xtention
IT with care.

Information security and data protection in health and social care

Your data is safe with us.

Information security and data protection from a single source

Information security and data protection are integral to health and social care systems. Today's healthcare institutions must meet stringent requirements, especially when it comes to protecting confidential patient data. The important questions to consider are whether your current level of security is sufficient and how you can ensure that you comply with laws and standards in the future.

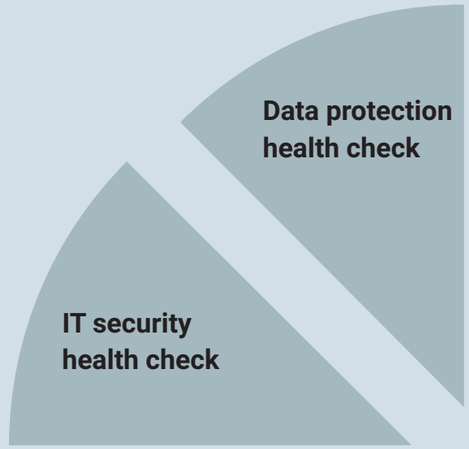
The x-tention group has decades of experience in healthcare IT and is familiar with the particular security requirements of hospitals and social care institutions. Drawing on that expertise, we offer a wide range of information security and data protection services.

Health check

WHAT'S YOUR CURRENT STATUS?

As part of our health check we review your current level of security and data protection. Using that information, we recommend actions and measures that are tailored to your needs.

For more information, see page 5.



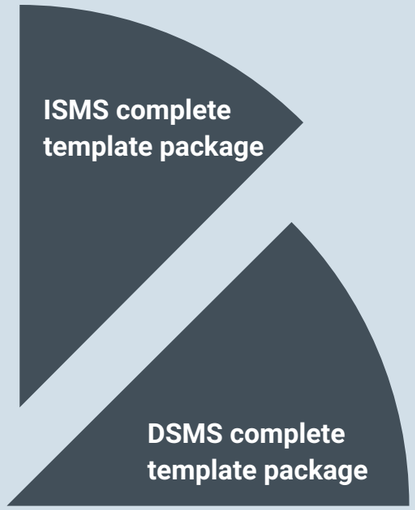
CISO/DPO

HOW CAN YOU SAFEGUARD ONGOING OPERATIONS?

An external chief information security officer (CISO) and external data protection officer (DPO) advise on and monitor compliance with laws and standards. Our specialists answer questions on information security and data protection and ensure that your company undergoes regular audits and holds frequent awareness training.

For more information, see page 14.

'Security is a process, not a product' (Bruce Schneier)

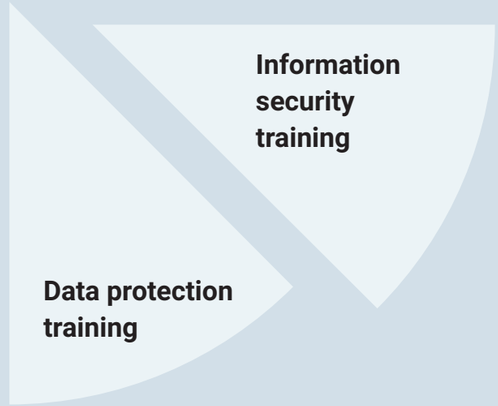


Management system

HOW CAN YOU SET UP AN ISMS/DPMS?

x-tention's tried and tested complete template package allows you to set up an information security or data protection management system. Our comprehensive template packages support you during implementation and ongoing operations. They include boilerplate texts, pre-configured workflows and process descriptions, plus checklists, training concepts, key performance indicators and lots more. They help you quickly and easily track your compliance with laws and standards.

For more information, see page 8.

