ITERCON
GRUPO CYCLUS

ERKLÄRUNG ZUR INFORMATIONSSICHERHEIT

Contenido

Kontrolle der Fassungen

Datum	Ausgabe/Überarbeitung	Vorgenommene Änderungen
16/04/2024	1.00	Ursprüngliche Ausarbeitung

ZIEL

Unter Berücksichtigung des „ITERCON-Kontextes für das Managemensystem für Informationssicherheit (ISMS)“, der die internen und externen Aspekte des Unternehmens, die entsprechenden Interessengruppen, die Anforderungen an die Informationssicherheit sowie die Schnittstellen und Abhängigkeiten zwischen den vom Unternehmen durchgeführten Maßnahmen festlegt, umfasst der Geltungsbereich des ISMS die Informationssysteme, die die Vorgänge in den Bereichen Planung, Einkauf und Produktion unterstützen.

Mit der Einführung eines Informationssicherheits-Managementsystems (ISMS) wird die Arbeit, die von der gesamten Organisation in diesem Bereich geleistet wird, konkret sichtbar gemacht.

ANWENDBARKEIT

Um das von der Geschäftsführung angestrebte Ziel zu erreichen, ist Folgendes erforderlich:

- Einführung einer Methodik zur Einführung und Aufrechterhaltung eines ISMS gemäß der Norm UNE-EN ISO/IEC 27001:2022
- Erstellung der zu befolgenden Richtlinien und Vorschriften, um alle Informationssysteme ordnungsgemäß zu sichern.
- Die Mitteilung an alle Mitarbeiter, die eine aktive Rolle bei der Nutzung eines der Informationssysteme spielen, über die ausgearbeiteten Richtlinien, um sie von den geplanten durchzuführenden Maßnahmen und die Folgen einer Nichteinhaltung in Kenntnis zu setzen.

Die Vorschriften müssen den betreffenden Mitarbeitern jederzeit zur Einsichtnahme zur Verfügung stehen und bei Zweifeln bezüglich der Anwendbarkeit können sie sich an den für die Informationssicherheit verantwortlichen Mitarbeiter wenden.

ROLLEN UND VERANTWORTLICHKEITEN

DieGeschäftsleitung	• Genehmigung der Richtlinie und ihrer späteren Änderungen • Gewährleistung der Einhaltung der Richtlinie und ihrer späteren Änderungen
Beauftragter für Informationssicherheit	• Erstellung der Richtlinie • Überwachung der ordnungsgemäßen Einhaltung der Richtlinie • Vorschlagen spezieller Strategien und Lösungen für die Einführung der erforderlichen Kontrollen zur Umsetzung der im ISMS festgelegten Sicherheitsrichtlinien.
Systemverantwortlicher	• Umsetzung von Sicherheitsmaßnahmen, um die Anwendung der vorliegenden Richtlinie zu gewährleisten

Benutzer	• Anwendung der nachfolgend aufgeführten Sicherheitsmaßnahmen, die in seinen Zuständigkeitsbereich fallen, um den Schutz der Informationsressourcen zu gewährleisten

EINHALTUNG

Die Einhaltung der Richtlinie ist verpflichtend und gilt für alle diejenigen, die mit ITERCON in Verbindung stehen oder bei ITERCON angestellt sind oder für das Unternehmen Dienstleistungen erbringen.

Die eingerichteten Kontrollen werden regelmäßig überprüft, um die ordnungsgemäße Nutzung der Systeme des Unternehmens zu gewährleisten.

Mitarbeiter des Unternehmens, die gegen die Richtlinie verstoßen, werden als Zuwiderhandelnde angesehen. Gegen sie werden die im Abschnitt „Nichteinhaltung der Richtlinie" vorgesehenen Strafen verhängt, wobei die Schwere des Verstoßes im Rahmen des jeweils geltenden Sanktionssystems bewertet wird.

ERKLÄRUNG ZUR INFORMATIONSSICHERHEIT

Die Geschäftsleitung von ITERCON verpflichtet sich, die erforderlichen Mittel bereitzustellen, um das Mangementsystem zur Informationssicherheit (ISMS) des Unternehmens einzurichten, umzusetzen, aufrechtzuerhalten und zu verbessern, und durch die Einrichtung des Ausschusses für Informationssicherheit Führungsstärke und Engagement in diesem Bereich zu zeigen.

Informationen gehören zu den wichtigsten Aktiva sowohl für das Unternehmen als auch für den Kunden. Deshalb müssen ihre Vertraulichkeit, Authentizität und Integrität gewährleistet sein, sei es bei der Verarbeitung, Speicherung oder Übertragung.

