xtention
IT with care.

Informationssicherheit und Datenschutz im Gesundheits- und Sozialwesen

Ihre Daten sind bei uns sicher.

Informationssicherheit und Datenschutz aus einer Hand

Informationssicherheit und Datenschutz sind aus dem Gesundheits- und Sozialwesen nicht mehr wegzudenken. Besonders der Schutz vertraulicher Patientendaten stellt hohe Anforderungen an eine moderne Gesundheitseinrichtung. Entscheidend sind dabei die Fragen, ob Ihr derzeitiges Sicherheitsniveau ausreichend ist und wie Sie zukünftig die Einhaltung der gesetzlichen und normativen Vorgaben sicherstellen können.

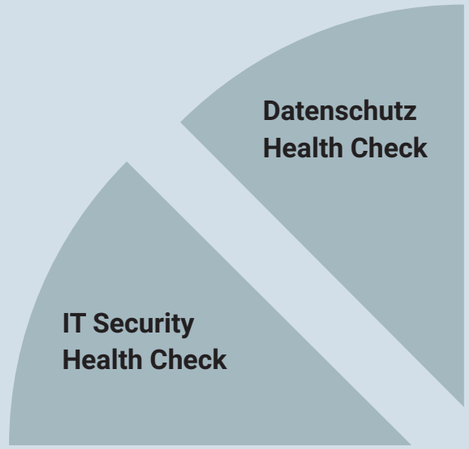
Die x-tention Unternehmensgruppe verfügt über jahrzehntelange Erfahrung in der Gesundheits-IT und kennt die speziellen Sicherheitsanforderungen von Krankenhäusern und sozialen Einrichtungen. Darauf aufbauend bieten wir Ihnen ein breites Sortiment an Dienstleistungen im Bereich Informationssicherheit und Datenschutz.

Health Check

WO STEHEN SIE?

Im Rahmen unseres Health Checks wird Ihr aktuelles Sicherheits- oder Datenschutzniveau überprüft. In der Folge werden daraus maßgeschneiderte Handlungs- und Maßnahmenempfehlungen für Sie abgeleitet.

Mehr Informationen finden Sie auf Seite 5.

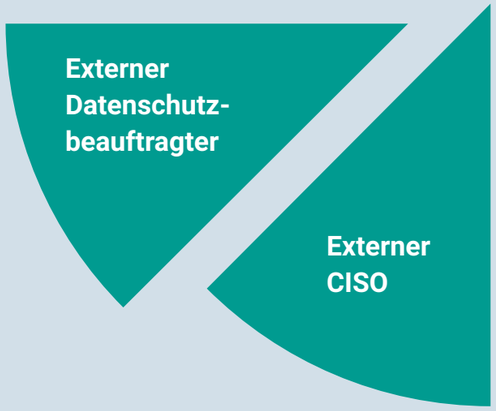


CISO/DSB

WIE KÖNNEN SIE DEN LAUFENDEN BETRIEB SICHERSTELLEN?

Der externe Informationssicherheitsbeauftragte (CISO) und der externe Datenschutzbeauftragte (DSB) beraten und überwachen die Einhaltung gesetzlicher und normativer Vorgaben für Sie. Unsere Spezialisten geben Antworten auf Fragen zur Informationssicherheit und zum Datenschutz und sorgen für regelmäßige Audits und Awareness-Trainings in Ihrem Unternehmen.

Mehr Informationen finden Sie auf Seite 14.



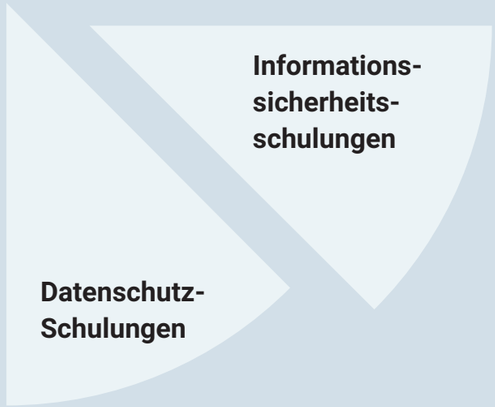
„Security is a process, not a product.“ (Bruce Schneier)

Management-system

WIE KÖNNEN SIE EIN ISMS/DSMS AUFBAUEN?

