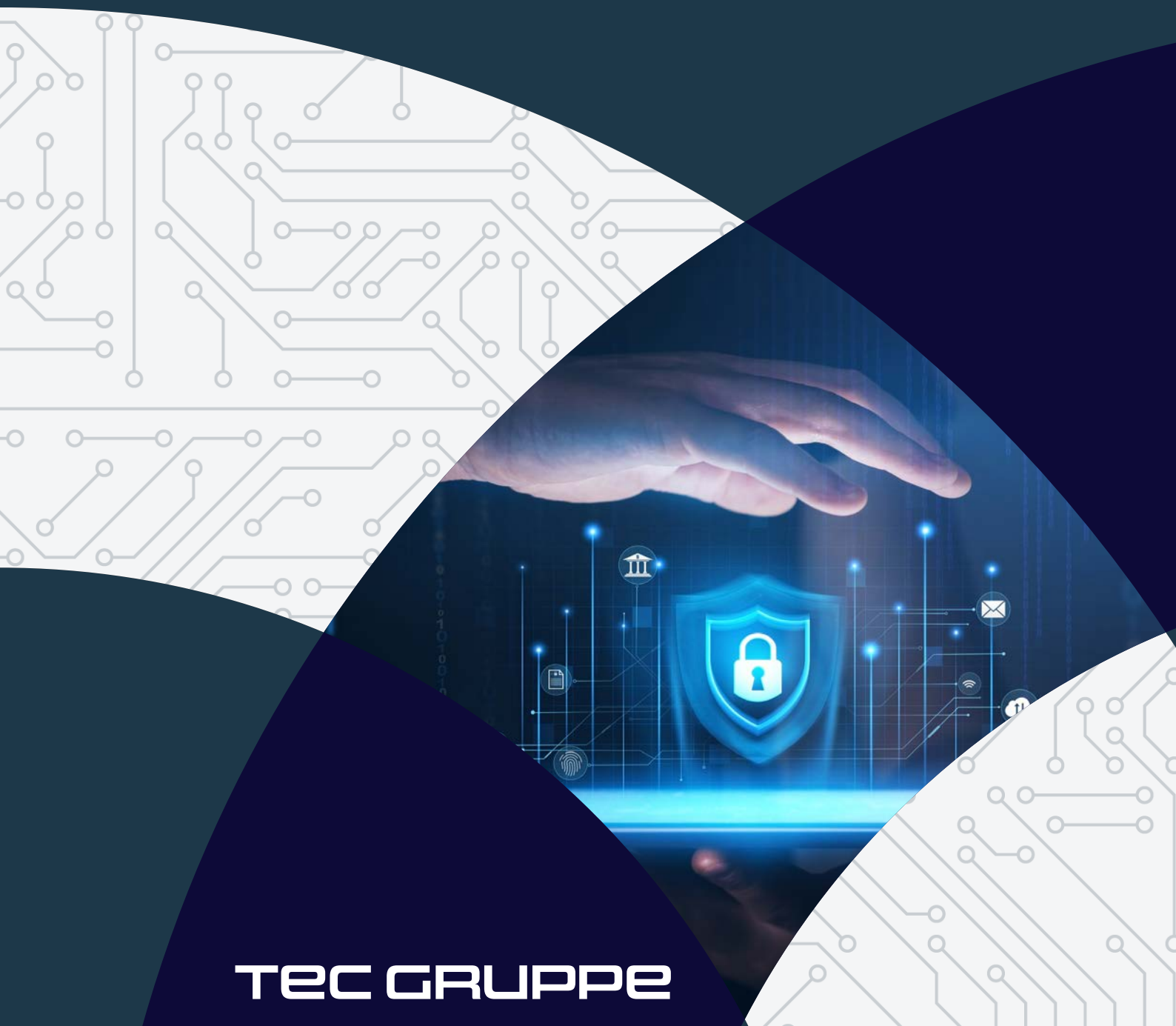
KEIN SCHISS VOR NIS

Mit Ihrer übersichtlichen Checkliste zu NIS haben Sie alles im Blick auf Ihrem Weg zur NIS-Konformität.

