware of information security topics.
- Our developers also receive annual training and information security briefings. We also work together with our partners to simulate real-world examples from practice.
- Once a year, our Information Security Officer (ISO) conducts an annual project audit with the respective project managers to confirm compliance with information security requirements.

The exceptional importance attached to information security at Formcentric is also reflected by our staffing structure. Our Information Security Officer Christian Bockrath reports directly to

the Formcentric Management Board. If you have any questions on this topic, please mail us at christian.bockrath@formcentric.com.