Das praxiserprobte Vorlagen-Komplettpaket von x-tention ermöglicht den Aufbau eines Managementsystems für Informationssicherheit oder Datenschutz. Unsere umfassenden Vorlagenpakete bestehend aus vorformulierten Textbausteinen, vorgefertigten Prozessabläufen und Prozessbeschreibungen sowie Checklisten, Schulungskonzepten, Kennzahlen und vielem mehr unterstützen Sie optimal bei der erfolgreichen Einführung und im laufenden Betrieb. Gesetzliche und normative Vorgaben lassen sich damit schnell und einfach abbilden und einhalten.

Mehr Informationen finden Sie auf Seite 8.

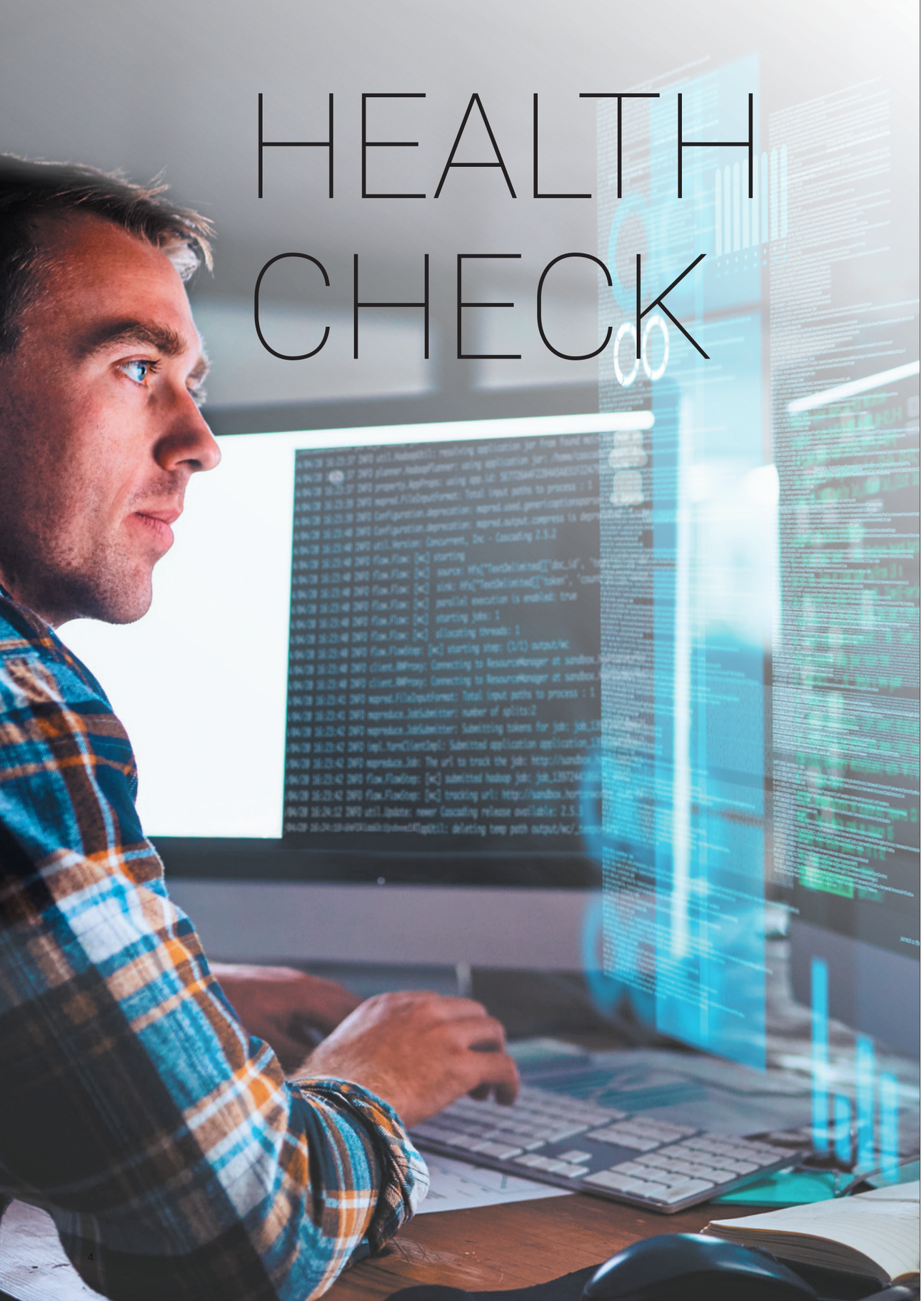


Security Awareness

WIE BRINGEN SIE DIE THEMEN ZU IHREN MITARBEITERN?

