RICHTLINIE
SICHERHEITSPOLITIK

DOKUMENTENLENKUNG

Dokumenteninformation

Klassifikation:	Öffentlich
Verteilerkreis:	
Versionsnummer:	1.0
Dokumententitel:	Sicherheitspolitik
Dokumentenverantwortlich:	Matthias Klinski
Freigabe:	Vorstand
Revisionsintervall:	Jährlich

Freigabe

Durch die Freigabe und Inkraftsetzung der „Sicherheitspolitik“ durch den Vorstand sind alle Mitarbeiterinnen und Mitarbeiter verpflichtet, sich an die Vorgaben des Informationssicherheitsmanagementsystem (ISMS) zu halten und die Regelungen umzusetzen.

Karl Weidlinger

Adolf Scheuchenpflug

Peter Gal

Walter Pertl

INHALTSVERZEICHNIS

1 EINLEITUNG

Als eines der bedeutendsten Unternehmen der österreichischen Bauwirtschaft ist SWIETELSKY seinen Mitarbeitern, Kunden und Vertragspartnern verpflichtet, höchste Standards in allen Unternehmensbereichen umzusetzen.

Aufgrund der an das Unternehmen gestellten gesetzlichen, aber auch wirtschaftlichen Anforderungen wird deshalb ein besonderes Augenmerk auf die Informationssicherheit im Unternehmen gelegt.

Als Informationssicherheit definiert SWIETELSKY den Schutz von physischen und elektronischen Informationen, sowie der zur Informationsverarbeitung notwendigen Systeme im Hinblick auf deren Vertraulichkeit, Integrität und Verfügbarkeit.

2 ANWENDUNGSBEREICH

Der Anwendungsbereich dieser Sicherheitspolitik umfasst den Konzern Swietelsky und dessen Konzerntöchter mit allen ihren Mitarbeitern, Standorten und Leistungen.

3 GRUNDSÄTZE

3.1 Management Auftrag

Der Vorstand der SWIETELSKY verabschiedet hiermit die Informationssicherheitspolitik als Bestandteil ihrer Unternehmensstrategie.

Der Vorstand unterstützt die Ziele und Prinzipien der Informationssicherheit im Einklang mit der Geschäftsstrategie und den Geschäftszielen.

Durch die Etablierung eines Informations-Sicherheits-Management-Systems (ISMS) und der Bereitstellung der notwenigen Ressourcen schafft der Vorstand die Möglichkeiten die Ziele des ISMS erreichen zu können. Als oberste Instanz des ISMS trägt der Vorstand aktiv zum Erfolg des ISMS bei.

3.2 Stellenwert der Informationssicherheit

SWIETELSKY ist in ihrer Geschäftstätigkeit wesentlich von der Verfügbarkeit von Informationen, sowie zunehmend vom ordnungsgemäßen Funktionieren ihrer Informationssysteme abhängig. Informationsverarbeitung und Digitalisierung gewinnt in der Bauwirtschaft zunehmend an Bedeutung. Vernetzungen innerhalb des Unternehmen aber auch mit Kunden, Lieferanten und Arbeitsgemeinschaften unterstützen maßgeblich die Leistungserbringung. Ausfälle von Kernsystemen können bereits nach kurzer Zeit betriebswirtschaftliche Schäden sowie Schäden an der Reputation von SWIETELSKY verursachen.

Informationssicherheit schafft das notwendige Vertrauen, sowohl intern als auch bei Kunden und Partnern, um die Digitalisierung weiter voranzutreiben und dadurch entstehende Risiken zu adressieren. Deshalb wird das Thema in Bezug auf rechtliche, technologische und organisatorische Belange aktiv vom Vorstand bzw. den hierzu vom Vorstand Beauftragten betrieben.

4 KONTEXT DER ORGANISATION

Im Jahr 1936 gründet Dipl. Ing. Hellmuth Swietelsky das Bauunternehmen. Heute gehört die SWIETELSKY AG mit durchschnittlich mehr als 10.000 Mitarbeiterinnen und Mitarbeitern zu den bedeutendsten Unternehmen der österreichischen Bauindustrie.