Quelle: https://www.nis.gv.at



TEC GRUPPE

IHRE NIS-CHECKLISTE

Kategorien und Sicherheitsmaßnahmen der NIS Verordnung

1. Governance und Risikomanagement

- [ ] **Risikoanalyse**

  Risikoanalyse der Netz- und Informationssysteme durchführen und regelmäßig anpassen

- [ ] **Sicherheitsrichtlinie**

  Sicherheitsrichtlinie erstellen und periodisch aktualisieren

- [ ] **Überprüfungsplan der Netz- und Informationssysteme**

  Planung und Durchführung der periodischen Überprüfung der Netz- und Informationssystemsicherheit

- [ ] **Ressourcenmanagement**

  Kurz-, mittel- und langfristige Verfügbarkeit aller für die Funktionsfähigkeit der Net- und Informationssysteme erforderlichen personellen, finanziellen sowie technisches Ressourcen werden sichergestellt

- [ ] **Informationssicherheitsmanagementsystemprüfung**

  Periodische Überprüfung des Informationssicherheitsmanagementsystems festlegen und durchführen

- [ ] **Personalwesen**

  Sicherheitsrelevante Aspekte, wie Fort- und Weiterbildungen in sicherheitsrelevanten Themengebieten sowie Sensibilisierung in Sicherheitsfragen für alle Mitarbeiter, aber auch die Sicherstellung der Vertrauenswürdigkeit der Mitarbeiter laufend berücksichtigen und umsetzten

2. Umgang mit Dienstleistern, Lieferanten und Dritten

- [ ] **Beziehungen mit Dienstleistern, Lieferanten und Dritten**

  Anforderungen an Dienstleister, Lieferanten und Dritte für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme festzulegen und periodisch überprüfen

- [ ] **Leistungsvereinbarungen mit Dienstleistern und Lieferanten**

  Leistungsvereinbarungen mit Dienstleistern und Lieferanten periodisch überprüfen und überwachen

3. Sicherheitsarchitektur

- [ ] **Systemkonfiguration**

  Netz- und Informationssysteme sicher konfigurieren, die Konfiguration strukturieren, dokumentieren und aktuell halten

- [ ] **Vermögenswerte**

  Vermögenswerte, die im Zusammenhang mit Netz- und Informationssystemen stehen, strukturieren, analysieren und dokumentieren

- [ ] **Netzwerksegmentierung**

  Eine Segmentierung der Netzwerke innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf vornehmen

- [ ] **Netzwerksicherheit**

  Die Sicherheit innerhalb der Netzwerksegmente und der Schnittstellen zwischen den Netzwerksegmenten ist zu gewährleisten

- [ ] **Kryptographie**

  Vertraulichkeit, Authentizität und Integrität von Informationen durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherstellen

4. Systemadministration

- [ ] **Administrative Zugangsrechte**

  Administrative Zugangsrechte eingeschränkt nach dem Minimalrechtsprinzip zuweisen. Diese Zuweisungen periodisch überprüfen und gegebenenfalls anpassen

- [ ] **Systeme und Anwendungen zur Systemadministration**

  Systeme und Anwendungen zur Systemadministration ausschließlich für Tätigkeiten zum Zweck der Systemadministration verwenden

5. Identitäts- und Zugriffsmanagement

- [ ] **Identifikation und Authentifikation**

  Verfahren umsetzen und Technologien einsetzen, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten

- [ ] **Autorisierung**

  Verfahren umsetzen und Technologien einsetzen, die unautorisierte Zugriffe auf Netz- und Informationssysteme unterbinden

6. Systemwartung und Betrieb

- [ ] **Systemwartung und Betrieb**

  Abläufe und Vorgänge zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen einführen und periodisch überprüfen

- [ ] **Fernzugriff**

  Fernzugriff eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten

7. Physische Sicherheit

- [ ] **Physische Sicherheit**

  Physischen Schutz der Netz- und Informationssysteme, insbesondere den physischen Schutz vor unbefugtem Zutritt und Zugang, gewährleisten

8. Erkennung von Vorfällen

- [ ] **Erkennung**

  Mechanismen zur Erkennung und Bewertung von Vorfällen sind umzusetzen

- [ ] **Protokollierung und Monitoring**

  Mechanismen zu Protokollierung und Monitoring, insbesondere von für die Erbringung des wesentlichen Dienstes essentiellen Tätigkeiten und Vorgängen, umsetzen

- [ ] **Korrelation und Analyse**

  Mechanismen zur Erkennung und adäquaten Bewertung von Vorfällen durch die Korrelation und Analyse der ermittelten Protokolldaten umzusetzen

9. Bewältigung von Vorfällen

- [ ] **Vorfallsreaktion**

  Prozesse zur Reaktion auf Vorfälle sind zu erstellen, aufrechtzuerhalten und zu erproben

- [ ] **Vorfallsmeldung**

  Prozesse zur internen und externen Meldung von Vorfällen sind erstellen, aufrechterhalten und erproben

- [ ] **Vorfallsanalyse**

  Prozesse zur Analyse und Bewertung von Vorfällen und zur Sammlung relevanter Informationen erstellen, aufrechterhalten und erproben, um den kontinuierlichen Verbesserungsprozess zu fördern

