

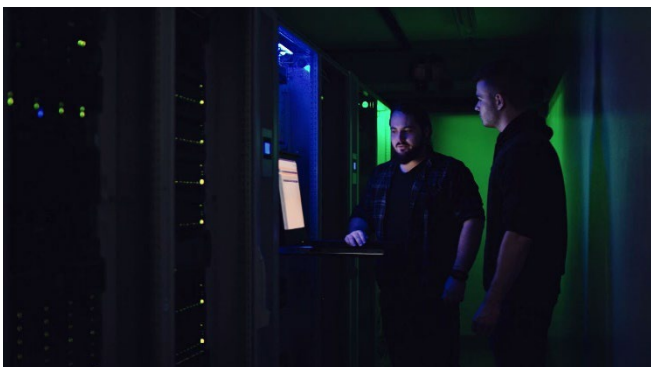
Informationssicherheitsleitlinie

Die Rosenberger-Gruppe mit Hauptsitz in Fridolfing ist ein mittelständisches Industrieunternehmen in Familienbesitz und wurde 1958 gegründet. Heute zählt dieses zu den weltweit führenden Herstellern von standardisierten und kundenspezifischen Verbindungslösungen in Hochfrequenz-, Hochvolt- und Faseroptik-Technologie.



Das Produktportfolio umfasst HF-Koaxialsteckverbinder, -Komponenten und -Zubehör, HF-Messtechnik-Produkte sowie konfektionierte Kabel. Namhafte High-Tech-Unternehmen in Mobil- und Telekommunikation, industrieller Messtechnik, der Automobil-Elektronik, Datentechnik, Medizin- und Industrieelektronik oder Luft- und Raumfahrt setzen auf die Präzision und Qualität unserer Produkte. Im Bereich Industries konzipiert Rosenberger innovative Systemlösungen für M2M-Anwendungen, z. B. Telematik-Projekte. Der Bereich Präzisionsfertigung produziert kundenspezifische Komponenten für die Antriebs-, Nutzfahrzeug- und Maschinenbauindustrie.

1. Geltungsbereich und Dokumenten-Management



Den Informationssystemen der Rosenberger-Gruppe und deren Sicherheit und Verfügbarkeit kommt im Unternehmen eine Schlüsselrolle zu. Sowohl die Vorstandsführung der Rosenberger-Gruppe als auch alle mitarbeitenden Personen müssen dafür Sorge tragen, dass die

von Informationssystemen abhängigen Geschäftsprozesse aufrechterhalten werden.

Die vorliegende Informationssicherheitsleitlinie adressiert dieses Erfordernis im Hinblick auf die Sicherheit der Informationsverarbeitung innerhalb der Rosenberger-Gruppe.

Die Informationssicherheitsstrategie der Rosenberger-Gruppe bildet den Rahmen, nach dem die Informationssicherheitsrichtlinien erstellt werden. Die Informationssicherheitsstrategie bezieht sich auf Informationen jeglicher Form und hat insbesondere das Ziel, die folgenden Informationseigenschaften zu schützen:

- Vertraulichkeit
- Verfügbarkeit
- Integrität

Die Vorstandsführung, die Geschäftsführung und das Rosenberger Management Board unterstreichen mit dieser Informationssicherheitsstrategie den hohen Stellenwert und die kritische Bedeutung der Informationssicherheit und des Datenschutzes innerhalb der Gruppe.

2. Anforderungen, Risiken und Ziele

Das Vertrauen unserer Kunden und letztlich unser Geschäftserfolg beruhen darauf, dass wir insbesondere

- die gesetzlichen Vorgaben und hier insbesondere die Datenschutzgesetze einhalten (Compliance),
- unsere Betriebsgeheimnisse schützen,
- die Vertraulichkeit der Daten unserer Kunden wahren,
- die relevanten rechtlichen, regulatorischen und vertraglichen Anforderungen erfüllen,
- Projekte und Dienstleistungen in der geplanten bzw. zugesicherten Zeit abwickeln.