Mit Niederlassungen in 4 Kernländern (Österreich, Deutschland, Tschechien, Ungarn) und 15 weiteren Ländern befindet sich das Unternehmen vollständig in privatem Besitz. Die Aktivitäten von SWIETELSKY erstrecken sich auf alle Sparten des Bauwesens. Der Konzern bietet dabei mit höchster Qualität, Flexibilität und Termintreue Projekte aller Dimensionen an.

„Dezentrale Organisation in Profit-Zentren, delegierte Verantwortung, sowie Beteiligung am Erfolg bewirkt, dass unsere motivierten und kompetenten Mitarbeiter/-innen als „Unternehmer/-innen im Unternehmen" tätig sein können." - Philosophie von SWIETELSKY

4.1 Interne Zusammenhänge

SWIETELSKY ist ein dezentral organisiertes Unternehmen mit diversen eigenständigen Unternehmensbereichen, welche in Europa und Australien tätig sind. Common Services, wie Personal, Finanz oder IT, werden zentral gesteuert.

Zur Erfüllung von Kundenwünschen, Ausschreibungsanforderungen und zur Steuerung von Maßnahmen betreibt SWIETELSKY neben dem ISMS auch noch weitere Managementsysteme. Diese werden durch die jeweiligen Beauftragten unabhängig voneinander betrieben, wobei regelmäßige Abstimmungen dafür sorgen, dass die Managementsysteme im Einklang miteinander betrieben werden.

4.2 Externe Zusammenhänge

Die Aktivitäten von SWIETELSKY erstrecken sich auf alle Sparten des Bauwesens. Zur Erfüllung der Aufgaben ist eine enge Zusammenarbeit mit diversen Lieferanten, Auftraggebern, Subunternehmen und anderen Mitbewerben in Form von Arbeitsgemeinschaften nötig.

5 INTERESSIERTE PARTEIEN

Es gibt verschieden interessierte Parteien die Anforderungen an ein ISMS der SWIETELSKY stellen.

5.1 Vertragspartner (Kunden, Lieferanten, Arbeitsgemeinschaften)

Vertragspartner erwarten einen vertrauensvollen Umgang mit deren Daten aber vor allem einen reibungslosen Betriebsablauf und somit auch die Verfügbarkeit der Dienste.

5.2 Interne Parteien (Geschäftsbereiche, Mitarbeiter)

Interne Parteien erwarten funktionierende Services die jederzeit zur Verfügung stehen. Ausfallzeiten sollen so gering wie möglich sein und keinesfalls ungeplant passieren. Sicherheit soll im Hintergrund erfolgen und möglichst nicht die Arbeit beeinflussen oder erschweren. Vereinzelt werden auch hohe Anforderungen an die Vertraulichkeit gestellt.

5.3 Shareholder (Geschäftsführung, Eigentümer)

Die Shareholder erwarten eine Absicherung gegen Betriebswirtschaftliche-, Rechtliche- und Reputationsrisiken. Das ISMS soll Ressourcen effizient einsetzen und durch Zertifizierungen einen Wettbewerbsvorteil ermöglichen.

5.4 Öffentlichkeit Verwaltung (Behörden, Gesetzgeber)

Die öffentliche Verwaltung erwartet, dass alle Gesetze eingehalten werden. Alle Informationen die übertragen werden, müssen fristgerecht, korrekt und vollständig bei der öffentlichen Stelle ankommen.

6 ORGANISATION

Innerhalb des ISMS sind folgende maßgeblichen Rollen und Verantwortungen definiert:

7 ZIELE

Die Ziele des ISMS leiten sich von den Grundsätzen des Verhaltenskodex von SWIETELSKY ab.

Den hier beschriebenen strategischen Zielen des ISMS werden operative Ziele zugeteilt. Diese werden mittels Kennzahlen jährlich gemessen.

7.1 Wir schützen die Vermögenswerte des Unternehmens

7.1.1 Vermeidung ungeplanter Ausfallzeiten von zentralen IT-Services

Ausfälle von zentralen Services können sich innerhalb von kurzer Zeit auf den Geschäftsbetrieb auswirken und zu finanziellen Schäden führen.