10. Betriebskontinuität

- [ ] **Betriebskontinuitätsmanagement**

  Die Wiederherstellung der Erbringung des wesentlichen Dienstes auf einem zuvor festgelegten Qualitätsniveau nach einem Sicherheitsvorfall gewährleisten

- [ ] **Notfallmanagement**

  Notfallpläne erstellen, anwenden, regelmäßig bewerten und erproben

11. Krisenmanagement

- [ ] **Krisenmanagement**

  Rahmenbedingungen und Prozessabläufe des Krisenmanagements für die Aufrechterhaltung des wesentlichen Dienstes vor und während eines Sicherheitsvorfalls definieren, umsetzen und erproben

Sicherer mit CoreTEC

CoreTEC schützt seit über 20 Jahren durch die Einrichtung von geeigneten organisatorischen und technischen Mitteln vor dem unberechtigten Zugriff auf die Informationen und Netzwerksysteme unserer Kunden. Unsere 100%ige Spezialisierung auf Informationssicherheit und IT Security garantiert ein hohes Maß an Qualität und Services, auf das wir sehr stolz sind. Unsere ISO 27001 Beratungsleistungen helfen dabei, höchste Standards für Informationssicherheit zu erreichen und aufrechtzuerhalten.

Wir verstehen die Bedeutung des NIS Gesetzes und stellen mit der Durchführung von umfassenden Audits und Reifegradanalysen sicher, dass Ihre Organisation vollständig mit den gesetzlichen Anforderungen konform ist.

CoreTEC GmbH

Ernst-Melchior-Gasse 24/DG
1020 Wien

T +43 1 503 72 73-0
M office@coretec.at
W www.coretec.at

Guarding your Security

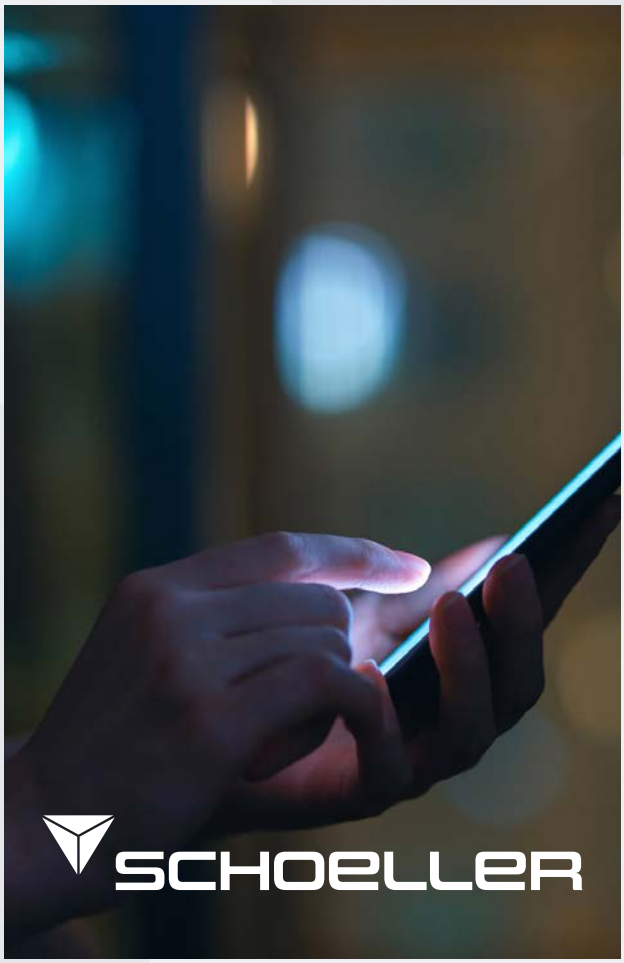
SCHOELLER network control bietet seit 25 Jahren professionelle Lösungen im Bereich IT und Telekommunikation an. Wir haben uns auf die Analyse, Optimierung und Sicherheit von IT-Ressourcen spezialisiert und sorgen so zuverlässig für die Sicherheit Ihres Netzwerks.

Seit 2014 sind wir Teil der TEC Gruppe, die mit ihrem Team aus IT-Spezialisten das gesamte Spektrum von IT-Dienstleistungen abdeckt. Das umfasst Planung, Entwicklung und Implementierung maßgeschneiderter Softwarelösungen, Installation und 24×7 Betrieb der IT-Infrastruktur, Performance-Analyse und Optimierung von Hard- und Software, IT Security-Dienstleistungen bis hin zur Bereitstellung von hochqualifiziertem IT-Personal.