Unsere Awareness-Trainings und unsere eLearning-Plattform ermöglichen moderne Wissensvermittlung und Bewusstseinsbildung zum Thema Informationssicherheit und Datenschutz.

Mehr Informationen finden Sie auf Seite 11.



Health Check

Haben Sie ein angemessenes Informations-sicherheits- und Datenschutzniveau?

Im Rahmen unserer Health Checks wird Ihr aktuelles Sicherheits- oder Datenschutzniveau überprüft. In der Folge werden daraus maßgeschneiderte Handlungs- und Maßnahmenempfehlungen für Sie abgeleitet.

Zur Erhebung des aktuellen Informationssicherheits- oder Datenschutzniveaus stehen Ihnen der Datenschutz und der IT Security Health Check zur Verfügung.

Dabei handelt es sich um Fragenkataloge – entwickelt von x-tention –, die ein vergleichbares und managementtaugliches Gesamtbild Ihres Sicherheits- und Datenschutzniveaus darstellen.

DATENSCHUTZ HEALTH CHECK

IT SECURITY HEALTH CHECK

Als Ergebnis erhalten Sie:

- Den vollständigen Health Check mit allen besprochenen Fragen
- Eine Management-Summary zum Health Check mit den Ergebnissen zu möglichen Haftungsrisiken und kritischen Bereichen mit Handlungsbedarf
- Management-Meeting zur Erläuterung und Diskussion der Ergebnisse mit IT-Sicherheits- und Datenschutzexperten
- Handlungs- und Maßnahmenempfehlungen zur umgehenden Risikoreduktion (Quick Wins) und Einhaltung gesetzlicher und normativer Vorgaben

Schritt 1
Analyse

Schritt 2
Benchmark

Schritt 3
Maßnahmen

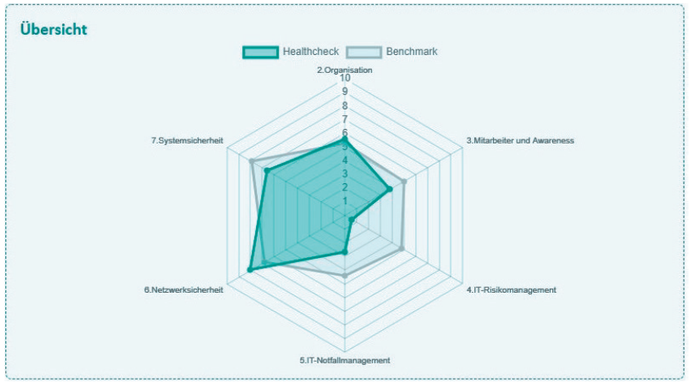
1. Analyse

Die Analyse wird im Rahmen eines halbtägigen Workshops gemeinsam mit Ihren Ansprechpartnern aus Management, IT und Datenschutz durchgeführt. Alle kritischen Faktoren zum Thema Informationssicherheit bzw. Datenschutz werden in Form eines persönlichen Interviews erhoben und dokumentiert.

2. Benchmark

Von besonderer Relevanz ist neben der Erfüllung der Compliance-Anforderungen auch die Einstufung des eigenen Informationssicherheits- bzw. Datenschutzniveaus im Vergleich zu anderen vergleichbaren Einrichtungen im Gesundheits- und Sozialwesen.

Die Ergebnisse aus der Analyse der Ist-Situation werden einem Benchmark unterzogen. Dieser Benchmark spiegelt den aktuellen Umsetzungsgrad von technischen und organisatorischen Maßnahmen hinsichtlich Informationssicherheit bzw. Datenschutz im Vergleich zu mehr als 200 ausgewählten Einrichtungen im Gesundheits- und Sozialwesen aus den letzten Jahren wider.



Der Benchmark beinhaltet folgende Ergebnisse:

- Vergleich Ihrer Standorte zueinander (z. B. zur Definition von internen Sicherheits-Mindeststandards)
- Vergleich zum Branchen-Durchschnitt aus dem Gesundheits- und Sozialwesen
- Vergleich zu relevanten gesetzlichen und normativen Vorgaben

3. Maßnahmen

Im Rahmen eines Management-Termins werden die Ergebnisse von IT-Sicherheits- oder Datenschutzexperten erläutert und gemeinsam mit Ihrem Management diskutiert.

Sie erhalten klare Handlungs- und Maßnahmenempfehlungen zur umgehenden Reduktion möglicher Haftungsrisiken und zur Einhaltung gesetzlicher und normativer Vorgaben.