7.1.2 Vermeidung finanzieller Schäden durch Cyberkriminalität

Kriminelle Handlungen über elektronische Medien können zu schweren finanziellen Schäden führen.

7.2 Wir gehen mit Geschäftsunterlagen und Informationen vertraulich um

7.2.1 Schutz der Vertraulichkeit von Informationen

Die ungewollte Weitergabe oder Veröffentlichung von Informationen kann kritische Auswirkung auf die Reputation von SWIETELSKY haben, sowie rechtliche und vertragliche Konsequenzen nach sich ziehen.

7.3 Wir halten IT-Sicherheits- und Datenschutzstandards ein

7.3.1 Etablierung eines IT-Sicherheitsniveaus am Stand der Technik

Durch Etablierung eines ISMS und der Ausrichtung von Sicherheitsmaßnahmen nach ISO/IEC 27001 sowie einer externen Zertifizierung weisen wir, gegenüber Dritten, ein Sicherheitsniveau am Stand der Technik nach.

7.4 Wir entwickeln uns weiter

7.4.1 Awareness-Bildung des Personals

Kontinuierliche Schulungen und Trainings sind die Basis zur Weiterentwicklung der Awareness von Swietelsky Mitarbeiterinnen und Mitarbeitern.

7.4.2 Ständige Verbesserung des ISMS und der Sicherheitsmaßnahmen

Die Etablierung eines kontinuierlichen Verbesserungsprozesses im Rahmen des ISMS sorgt für eine ständige Evaluierung und Weiterentwicklung bestehender Maßnahmen, sowie für die Identifikation neuer, risikobasierten Maßnahmen.

8 UMSETZUNG

Zur Umsetzung dieser Sicherheitspolitik werden innerhalb des ISMS folgende Kernkomponenten und Prozesse etabliert:

9 GELTUNGSBEREICH ISO/IEC 27001

Obwohl sich der Geltungsbereich dieser Sicherheitspolitik und des ISMS auf das gesamte Unternehmen erstreckt, ist die externe Zertifizierung nach ISO/IEC 27001 auf folgenden Geltungsbereich beschränkt:

Im Geltungsbereich des ISMS befinden sich die konzernweite Bereitstellung und der Betrieb der zentralen IT-Services und der dafür notwendigen Infrastruktur in Österreich.

The ISMS scope includes company-wide provision and operation of central IT-services and therefor needed infrastructure in Austria.

Dienstleistungen

Die zentralen IT-Services sowie der Betrieb der IT-Infrastruktur sind die relevanten Dienstleistungen für den Geltungsbereich.

Prozesse

Als primäres Betrachtungsobjekt gilt der Prozess IT-Betrieb federführend für die Aufgaben des Geltungsbereich.

Abteilung / Bereiche

Zuständig für den Geltungsbereich ist der Bereich IT & Prozesse mit den Abteilungen IT Benutzerservice, IT-Infrastruktur, ERP & Prozesse sowie Cyber Security.

Standorte

Im Geltungsbereich sind die zentralen IT-Büros, Server- und Backupräume sowie IT-Backupstandorte in Österreich.

Schnittstellen

Im Rahmen des Geltungsbereich erfolgt eine enge Zusammenarbeit mit diversen Schnittstellen, wie Personal, Qualitätsmanagement, Digitalisierung, Gebäudemanagement, Recht sowie Dienstleistern und Outsourcing-Partnern.

IT-Systeme & Applikationen

Im Geltungsbereich befinden sich unteranderem mobile und stationäre IT-Geräte, Speicherlösungen und zugehörige Backups, Zutrittskontrollen und Benutzerverwaltungen sowie Bau- und Personalsoftware.

Legale Einheiten

Alle für den Geltungsbereich relevanten Prozesse, Personen, Abteilungen und Standorte sind Teil von SWIETELSKY.

Informationen

Im Geltungsbereich sind alle für die Bereitstellung der Services relevanten Informationen.

ANHANG
VERSIONSVERLAUF

Datum	Autor	Version	Beschreibung
13.07.2020	Matthias Klinski	1.0	Initiale Erstellung