DATOLUTION
A member of SCHRANER-Group

Leitlinie zur Informationssicherheit

der DATOlution GmbH

DOKUMENTEN-EIGENSCHAFTEN	
	• Ersteller: Informationssicherheitsbeauftragter • Prüfer: Dr. Verena Schraner • Klassifizierung: **S1 öffentlich** • Gültigkeitszeit: Unbegrenzt • Überarbeitungsintervall: Jährlich • Nächste Überarbeitung: Oktober 2023 • Dateiname: DL-IS-Leitlinie
	ÖFFENTLICH

VERSIONSHISTORIE

Version	Datum	Änderungen	Autor
0.2	09.12.21	Initiales Dokument	Gräfe / Ijoschina
0.3	14.12.21	Eintrag des ISB Abschnitt „Bekanntmachung“ eingefügt	Gräfe
0.4	15.10.22	Layout und ISB aktualisiert	Gräfe
0.5	05.01.23	Satz zur Berichtslinie des ISB ergänzt	Gräfe
0.5	16.01.2023	Inhaltliche Überprüfung und Überarbeitung	Schraner
0.5	17.01.2023	Inhaltliche Finalisierung	Ijoschina
0.5	18.01.2023	Überarbeitung der Formatierung	Ijoschina
0.5	19.01.2023	Inhaltliche Überprüfung	Schraner
0.5	19.01.2023	Einarbeitung der Verbesserungsvorschläge von Verena Schraner	Ijoschina
0.5	23.01.2023	Freigabe	Schraner

INHALT

1. EINLEITUNG

Das Unternehmen wurde im Jahr 2016 mit dem Ziel gegründet, den sicherheitstechnischen und gebäudetechnischen Markt mit digitalen Lösungen und daran gekoppelten Dienstleistungen zu unterstützen. Der Fokus liegt hierbei derzeit auf Brandmeldeanlagen, soll aber zukünftig auf weitere sicherheitstechnische Anlagen, wie z.B. Einbruchmeldeanlagen oder Video-Anlagen ausgeweitet werden.

Die Informationsverarbeitung spielt eine Schlüsselrolle in der Leistungserbringung der DATOlution GmbH. Daher sind Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten und Informationen von existentieller Bedeutung für Erfolg, Ansehen und Fortbestand des Unternehmens.

Vor diesem Hintergrund ist ein angemessenes Niveau der Informationssicherheit in den Geschäftsprozessen der DATOlution GmbH zu organisieren. Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für die Informationssicherheit trägt die Geschäftsleitung der DATOlution GmbH.

Die vorliegende Leitlinie beschreibt die allgemeinen Ziele, Strategien und Organisationsstrukturen, welche für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind.

Die Begriffe „Daten“ und „Informationen“ werden in dieser Leitlinie synonym benutzt. Während mit Daten oftmals „Rohdaten/unverarbeitete Daten“ und mit Informationen „verarbeitete/aggregierte Daten“ gemeint sind, so wird bezüglich der Informationssicherheit kein Unterschied zwischen Daten und Informationen gemacht.

2. GELTUNGSBEREICH DES ISMS

Der Geltungsbereich des ISMS umfasst alle Bereiche des Unternehmens DATOlution GmbH. Sowohl der Standort in Erlangen als auch die Mitarbeiter in mobilen Arbeitssituationen sind Teil des ISMS.

Somit ist diese Leitlinie und die daraus resultierenden Vorschriften und Maßnahmen von allen Mitarbeitern der DATOlution GmbH zu beachten und einzuhalten.

3. STELLENWERT DER INFORMATIONSSICHERHEIT

Die Informationsverarbeitung nimmt für die Erfüllung der Unternehmensziele eine Schlüsselfunktion ein. Alle wesentlichen strategischen wie operativen Funktionen und Aufgaben werden durch Informationstechnik maßgeblich unterstützt. Um einen kontinuierlichen Geschäftsbetrieb zu gewährleisten, muss daher der Ausfall von IT-Systemen kurzfristig kompensiert werden können.