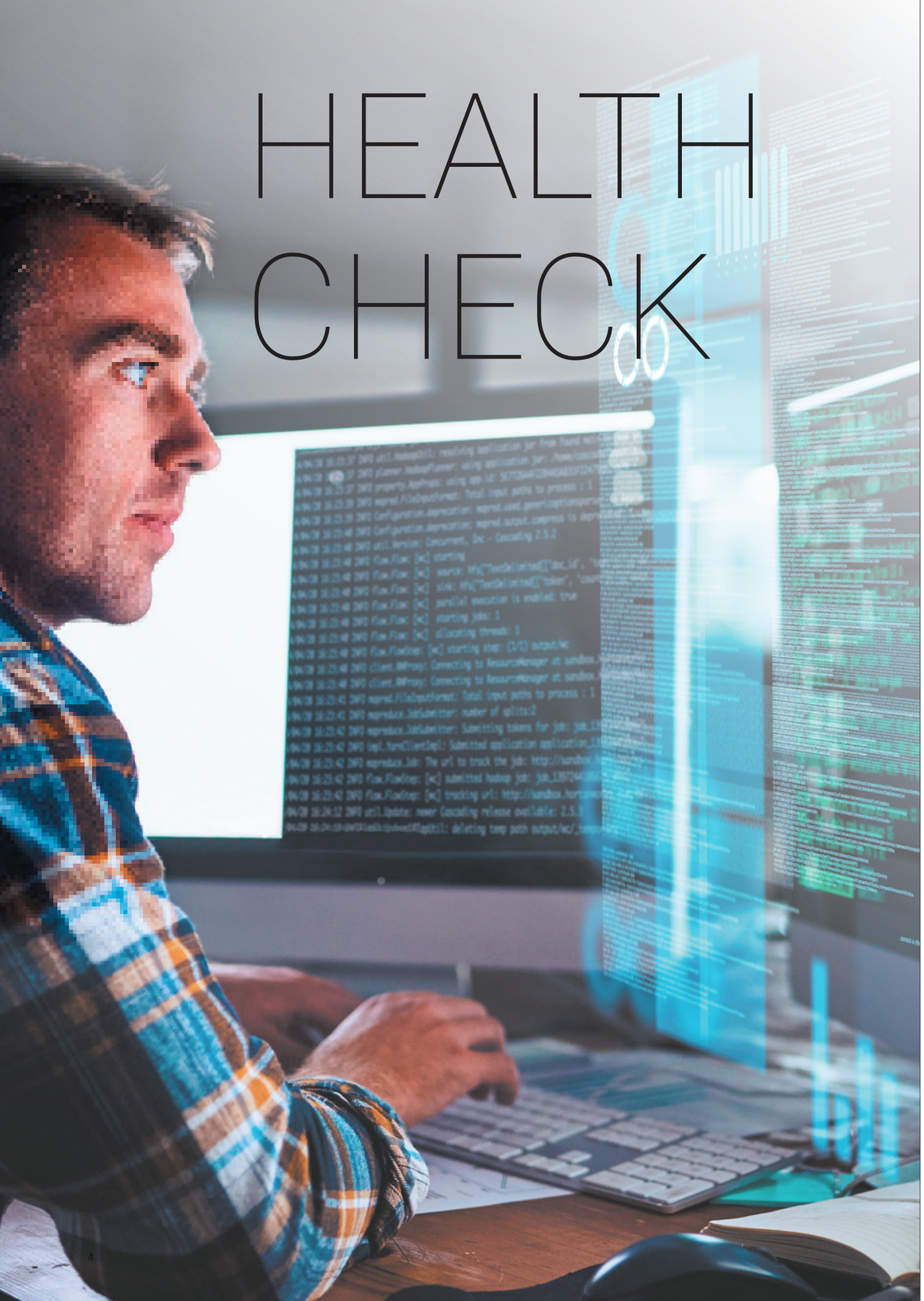


Security awareness

HOW CAN YOU PRESENT THESE TOPICS TO YOUR EMPLOYEES?

Our awareness training sessions and state-of-the-art e-learning platform allow you to train your employees and deepen their understanding of information security and data protection.

For more information, see page 11.



Health check

Do you have adequate information security and data protection?

