SCHILLER GRUPPE CYBERSICHERHEITSPOLITIK

Engagement für Cybersicherheit

INFORMATIONSSICHERHEIT

SCHILLER ist der Cybersicherheit verpflichtet:

- Wir sind bestrebt, die ISO-Norm 27001 und andere geltende Anforderungen in Bezug auf die Informationssicherheit einzuhalten, um die Cybersicherheitsrisiken in allen unseren Geschäftsbereichen wirksam zu verwalten und zu mindern.
- Wir verpflichten uns, unsere Compliance-Verpflichtungen zu erfüllen.
- Unsere Massnahmen zielen darauf ab, den Schutz von personenbezogenen Daten und ePHI in Übereinstimmung mit den geltenden Datenschutzgesetzen zu gewährleisten.
- Wir sorgen dafür, dass die Cybersicherheit nahtlos in unsere Geschäftsprozesse integriert wird, und halten unsere Verpflichtung zu Cybersicherheit und Qualitätsmanagement aufrecht.
- Wir setzen uns Ziele, die mit der strategischen Ausrichtung und dem Kontext unserer Organisation vereinbar sind.
- Durch den Schutz von Geschäftsgeheimnissen und geschützten Informationen vor unbefugtem Zugriff und Offenlegung untermauern wir unser Engagement für die Bereitstellung von Medizinprodukten und Dienstleistungen höchster Qualität.

STÄNDIGE VERBESSERUNG

SCHILLER ist bestrebt, die Informationssicherheit kontinuierlich zu verbessern

- Zu unserem Engagement gehören regelmässige Risikobewertungen und die Einführung geeigneter technischer und organisatorischer Kontrollen zur Bewältigung von Cybersicherheitsrisiken.
- Wir führen Audits und Überprüfungen durch, um die kontinuierliche Eignung, Angemessenheit und Wirksamkeit der Cybersicherheitsmassnahmen zu bewerten.
- Wir ermitteln Verbesserungsmöglichkeiten und sorgen dafür, dass die erforderlichen Ressourcen zur Verfügung stehen.
- Wir integrieren robuste Cybersicherheitspraktiken in unser Qualitätsmanagementsystem, um die höchsten Standards für unsere Produkte und Dienstleistungen zu gewährleisten.

BEWUSSTSEIN DER MITARBEITENDEN

SCHILLER informiert und schult seine Mitarbeitenden in Sachen Cybersicherheit

- Wir verpflichten uns, die Integrität, die Vertraulichkeit und die Verfügbarkeit von Informationen zu schützen. Dazu gehören Produktionsprozesse, ICT-Infrastruktur, personenbezogene Daten, elektronische geschützte Gesundheitsinformationen (ePHI) und Geschäftsgeheimnisse.
- Wir kommunizieren diese Politik an unsere Mitarbeitenden.
- Wir stellen sicher, dass unsere Mitarbeitenden über die Risiken der Cybersicherheit und die Vorteile eines effektiven Managements und der Beherrschung dieser Risiken in unseren Betrieben informiert sind.
- Unsere Mitarbeitenden sind sich der Bedeutung der Cybersicherheit bewusst und halten sich an die geltenden Vorschriften.