Als Hersteller von Softwarelösungen und daran angrenzende Dienstleistungen genießt die Informationssicherheit im Unternehmen einen sehr hohen Stellenwert.

4. GRUNDSÄTZE DER INFORMATIONSSICHERHEIT

Informationssicherheit bezeichnet die angemessene Aufrechterhaltung der Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit für Informationen und zugeordnete physische, technische

sowie personelle Werte entsprechend den geschäftlichen, gesetzlichen und regulatorischen Anforderungen eines Unternehmens. Dabei ist es unerheblich, in welcher Darstellungsform die Informationen vorliegen.

Dies beinhaltet insbesondere die Analyse und Behandlung von Risiken, welche die o.g. Sicherheitsziele gefährden und durch die Umsetzung angemessener Maßnahmen auf ein akzeptierbares Maß reduziert werden. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten und Informationen.

Dabei bedeuten:

- → **Vertraulichkeit:** Vertrauliche Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.
- → **Integrität:** Der Begriff der Integrität bezieht sich sowohl auf Informationen als auch auf das gesamte IT-System. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Auf IT-Systeme bezogen, bedeutet Integrität, dass Informationen und Daten ordnungsgemäßes verarbeitet und übertragen werden müssen. Nur dann kann die Integrität von Daten und Informationen sichergestellt werden.
- → **Verfügbarkeit:** Die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen müssen dem Anwender zum richtigen Zeitpunkt am richtigen Ort zur Verfügung stehen.

5. ZIELE DER INFORMATIONSSICHERHEIT

5.1. Übergeordnetes Ziel

Es ist das übergeordnete Ziel der DATOlution GmbH, dass alle Systeme und Anwendungen, die der …

- → Erstellung
- → Speicherung
- → Sicherung
- → Verarbeitung
- → Übertragung

… von Daten und Informationen dienen, **so ausgewählt, integriert und konfiguriert sind**, dass für die auf ihnen verarbeiteten Informationen zu jeder Zeit und unter allen Umständen **das angemessene Maß an**

- → Vertraulichkeit
- → Integrität
- → Verfügbarkeit

sichergestellt ist.

Dies schließt ausdrücklich alle beteiligten Mitarbeiter mit ein, sowohl am Standort in Erlangen als auch in mobilen Arbeitssituationen. Diese sind im erforderlichen Umfang bezüglich der Informationssicherheit zu sensibilisieren und zu qualifizieren.

Belange der Informationssicherheit sind zu berücksichtigen

- → in der Gestaltung der Organisationsstrukturen
- → bei der Schaffung und Besetzung von Funktionen und Rollen
- → bei der Führung von Mitarbeitern (Sensibilisierung, Schulung, Weiterbildung)
- → der Klassifizierung, Kennzeichnung, Handhabung, Übertragung und dem Schutz von Informationen
- → bei der Steuerung des Zugangs zu Informationen
- → bei der Auswahl, Beschaffung und Entsorgung von IT-Produkten und Hilfsmitteln
- → bei der Handhabung von Informationssicherheitsvorfällen und Notfällen
- → bei Change-Management Prozessen
- → bei der Zusammenarbeit mit Behörden und Externen
- → der Nutzung von Diensten (z.B. Clouddienste)
- → bei der Entwicklung und Bereitstellung von Produkten sowie Dienstleistungen
- → bei der Verbesserung der IT-Sicherheit unserer eigenen Produkte und Dienstleistungen

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Dieser wird durch den Wert der zu schützenden Informationen und der IT-Systeme definiert.

5.2. Sicherheitsziele

Die in den nachfolgenden Abschnitten genannten Ziele dienen dazu, die an die DATOlution GmbH gestellten gesetzlichen, regulatorischen und vertraglichen Anforderungen zu erfüllen. Sie werden mindestens jährlich überprüft und bei Bedarf aktualisiert.