Sie erhalten:

- Maßnahmenempfehlungen zur umgehenden Risikoreduktion
- Maßgeschneiderte und branchenübliche Sicherheits- oder Datenschutzmaßnahmen
- Handlungsempfehlungen für aktuelle und zukünftige Herausforderungen

Ihre Vorteile

- **Kompakter Überblick**
  Durch die grafische Darstellung der Ergebnisse in aussagekräftigen Diagrammen sehen Sie auf einen Blick Ihre Stärken und Potenziale.
- **Maßgeschneiderte Handlungsempfehlungen**
  Wir liefern Vorschläge für Verbesserungsmaßnahmen, die Sie direkt umsetzen können. Somit ist es möglich, Haftungsrisiken unverzüglich zu reduzieren.
- **Fixpreis**
  Alle Termine, Ergebnisse und Handlungsempfehlungen sind im Fixpreis inkludiert. Sie können das Ergebnis entweder rein informativ verwenden oder weitere Maßnahmen daraus ableiten und planen. Sie gehen keine weiteren Verpflichtungen ein.

MANAGEMENT-SYSTEM

Informationssicherheits- und Datenschutz-Managementsystem

Erfüllen Sie die KRITIS- und DSGVO-Vorgaben?

x-tention unterstützt Sie bei der Umsetzung konkreter Handlungs- und Maßnahmenempfehlungen basierend auf Ihrem Health Check. Mit dem Aufbau eines umfassenden Informationssicherheits- oder Datenschutz-Managementsystems (ISMS bzw. DSMS) lassen sich gesetzliche und normative Vorgaben einhalten. Besonders die Einhaltung der Vorgaben aus der NIS-Richtlinie für Betreiber „kritischer Infrastrukturen" (KRITIS) sowie Maßnahmen zum Schutz personenbezogener Daten aus der Datenschutzgrundverordnung (DSGVO) lassen sich schnell und einfach abbilden.

Das praxiserprobte Vorlagen-Komplettpaket von x-tention bestehend aus vorformulierten Textbausteinen, vorgefertigten Prozessabläufen und Prozessbeschreibungen sowie Checklisten, Schulungskonzepten und vielem mehr unterstützt Sie optimal bei der erfolgreichen Einführung und im laufenden Betrieb eines Informationssicherheits- oder Datenschutz-Managementsystems.

Schritt 1 Schritt 2

Vorlagen befüllen

Als Basis für die Einführung eines ISMS oder DSMS in Ihrer Organisation erhalten Sie ein Vorlagen-Komplettpaket, das auf den Gesundheitsbereich zugeschnitten ist. Zusätzlich stehen Ihnen bei der Befüllung der Vorlagen die Experten von x-tention gerne zur Seite.

Managementsystem einführen

Mit den befüllten Dokumenten können Sie das ISMS bzw. DSMS unmittelbar einführen und Richtlinien, Prozesse und Vorgaben im laufenden Betrieb ein- bzw. umsetzen.

„Wir helfen Ihnen, ein praxistaugliches ISMS/DSMS aufzubauen – Sie sparen Zeit und Geld."

Informationssicherheits-Managementsystem (ISMS)

Erfüllung aller Anforderungen der KRITIS-V/NIS-Richtlinie, der ISO/IEC27001 sowie der B3S der DKG zur praxistauglichen Umsetzung eines ISMS. Hervorragende Grundlage für eine Zertifizierung nach ISO/IEC27001 bzw. für einen erfolgreichen Nachweis gemäß § 8a BSIG.

Richtlinien:
- Informationssicherheitsrichtlinie
- Datenklassifizierungsrichtlinie
- Benutzerrichtlinie
- Kennwortrichtlinie
- Kryptographierichtlinie
- Nutzungsrichtlinie
- Rechenzentrumszutritt für Drittfirmen
- Zugriffs- und Zutrittskontrollrichtlinie

Prozessbeschreibung:
- ISMS
- Unternehmensbeschreibung
- Backup und Recovery
- Monitoring
- Patch Management
- Security Incident Management
- Change Management
- Business Continuity Management
- Rechenzentrumsinfrastruktur
- Netzwerk und Netzwerksicherheit
- Anti-Malware-Systeme
- Active Directory
- Personalmanagement
- Anforderungsmanagement
- Lizenzmanagement
- Vertragswesen

IT-Risikomanagement
Auditplanung
Management Review
Schulungskonzept
Kennzahlen
Statement of Applicability

Datenschutz-Managementsystem (DSMS)

Erfüllung der gesetzlichen Anforderungen der DSVGO sowie der nationalen Datenschutzgesetze in Deutschland, Schweiz und Österreich zur praxistauglichen Umsetzung eines DSMS.