As part of our health check we review your current level of security and data protection. Using that information, we recommend actions and measures that are tailored to your needs.

To determine your current level of information security or data protection, we provide a Data Protection Health Check and an IT Security Health Check.

These are questionnaires created by x-tention that reveal the big picture of your security and data protection situation in a way that is comparable and management-friendly.

DATENSCHUTZ HEALTH CHECK

IT SECURITY HEALTH CHECK

Results include:

- The full health check with all questions that were discussed
- A management summary of the health check, including findings about potential liability risks and critical areas where action is required
- A management meeting to explain and discuss the results with IT security and data protection experts
- Recommendations for actions and measures to rapidly minimize risks (quick wins) and comply with laws and standards

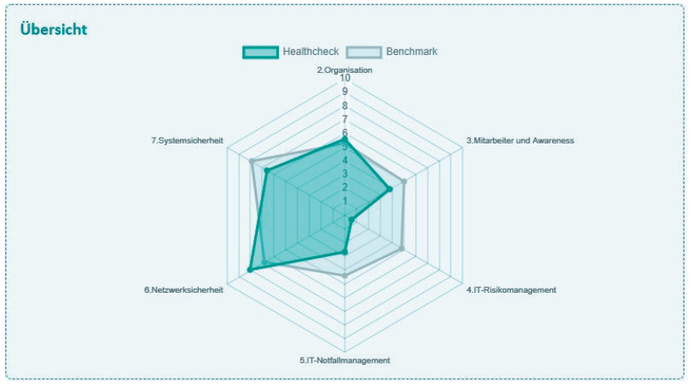
1. Analysis

The analysis is performed during a half-day workshop together with representatives from management, IT and data protection. All critical factors relating to information security and/or data protection are gathered and documented during a face-to-face interview.

2. Benchmark

As well as fulfilling compliance requirements, it is important to measure your own level of information security and data protection against that of other similar health and social care institutions.

The results of your current status analysis are compared with a benchmark. This benchmark reflects the degree to which you currently apply technical and organizational measures for information security and data protection, compared with results from more than 200 selected health and social care institutions in recent years.



The benchmark includes the following results:

- Comparison of your branches (e.g. to define internal minimum security standards)
- Comparison with the health and social care industry average
- Comparison with relevant laws and standards

3. Measures

IT security or data protection experts meet with your management team to explain and discuss the results.

You receive clear recommendations for actions and measures, enabling you to minimize potential liability risks and comply with laws and standards without delay.

You receive:

- Recommended measures to minimize risks without delay
- Tailored security or data protection measures in line with common industry practice
- Recommendations for action related to current and future challenges

Benefits

- **Compact overview**
  The results are presented graphically in clear diagrams, allowing you to see your strengths and opportunities at a glance.
- **Tailored recommendations for action**
  We suggest improvement measures that you can apply straight away, thereby reducing liability risks without delay.
- **Fixed cost**
  The fixed cost includes all appointments, results and recommendations for action. You can either use the result for purely informational purposes or to determine and plan additional measures. You are not committed to anything beyond that.

MANAGEMENT SYSTEM

Information security and data protection management system

Are you fulfilling GDPR and critical infrastructure requirements?

x-tention supports you in implementing specific recommended actions and measures based on your health check. Setting up an extensive information security (ISMS) or data protection management system (DPMS) helps you to comply with laws and standards. In particular, you can quickly and easily track your compliance with the regulations for operators of essential services (OES) in the NIS Directive and with personal data protection measures in the General Data Protection Regulation (GDPR).

Our tried and tested complete template package supports you during the implementation and ongoing operation of an information security or data protection management system. The package includes boilerplate texts, pre-configured workflows and process descriptions, plus checklists, training concepts and lots more.

Step 1 Step 2

Fill in templates

As a starting point for implementing an ISMS or DPMS, you will receive a complete template package that is tailored to the healthcare sector. In addition, our x-tention experts will be on hand to provide support when filling in the templates.

