INFORMATIONENSICHERHEITSPOLITIK

Telmekom S.r.l. ist ein Unternehmen, das im Bereich der Telekommunikationsdienstleistungen und der Bereitstellung von IKT-Lösungen tätig ist.
Mit dem ständig zunehmenden Einsatz neuer Technologien **betrachtet Telmekom S.r.l.** es als Priorität, Garantien für die Qualität der angebotenen Dienstleistungen und Produkte, die Sicherheit der Informationen und deren korrekte Behandlung zu geben. Qualität und Sicherheit gelten als unverzichtbare Faktoren und grundlegende Anforderungen von strategischem Wert, die leicht in einen Wettbewerbsvorteil umgewandelt werden können.

Aus diesem Grund hat die Geschäftsführung der **Telmekom S.r.l.**im Einklang mit der Mission des Unternehmens verlangt, dass das Management aller Prozesse in Übereinstimmung mit den Anforderungen der Norm ISO/IEC 27001 und den regulatorischen Anforderungen des Gesetzesdekrets 196/03 und der EU-Verordnung 679/2016 eingerichtet wird, um nicht nur das Geschäft und die Vermögenswerte des Unternehmens, sondern auch die Rechte und Freiheiten des Einzelnen zu schützen.

Die Geschäftsführung von **Telmekom S.r.l.** hat diese Richtlinie zur Informationssicherheit und zum Datenschutzmanagement auf allen Ebenen seiner Organisation eingeführt und verbreitet.

Der Zweck dieser Richtlinie besteht darin, sicherzustellen, dass Sie vor allen internen oder externen Bedrohungen geschützt und geschützt sind.
Vorsätzlich oder versehentlich:

- über die Informationen, die für die Geschäftstätigkeit **von Telmekom S.r.l. erforderlich sind.**(von denen personenbezogene Daten nur eine der zu schützenden Informationsklassen sind),
- der Informationen seiner Kunden, die im Lebenszyklus der ihnen zur Verfügung gestellten Produkte und Dienstleistungen verwaltet werden.

Diese Richtlinie gilt unterschiedslos für alle Prozesse, Funktionen und Ebenen der Organisation **von Telmekom S.r.l**.
Die Umsetzung dieser Richtlinie ist für alle Mitarbeiter obligatorisch und muss sie jeder externen Partei mitteilen, die in irgendeiner Funktion an der Verarbeitung von Informationen beteiligt sein kann, die in den Geltungsbereich des Informationssicherheitsmanagementsystems fallen.

Die zu schützenden Informationsgüter bestehen aus allen Informationen, die über die bereitgestellten Dienste verwaltet werden und sich in allen Büros des Unternehmens befinden.
Sie müssen sicherstellen:

- Die Vertraulichkeit von Informationen: Das heißt, die Informationen dürfen nur von denjenigen zugänglich sein, die dazu berechtigt sind.
- die Integrität von Informationen, d.h. die Richtigkeit und Vollständigkeit von Informationen zu schützen und
- Methoden für ihre Ausarbeitung.
- Die Verfügbarkeit von Informationen, d. h. dass autorisierte Benutzer tatsächlich auf die Informationen und die darin enthaltenen Assets zugreifen können.

Das Fehlen eines angemessenen Sicherheitsniveaus kann zu einer Schädigung des Unternehmensimages, zu mangelnder Kundenzufriedenheit, zum Risiko von Strafen im Zusammenhang mit der Verletzung der geltenden Gesetze und Vorschriften sowie zu wirtschaftlichen und finanziellen Schäden führen.

Die Einhaltung und Umsetzung der Politik liegt in der Verantwortung des gesamten Personals und aller externen Parteien,
die Beziehungen pflegen und mit **Telmekom S.r.l. zusammenarbeiten.** und die in irgendeiner Weise an der Verarbeitung von Daten und Informationen beteiligt sind, die in den Geltungsbereich des Informationssicherheits- und Datenschutzmanagementsystems fallen. Jeder ist auch dafür verantwortlich, alle Anomalien und Verstöße zu melden, von denen er Kenntnis erlangt.
Jeder, Mitarbeiter, Berater und/oder externe Mitarbeiter des Unternehmens, der vorsätzlich oder fahrlässig die festgelegten Sicherheitsregeln missachtet und **Telmekom S.r.l. Schaden zufügt.**, kann in den geeigneten Foren und unter vollständiger Einhaltung der gesetzlichen und vertraglichen Beschränkungen verfolgt werden.

Die Geschäftsleitung wird die Wirksamkeit und Effizienz des Managementsystems für Informationssicherheit und Datenschutz regelmäßig überprüfen, um die Aktivierung eines Prozesses zu fördern und zu fördern.
Kontinuierliche Verbesserung, auch als Reaktion auf Veränderungen im internen und externen Umfeld.

Die Geschäftsleitung unterstützt aktiv Aktivitäten im Zusammenhang mit dem Management der Informationssicherheit und des Datenschutzes
durch eine klare Richtung, ein klares Bekenntnis, klare Aufträge und die Anerkennung der Verantwortung für Informationssicherheit und Datenschutz.

Das Engagement der Geschäftsleitung wird durch eine Struktur umgesetzt, deren Aufgaben sind:

- sicherzustellen, dass alle Ziele der Informationssicherheit und des Datenschutzes identifiziert werden,
- sowie die Einhaltung der Geschäftsanforderungen;
- Festlegung von Unternehmensrollen und Verantwortlichkeiten für die Entwicklung und Pflege des ISMS;
- ausreichende Ressourcen für die Planung, Durchführung, Organisation, Kontrolle, Überprüfung, Verwaltung und kontinuierliche Verbesserung des ISMS bereitzustellen;
- zu überprüfen, ob das ISMS in alle Geschäftsprozesse integriert ist und dass Verfahren und Kontrollen effektiv entwickelt werden;
- Genehmigung und Unterstützung aller Initiativen zur Verbesserung der Informationssicherheit und des Datenschutzes;
- Aktivierung von Programmen zur Verbreitung des Bewusstseins und der Kultur der Informationssicherheit und des Datenschutzes.

Lana, 24.04.2024 DIE GESCHÄFTSFÜHRUNG