Richtlinien:
- Benutzerrichtlinie
- Datenschutzrichtlinie

Datenschutzorganisation
Verfahrensverzeichnis
Datenschutz-Folgenabschätzung
Ist-Analyse inkl. TOMs
Schulungsmaßnahmen
Auditplan
Auftragsverarbeitung
Betroffenenrechte
Data Breach
Einwilligungsprozess
Informationspflichten
Privacy by Design / by Default
Löschkonzept

Auszug aus der Informationssicherheitsrichtlinie:

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.

Ihre Vorteile:

- Unsere Vorlagen enthalten Erfahrungswerte aus knapp 10 Jahren zertifiziertem ISMS-Betrieb.
- Textbausteine und Inhalte sind umfassend vorformuliert und kommentiert.
- Experten mit fundiertem Know-how aus dem Gesundheits- und Sozialwesen stehen Ihnen zur Seite.
- Deutliche Zeitersparnis und Aufwandsreduktion beim ISMS-Aufbau.
- Perfekte Basis für eine ISO/IEC 27001-Zertifizierung und einen erfolgreichen Nachweis gemäß § 8a BSIG.
- Keine Spezialsoftware notwendig – Sie benötigen nur Microsoft Office.

SECURITY AWARENESS

Security Awareness

Moderne Wissensvermittlung zum Thema Informationssicherheit und Datenschutz

Ohne eine durchgängige Bewusstseinsbildung und Sensibilisierung der Mitarbeiter kann kein ganzheitliches Sicherheitsniveau erreicht werden. Daher sollten alle Mitarbeiter angemessen, zeitgemäß und in regelmäßigen Intervallen geschult werden.

eLearning-Plattform

Neben interaktiven Workshops unterstützt Sie x-tention mit einer zeitgemäßen Trainingsplattform zur Steigerung des Sicherheitsbewusstseins Ihrer Mitarbeiter und zur nachhaltigen Wissensvermittlung für all jene Themen, die in Ihrem Unternehmen wichtig sind. Die Plattform kann als internes und interaktives Kommunikationswerkzeug zwischen Schulungsverantwortlichen, Entscheidungsträgern und Mitarbeitern eingesetzt werden.

Das große Plus:

Die eLearning-Kurse können von den Mitarbeitern orts- und zeitunabhängig durchgeführt werden. Dies geht so weit, dass die Security-Awareness-Trainings sogar von zuhause über das Internet oder von unterwegs via Smartphone absolviert werden können.

Wissensüberprüfung mit Hilfe von Fragen

(wie z. B. kurze Multiple-Choice-Fragen)

Einbinden von Videos

Auswertungen mit Export-möglichkeiten

Anpassbares Design und modulares Kurssystem

Freie Inhalts-gestaltung

Interaktive SCORM-Module

Unsere eLearning-Inhalte:

- Grundinformationen zum Datenschutz (DSGVO, DSG)
- Umgang mit Passwörtern
- Spam und Phishing
- Umgang mit Smartphones
- Ransomware
- Social Engineering
- Umgang mit mobilen Datenträgern
- Clear Desk

Ihre Vorteile

- **Örtliche und zeitliche Unabhängigkeit**
  Die Awareness-Trainings können von den Mitarbeitern genau dort, wo sie sich örtlich gerade befinden, und wann sie Zeit dazu haben, d. h. auch von zuhause oder via Smartphone, durchgeführt werden.
- **Zeitaufwand pro Mitarbeiter von weniger als 5 Minuten pro Monat**
  Die eLearning-Inhalte werden in kurzen, regelmäßigen Intervallen zur Verfügung gestellt. Für die Mitarbeiter ist dabei keine Arbeitsunterbrechung erforderlich.
- **Keine Lizenzkosten**
  Für die Nutzung fallen keinerlei Lizenzgebühren an, da die eLearning-Plattform auf Open-Source-Produkten basiert.
- **Keine Personalressourcen zur Inhaltserstellung erforderlich**
  Die Kursinhalte werden Ihnen von x-tention zur Verfügung gestellt und individuell für Ihr Unternehmen angepasst. Sie müssen daher keine Zeit aufwenden, um die Kurse zu gestalten.
- **Kontinuierliches und praxisorientiertes Awareness-Training der Mitarbeiter**
  Das Bewusstsein Ihrer Mitarbeiter wird durch kontinuierliche Sensibilisierung und Thematisierung der für Sie wichtigen Inhalte gestärkt. Die Awareness-Trainings sind praxisorientiert und enthalten neben vielen Beispielen auch zahlreiche Tipps und Tricks für die Herausforderungen im beruflichen wie auch im privaten Alltag.