Set up management system

The filled-in documents will allow you to set up the ISMS or DPMS right away, implementing regulations, processes and rules in ongoing operations.

‘We help you set up a practicable ISMS/DPMS – saving you time and money.’

Information security management system (ISMS)

We help you fulfil all requirements in the NIS Directive, in ISO/IEC 27001 and in the German Hospital Federation’s Industry-Specific Security Standards (B3S) for the practical implementation of an ISMS. An excellent basis for ISO/IEC 27001 certification or for a successful compliance audit in line with Section 8a BSI Act.

Policies:
- Information security policy
- Data classification policy
- User policy
- Keyword policy
- Cryptography policy
- Usage policy
- Physical data centre access for third-party companies
- Physical and virtual access policy

Process description:
- ISMS
- Company description
- Backup and recovery
- Monitoring
- Patch management
- Security incident management
- Change management
- Business continuity management
- Data centre infrastructure
- Network and network security
- Anti-malware systems
- Active Directory
- Personnel management
- Requirements management
- Licence management
- Contract management

IT risk management
Audit planning
Management review
Training concept
Key performance indicators
Statement of applicability

Data protection management system (DPMS)

We help you meet statutory requirements contained in the GDPR and in German, Swiss and Austrian data protection legislation regarding the practicable implementation of a DPMS.

Policies:
- User policy
- Data protection policy

Data protection organization
Record of processing activities
Data protection risk assessment
Current status analysis inc. TOMs
Training measures
Audit plan
Data processing
Data subject rights
Data breach
Consent process
Right to be informed
Privacy by design/by default
Deletion concept

Excerpt from the information security policy:

2. Grundsätze

2.1 Management Commitment

Die Geschäftsführung der [Unternehmensbezeichnung] verabschiedet hiermit die Informationssicherheitsrichtlinie (= Leitlinie zur Informationssicherheit) als Bestandteil ihrer Unternehmensstrategie.

Die Geschäftsführung wird die Ziele und Prinzipien der Informationssicherheit in Einklang mit der Geschäftsstrategie und den Geschäftszielen unterstützen.

2.2 Stellenwert der Informationssicherheit

Informationssicherheitsmanagement in Bezug auf Informationssicherheit, Datenschutz und relevante rechtliche, technologische und auch organisatorische Belange wird aktiv von der Geschäftsführung bzw. den hierzu von der Geschäftsführung Beauftragten betrieben.

2.3 Geltungsbereich

Die vorliegende Informationssicherheitsrichtlinie gilt für den Standort [Standort einfügen].

Die Inhalte der Informationssicherheitsrichtlinie bzw. dessen integrierende und ausführende Dokumente sind allen Mitarbeitern im Geltungsbereich zu kommunizieren. Des Weiteren sind alle Mitarbeiter im Geltungsbereich zur Einhaltung der in der Informationssicherheitsrichtlinie festgelegten Bestimmungen verpflichtet sowie externe Auftragnehmer zu verpflichten.

Benefits:

- Our templates contain data based on experience from nearly 10 years of certified ISMS operations.
- Boilerplate texts and content are pre-formulated and have extensive commentary.
- You can rely on support from experts with in-depth knowledge of the health and social care sector.
- You save considerable time and effort when setting up your ISMS.
- This is an excellent basis for ISO/IEC 27001 certification and successful verification in accordance with Section 8a BSI Act.
- No special software is required – you only need Microsoft Office.

SECURITY AWARENESS

Security awareness

State-of-the-art training on information security and data protection

You can only reach a unified level of security by keeping your staff up to date with information security and data protection topics. For that reason, all employees should receive proper up-to-date training at regular intervals.

E-learning platform

As well as interactive workshops, x-tention supports you with a state-of-the-art training platform where employees can find out and learn about all of the topics important to your company. You can use the platform as an internal and interactive tool for communication between training officers, decision makers and employees.

The big advantage:

Employees can access e-learning courses at any time, from wherever they are. They can even access security awareness training sessions online from home or while out and about using their smartphone.