Dabei werden folgende Prinzipien befolgt:

- Der Ansatz der Informationssicherheit ist geschäftsorientiert, risikoorientiert und erfolgt in Übereinstimmung mit bewährten Vorgehensweisen.
- Alle Formen von Informationsressourcen, digital oder nicht, sind ausreichend und über ihren gesamten Lebenszyklus zu schützen.
- Alle mitarbeitenden Personen sind dafür verantwortlich, die Informationssicherheitsstrategie und die betreffenden Dokumente, Richtlinien und Arbeitsanweisungen zu verinnerlichen und in Übereinstimmung mit den hierin enthaltenen Vorgaben zu handeln.
- Die Verarbeitung von personenbezogenen Daten erfolgt unter Beachtung der datenschutzrechtlichen Grundsätze.

- Die kontinuierliche Verbesserung der Informationssicherheit und der zugehörigen Schutzmaßnahmen und -kontrollen ist ein fortlaufender Prozess und ist Ziel der Organisation.



Vor diesem Hintergrund ist der Geschäftserfolg unserer Gruppe davon abhängig, dass wir bestehende Risiken für die genannten Ziele erkennen, durch geeignete Maßnahmen vermeiden bzw. mindern und verbleibende Risiken geeignet behandeln. Zu den Risiken zählen die unvollständige bzw. nicht korrekte Einhaltung von gesetzlichen Vorgaben, die unbefugte und ggf. unbemerkte Weitergabe von Betriebsgeheimnissen, die Verletzung von Vorgaben unserer Kunden aufgrund von Systemausfall, Datenverlust oder unbefugter Preisgabe von Informationen.

3. Bedeutung der Sicherheit

Vor dem Hintergrund der externen und internen Anforderungen, vor allem aber den Sicherheitsanforderungen unserer Kunden muss Informationssicherheit ein integraler Bestandteil unserer gesamtheitlichen Unternehmenskultur sein. Alle mitarbeitenden Personen müssen sich der Notwendigkeit der Informationssicherheit bewusst sein und die grundsätzlichen Auswirkungen von Risiken auf den Geschäftserfolg der Gruppe kennen.

4. Grundsätzliche Regelungen



Für die Umsetzung der Sicherheitsziele und die Pflege des Informationssicherheits-Managementsystems (ISMS) haben der Vorstand und die Geschäftsleitung der Rosenberger-Gruppe einen Informationssicherheitsbeauftragten (CISO) ernannt und ihm die Aufgaben mit allen notwendigen Befugnissen übertragen, einheitliche Vorgaben für den Sicherheitsprozess zu schaffen, dafür zu sorgen, dass alle mitarbeitenden Personen ausreichend sensibilisiert sind, und die Einhaltung aller Sicherheitsrichtlinien entsprechend zu überprüfen bzw. überprüfen zu lassen.

Die Informationssicherheit der Rosenberger-Gruppe orientiert sich an TISAX (Trusted Information Security Assessment Exchange), der sich auf wesentliche Aspekte der internationalen Norm ISO/IEC 27001 stützt.

Diese umfassen die Durchführung von regelmäßigen internen und externen Audits, eine geeignete Dokumentenlenkung, die Managementbewertung und die Anwendung des Modells der kontinuierlichen Verbesserung (PDCA).

Jede mitarbeitende Person ist verpflichtet, die allgemeinen sowie die für den jeweiligen Arbeitsplatz geltenden Sicherheitsrichtlinien zu beachten und einzuhalten.

Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter

Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

5. Kontaktinformationen

Bei Fragen und Kommentaren bezüglich dieses Dokuments ist der Information Security Manager der Rosenberger-Gruppe zu kontaktieren:

InformationSecurity@rosenberger.com

Sofern personenbezogene Daten betroffen sind, ist zudem der betriebliche Datenschutzbeauftragte zu kontaktieren:

Datenschutz@rosenberger.com