ITERCON bekräftigt ausdrücklich seine Verpflichtung zur Umsetzung der Richtlinie für Informationssicherheit anhand folgenden Leitlinien:

- Die Informationen, deren Eigentümer und/oder Verwahrer ITERCON ist, dürfen nur für ordnungsgemäß befugte Personen zugänglich sein, unabhängig davon, ob sie dem Unternehmen angehören oder nicht.
- ITERCON muss die für das Unternehmen geltenden gesetzlichen, behördlichen und satzungsmäßigen Anforderungen sowie die vertraglichen Verpflichtungen erfüllen.
- ITERCON stellt die erforderlichen Mittel bereit, um das Managementsystem für Informationssicherheit zu veröffentlichen und seine Angemessenheit und Aktualität zu gewährleisten. Dadurch wird die ständige Verbesserung der Vorgänge und Dienstleistungen im Bereich der Informationssicherheit abgesichert.
- ITERCON führt einen Vorgang zum Schutz von Informationen durch und gewährleistet somit ihre Vertraulichkeit, Integrität und Verfügbarkeit.

- ITERCON wird die erforderlichen Kontrollmaßnahmen zur Risikominimierung gemäß der durchgeführten Risikoanalyse und den vom Unternehmen akzeptierten Risikostufen umsetzen.
- Alle Mitarbeiter im Bereich des ISMS von ITERCON müssen eine angemessene Schulung und Sensibilisierung im Bereich der Informationssicherheit absolvieren.
- Jeder Vorfall, der die Vertraulichkeit, Integrität und/oder Verfügbarkeit von Informationen gefährden könnte oder gefährdet hat, muss erfasst und untersucht werden, um entsprechende Korrektur- und/oder Präventivmaßnahmen zu ergreifen.
- Alle Mitarbeiter werden über die Informationssicherheit informiert und sind für sie verantwortlich, soweit es für die Ausübung ihrer Tätigkeit von Bedeutung ist.

ZIELE DER INFORMATIONSSICHERHEIT

- Abstimmung der Geschäftsstrategie auf die Informationssicherheit. ITERCON verpflichtet sich, die erforderlichen Sicherheitsanforderungen zu erfüllen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen sowie der Informationsressourcen, von denen sie verarbeitet, gespeichert oder verbreitet werden, zu gewährleisten.
- Einhaltung der geltenden Sicherheits- und Datenschutzgesetze und Einführung der für ihre Einhaltung erforderlichen Kontrollmaßnahmen.
- Gewährleistung der Aufrechterhaltung von Integrität und Qualität der Informationen sowie der Vorgänge zu ihrer Verarbeitung (Zugang, Speicherung, Übertragung und Löschung)
- Gewährleistung einer ununterbrochenen Erbringung der Dienstleistungen und Sicherstellung von Abläufen, die die Beständigkeit wichtiger Maßnahmen des Unternehmens gewährleisten. Dabei werden die Wiederherstellungszeiten der zugrunde liegenden Informationssysteme innerhalb akzeptabler Fristen gewährleistet.
- Verbreitung des festgelegten, der Informationssicherheit zugrunde liegenden Regelwerks zur Stärkung des Bewusstsein für Informationssicherheit unter den Mitarbeitern.
- Effektives Management von Sicherheitsvorfällen mit dem Ziel, ihre Folgen zu verringern.
- Reifemessung des eigenen Mangements zur Informationssicherheit
- Stetige Verbesserung des ISMS

ORGANISATION UND ZUSTÄNDIGKEITEN

- Für die Genehmigung dieser Richtlinie ist die Geschäftsleitung von ITERCON verantwortlich.
- Für die Überprüfung der Richtlinie ist der Ausschuss für Informationssicherheit zuständig.
- Der Beauftragte für Informationssicherheit ist für die Aufrechterhaltung der Richtlinie verantwortlich.

GÜLTIGKEIT UND AKTUALISIERUNG

Die vorliegende Richtlinie tritt mit ihrer Veröffentlichung in Kraft und wird mindestens einmal jährlich überprüft.

Zweck der regelmäßigen Überprüfungen ist es, die Richtlinie an Veränderungen im organisatorischen Umfeld anzupassen. Es werden dabei externe und interne Aspekte berücksichtigt und aufgetretene Vorfälle im Bereich der Informationssicherheit sowie im ISMS festgestellte fehlende Übereinstimmungen werden untersucht. All dies erfolgt unter Berücksichtigung der Ergebnisse aus den einzelnen Vorgängen der Risikobewertung.

VERSTÖSSE GEGEN DIE RICHTLINIE

Verstöße gegen die Richtlinie zur Informationssicherheit von ITERCON können erhebliche finanzielle Verluste und Verstöße gegen das Gesetz zur Folge haben sowie das Ansehen und den täglichen Geschäftsbetrieb des Unternehmens beeinträchtigen, da durch sie ITERCON verschiedenen geschäftlichen Risiken ausgesetzt wird.

Jeder Verstoß gegen diese Richtlinie und die übrigen Durchführungsvorschriften und -verfahren hat die Verhängung von Strafen zur Folge, deren Umfang sich nach dem Ausmaß und den Besonderheiten des Verstoßes richtet und mit dem geltenden Arbeitsrecht und dem anwendbaren Tarifvertrag übereinstimmt.