Knowledge check using questions

(e.g. short multiple-choice questions)

Include videos

Evaluations with export options

Customizable design and modular course system

Flexible content design

Interactive SCORM modules

Our e-leaning content:

- Basic information about data protection (GDPR, German Data Protection Act)
- Use of passwords
- Spam and phishing
- Use of smartphones
- Ransomware
- Social engineering
- Use of mobile data carriers
- Clear desk policy

Benefits

- **You are not tied to a particular time or place**
  Employees can take an awareness training session wherever they are and whenever they have time, including from home or using their smartphone.
- **Time investment of less than 5 minutes per month**
  E-learning content is provided at short, regular intervals, so staff do not need to break away from their work.
- **No licensing costs**
  There are no licensing fees to use the e-learning platform as it is based on open-source products.
- **Staff are not required to create content**
  x-tention provides course content and tailors it to your company's needs, so you do not have to spend time designing courses.
- **Ongoing, practice-oriented awareness training for employees**
  We help deepen employees' knowledge by continuing to raise their awareness and focus on content that is important to you. Awareness training sessions are practice-oriented, including example cases as well as numerous tips and tricks for overcoming challenges both at work and in private life.

External chief information security officer
External data protection officer

We take care of your information security and data protection

The external chief information security officer (CISO) and the external data protection officer (DPO) advise on and monitor regulations, laws and standards. They answer questions on information security and data protection and ensure that your company undergoes regular audits and holds frequent awareness training sessions.

External chief information security officer (CISO)

- You have access to a team of experts with in-depth knowledge
- Quick answers to your information security questions

Ongoing tasks:

- We provide information and advice on information security questions
- We inform and advise you about laws and standards related to information security and the state of the art
- We advise on and monitor the operation of company-wide IT risk management
- We coordinate and support you in solving problems and incidents related to IT security
- We assess IT security risks based on the state of the art
- We write concise statements with a focus on information security

Regular services:

- Annual security awareness training sessions
- Annual security audit
- Regular information security sessions at your location
- Annual management meeting

External data protection officer (DPO)

- You have access to a team of experts with in-depth knowledge
- Quick answers to your data protection questions

Ongoing tasks:

- We inform and advise our clients about GDPR obligations
- We monitor compliance with the GDPR, with other data protection regulations and with clients' strategies for protecting personal data
- We are a first point of contact for data subjects
- We provide consulting related to data protection impact assessments
- We work together with the data protection authority
- We write concise statements with a focus on data protection

Regular services:

- Annual data protection awareness training sessions
- Annual data protection audit
- Regular data protection sessions at your location
- Annual management meeting

'We take care of your information security and data protection so that you can concentrate on your core activities.'

Our certifications:

x-tention's data centre operations have been fully certified in accordance with **ISO/IEC 27001** since the beginning of 2011. Since then, x-tention has run an appropriate and **TÜV-certified information security management system (ISMS),** including IT risk management.

In December 2018 x-tention became the first company to be awarded the TÜV Austria 'Verified Data Protection Management System' certificate, which was converted into an **ISO/IEC 27701:2019 certificate** in November 2021.

x-tention's quality management system has been TÜV-certified in accordance with **ISO 9001** since 2019.

x-tention group

How to get in touch

x-tention Informationstechnologie
AT +43 7242 2155 office@x-tention.at
DE +49 6221 360550 office@x-tention.de
CH +41 43 222 60 22 office@x-tention.ch
UK +44 203 983 9860 office@x-tention.co.uk

soffico
DE +49 821 455 901 00 info@soffico.de

FAKTOR D consulting
DE +49 821 455 9021 00 info@xd-consulting.de

it for industries
AT +43 7242 2155 0 office@itforindustries.at

Cloud21 Ltd
UK +44 845 838 8694 info@cloud21.net

Michael Punz
Information Security and Data Protection

Telephone +43 7242 2155 6325
Mobile +43 664 80009 6325
Email michael.punz@x-tention.at