Externer Chief Information Security Officer
Externer Datenschutzbeauftragter

Wir kümmern uns um die Sicherheit und den Schutz Ihrer Daten

Der externe Chief Information Security Officer (CISO) und der externe Datenschutzbeauftragte (DSB) beraten und überwachen Vorschriften bzw. gesetzliche und normative Vorgaben. Sie geben Antworten auf Fragen zur Informationssicherheit und zum Datenschutz und sorgen für regelmäßige Audits und Awareness-Trainings.

Externer Chief Information Security Officer (CISO)

- Ein Team von kompetenten Experten mit fundiertem Know-how steht Ihnen als Ansprechpartner zur Verfügung
- Schnelle Antworten auf Ihre Fragen zum Thema Informationssicherheit

Laufende Aufgaben:

- Auskunft und Beratung zu Informationssicherheitsfragen
- Unterrichtung und Beratung zu gesetzlichen und normativen Vorgaben hinsichtlich Informationssicherheit und Stand der Technik
- Beratung und Kontrolle beim Betrieb eines unternehmensweiten IT-Risikomanagements
- Koordination von und Unterstützung bei der Behebung von IT-sicherheitsrelevanten Problemen und Sicherheitsvorfällen
- Sicherheitstechnische Einschätzung von IT-Risiken gemäß dem Stand der Technik
- Verfassen von kompakten Stellungnahmen mit dem Fokus auf Informationssicherheit

Regelmäßige Leistungen:

- Durchführung eines jährlichen Sicherheits-Awareness-Trainings
- Durchführung eines jährlichen Sicherheitsaudits
- Durchführung und Koordination regelmäßiger Informationssicherheitstermine vor Ort
- Durchführung eines jährlichen Management-Meetings

Externer Datenschutz-beauftragter (DSB)

- Ein Team von kompetenten Experten mit fundiertem Know-how steht Ihnen als Ansprechpartner zur Verfügung
- Schnelle Antworten auf Ihre Fragen zum Thema Datenschutz

Laufende Aufgaben:

- Unterrichtung und Beratung des Auftraggebers hinsichtlich der Pflichten nach der DSGVO
- Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften sowie der Strategien des Auftraggebers für den Schutz personenbezogener Daten
- Anlaufstelle für Betroffene
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit der Datenschutzbehörde
- Verfassen von kompakten Stellungnahmen mit dem Fokus auf Datenschutz

Regelmäßige Leistungen:

- Durchführung eines jährlichen Datenschutz-Awareness-Trainings
- Durchführung eines jährlichen Datenschutzaudits
- Durchführung und Koordination regelmäßiger Datenschutztermine vor Ort
- Durchführung eines jährlichen Management-Meetings

„Wir kümmern uns um Ihre Informationssicherheit und Ihren Datenschutz, damit Sie sich wieder auf Ihre eigentlichen Kerntätigkeiten konzentrieren können.“

Wir sind als Unternehmen zertifiziert nach:

Der Rechenzentrumsbetrieb von x-tention ist seit Anfang 2011 durchgängig nach **ISO/IEC 27001** zertifiziert und x-tention betreibt seitdem ein angemessenes und vom **TÜV zertifiziertes Informationssicherheits-Managementsystem (ISMS)** inklusive IT-Risikomanagement.

Im Dezember 2018 wurde x-tention als erstes Unternehmen mit dem TÜV-Austria-Zertifikat „Geprüftes Datenschutzmanagementsystem“ ausgezeichnet, welches im November 2021 in ein **ISO/IEC 27701:2019-Zertifikat** überführt wurde.

Seit 2019 ist zudem das Qualitätsmanagementsystem von x-tention vom TÜV nach **ISO 9001** zertifiziert.

x-tention Unternehmensgruppe

Ihr Kontakt zu x-tention

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 Limited
UK +44 845 838 8694 info@cloud21.net

Michael Punz
Informationssicherheit & Datenschutz

Telefon +43 7242 2155 6325
Mobil +43 664 80009 6325
E-Mail michael.punz@x-tention.at