L-06 Informationssicherheits-politik der SLM Solutions Group AG

Leitlinie

SLM Solutions Group
(im Folgenden SLM)

Geltungsbereich

Die Informationssicherheitspolitik gilt für alle Standorte und Mitarbeitenden der SLM Solutions Group AG.

Verantwortung

Der Vorstand von SLM trägt die Gesamtverantwortung für die Informationssicherheit und hat diese Informationssicherheitspolitik mit den festgehaltenen Zielen und den daraus abgeleiteten und abzuleitenden Konzepten verabschiedet. Sie unterstützt deren Erreichung durch geeignete personelle, materielle, organisatorische und technische Maßnahmen und die Bereitstellung der benötigten Ressourcen.

Die Geschäftsführung unterstützt und fördert die dazu notwendigen Strukturen und Prozesse und hat Verantwortliche benannt, die diese Informationssicherheitspolitik in Verfahrensanweisungen, Arbeitsanweisungen und Dokumentationen umsetzen und im Tagesgeschäft verankern.

Zweck

Die vorliegende Sicherheitsleitlinie ist eine Zusammenfassung aller Leitlinien zur Informationssicherheit von der SLM Solutions Group AG (“SLM”). Sie macht Vorgaben zum Stellenwert der Informationsverarbeitung und der Informationssicherheit, zu deren Zielen, zur Sicherheitsstrategie, dem definierten Geltungsbereich, zum Sicherheitsprozess sowie zur Sicherheitsorganisation.

Der Schutz sensibler Daten und Informationen des Geschäfts von SLM, der Kunden und Mitarbeitenden gehört zu den zentralen Werten SLMs.

Sicherheitsziele

Die Herstellung und Aufrechterhaltung der Informationssicherheit als wesentlicher Erfolgsfaktor für die Projektarbeit bei SLM wird durch die nachfolgend formulierten Ziele realisiert:

- ständige Verbesserung der Informationssicherheit innerhalb von SLM,
- frühzeitige Risikoidentifizierung und Risikominimierung,
- Sensibilisierung der Mitarbeitenden im Hinblick auf schützenswerte Informationen,
- Zusammenarbeit mit Herstellern und Entwicklern im Bereich der relevanten Branchen,
- durch Sicherheitsmängel oder -vorfälle darf es nicht zu kritischen Ausfällen und Beeinträchtigungen von Projekt- und Produktionsprozessen kommen,
- die für den Betrieb relevanten Gesetze und Vorschriften sowie vertragliche und aufsichtsrechtliche Verpflichtungen müssen eingehalten werden,
- durch Sicherheitsmängel oder -vorfälle darf kein nicht hinnehmbarer finanzieller Schaden entstehen,

- durch Sicherheitsmängel oder -vorfälle darf kein nicht tolerierbarer Reputationsverlust verursacht werden,
- durch Sicherheitsmängel oder -vorfälle darf kein nicht tolerierbarer Abfluss von personenbezogenen Daten, IT-Betriebsdaten, Entwicklungsdaten, Managementdaten oder Produktivdaten verursacht werden,
- die Aufrechterhaltung der Informationssicherheit muss als übergeordnetes Ziel den gleichen Stellenwert besitzen,
- die Sicherheitsziele betreffen alle Grundwerte der Informationssicherheit und richten sich nach den gesetzlichen Bestimmungen, insbesondere den jeweils aktuellen Schutzbedarfen der schützenswerten Informationen:

    - **Vertraulichkeit:** Zugang und Zutritt zu Informationsobjekten durch Unbefugte gilt es zu verhindern, insbesondere durch technische Maßnahmen, aber auch durch eine entsprechende Sensibilisierung der Mitarbeitenden wird die Vertraulichkeit geschützt und Manipulationen vorgebeugt.

    - **Integrität:** Fehlfunktionen und Unregelmäßigkeiten in Informationsobjekten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel.

    - **Verfügbarkeit:** Informationsobjekte und IT-Systeme in allen betriebsrelevanten Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandzeiten toleriert werden können.

Grundsätze

SLM verpflichtet sich, zum Schutz sensibler Daten geeignete Maßnahmen zur Sicherheit bei der elektronischen Verarbeitung zu ergreifen, sie zu dokumentieren, an die Mitarbeitenden zu kommunizieren und diese für die Belange des Datenschutzes und der Informationssicherheit zu sensibilisieren.

Daten und Informationen werden klassifiziert und mit Verfahren bearbeitet, die ihrer Klassifizierung angemessen sind.

SLM hat ein Risikomanagementsystem eingeführt, das Risiken für die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten und Informationen erkennt und auf ein angemessenes Maß begrenzt.

Veränderungen von Systemen und Anwendungen unterliegen einem definierten Change-Management-Prozess, der Aspekte des Datenschutzes und der Informationssicherheit berücksichtigt.

Durch regelmäßige interne Audits wird sichergestellt, dass die Vorgaben zum Datenschutz und zur Informationssicherheit von den Mitarbeitern umgesetzt und eingehalten werden, und dass Schwachstellen erkannt und Verbesserungsmöglichkeiten genutzt werden.