schoeller GmbH

Ernst-Melchior-Gasse 24/DG
1020 Wien

T +43 1 689 29 29-0
M office@schoeller.at
W www.schoeller.at



ONTEC digitalisiert Geschäftsprozesse

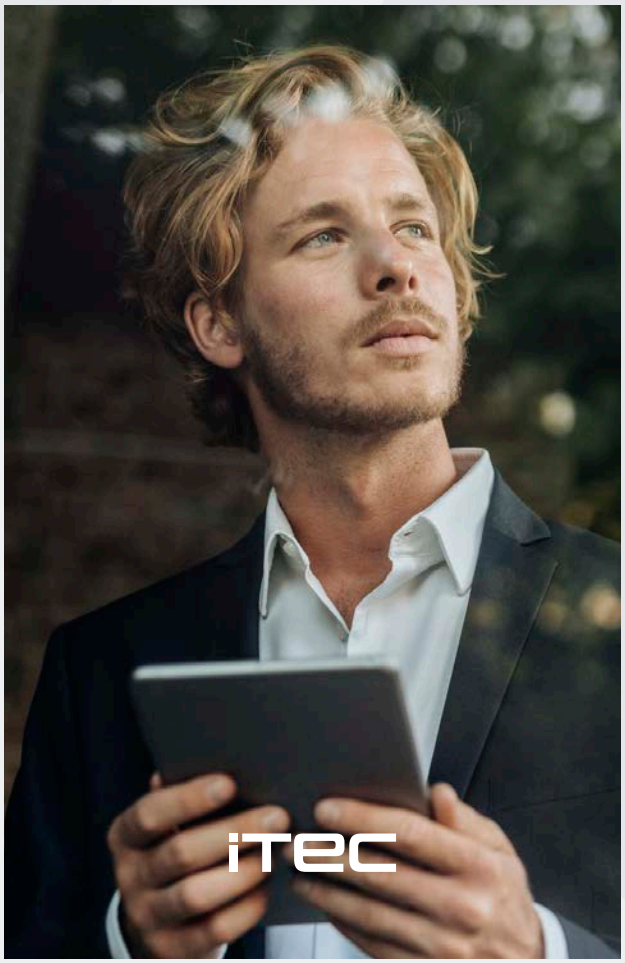
ONTEC ist ein ISO 27001-zertifizierter IT-Dienstleister und hat mehr als 20 Jahre Erfahrung mit der Digitalisierung businesskritischer Prozesse. Wir unterstützen erfolgreich große und mittelständische Unternehmen mit individuellen Softwaresystemen, Managed IT-Services und maßgeschneiderten KI-Lösungen. Dabei sind Securityaspekte ein integrativer Bestandteil. Da viele unserer Kunden kritische Infrastruktur betreiben, werden unsere Softwarelösungen und IT-Services regelmäßig und stets mit überzeugenden Ergebnissen auditiert.

Organisatorisch vertrauen unsere rund 100 Mitarbeitenden seit mehreren Jahren auf das Konzept Holacracy.

ONTEC AG

Ernst-Melchior-Gasse 24/DG
1020 Wien

T +43 1 20 55 20-0
M office@ontec.at
W www.ontec.at



Rekrutierung und Bereitstellung von IT-Fachkräften

Wir sind Experten für die Rekrutierung und Bereitstellung hochqualifizierter IT-Arbeitskräfte und einer der führenden IT-Personalberater auf dem österreichischen Markt. Viele Unternehmen aus hochsensiblen Bereichen wie Telekommunikation, Finance oder Verkehr vertrauen seit Jahren auf unser großes IT-Expertenteam und unser branchenspezifisches Know-How.

Dank unserer langjährigen Tätigkeit als IT-Personalberater haben wir ein umfangreiches Netzwerk und umfassende Kenntnisse der relevanten Märkte aufgebaut. Daher profitieren unsere Kunden von unserer Effizienz in Auswahl, Prozessabwicklung und Bereitstellung.

iTEC

Schlachthausgasse 10
1030 Wien

T +43 1 786 49 27-0
M itec@itec.at
W www.itec.at

TEC GRUPPE

Die TEC Gruppe ist ein Unternehmens-Verbund mit dem Schwerpunkt auf digitaler Transformation, Informationssicherheit & Cyber Security und IT-Personaldienstleitungen.

Sie ist seit über 25 Jahren zentrale Anlaufstelle für Software Development, Managed IT Services, Cyber Security und Informationssicherheit, KI und IT-Personaldienstleistungen.

Unsere 4 Unternehmen arbeiten nahtlos zusammen, um das bestmögliche Ergebnis für unsere Kunden zu erzielen.

TEC Gruppe

Ernst-Melchior-Gasse 24/DG
1020 Wien

T +43 1 20 55 20-0
M office@tec-gruppe.com
W www.tec-gruppe.com

CHECK POINT

CYBERARK

ENTRUST

POINTSHARP
security made easy

SentinelOne

VECTRA