5.2.1. Vertraulichkeit

Die durch IT-Systeme erhobenen, gespeicherten, verarbeiteten und weiter gegebenen Daten sind entsprechend ihrer Klassifizierung vertraulich zu behandeln und jederzeit vor unbefugtem Zugriff zu schützen. Zu diesem Zweck ist für alle Daten der Personenkreis, dem der Zugriff gestattet werden soll, zu bestimmen. Der Zugriff auf IT-Systeme, IT-Anwendungen und Daten sowie Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken. Jeder Mitarbeiter erhält eine Zugriffsberechtigung nur für die Daten, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt.

5.2.2. Integrität

Informationen und Software-Produkte sind gegen unbeabsichtigte Veränderung und vorsätzliche Verfälschung zu schützen. Alle Software-Produkte sollen stets aktuelle und vollständige Informationen liefern. Eventuelle verfahrens- oder informationsverarbeitungsbedingte Einschränkungen sind zu dokumentieren.

5.2.3. Verfügbarkeit

Für alle für den Betrieb unsere Software-Produkte und die Erbringung unserer Dienstleistungen

eingesetzten IT-Systeme sind die Zeiten, in denen sie verfügbar sein sollen, festzulegen. Betriebsunterbrechungen sind in diesen Zeiten weitgehend zu vermeiden, d. h. nach Zahl und Dauer zu begrenzen.

Die Beschreibung der notwendigen Verfügbarkeit umfasst

→ die regelmäßigen Betriebszeiten
→ die maximal tolerierbare Dauer einzelner Ausfälle

Ebenfalls festzulegen sind regelmäßig geplante Auszeiten, insbesondere zu Wartungszwecken.

6. KONTINUIERLICHE VERBESSERUNGEN

Das Managementsystem der Informationssicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit hin geprüft. Darüber hinaus wird auch die Sinnhaftigkeit und Angemessenheit der beschriebenen Maßnahmen hinterfragt und inwieweit sie in die betrieblichen Abläufe integriert werden können.

Durch kontinuierliche Überwachung der Regeln sowie deren Einhaltung seitens der Mitarbeiter wird das angestrebte Informationssicherheits- und Datenschutzniveau gewährleistet. Abweichungen werden dokumentiert und analysiert, um das ISMS weiterzuentwickeln und auf dem neuesten Stand zu halten.

7. INFORMATIONSSICHERHEITSORGANISATION

Die DATOlution GmbH hat ein ISMS-Team ins Leben gerufen, um die formulierten Ziele zu erreichen. Gesamtverantwortlich für das ISMS ist die Geschäftsleitung, die ihrerseits wiederum einen Informationssicherheits-Beauftragten (ISB) ernennt, der für die Einführung und regelmäßige Überprüfung des Systems verantwortlich ist. Der ISB steht in Fragen der Informationssicherheit beratend zur Seite und berichtet in dieser Funktion direkt an die Geschäftsleitung.

Das ISMS-Team ist seitens der Unternehmensführung mit ausreichenden finanziellen und zeitlichen Ressourcen ausgestattet, um sich regelmäßig weiterzubilden.

Darüber hinaus wurde ein Datenschutzbeauftragter bestellt, der angehalten ist, sich regelmäßig weiterzubilden.

8. PERSÖNLICHE VERANTWORTUNG

8.1. Geschäftsleitung

Die Geschäftsleitung der DATOlution übernimmt die Gesamtverantwortung für das ISMS. Die Geschäftsleitung der DATOlution bekennt sich zu ihrer Aufgabe, die in dieser Leitlinie beschriebenen Zielsetzungen zur Informationssicherheit zu unterstützen, und fordert alle Beschäftigten dazu auf, ebenfalls zur Aufrechterhaltung bzw. zur Verbesserung der Informationssicherheit beizutragen.

Die Geschäftsleitung erlässt verbindliche Regeln zur Informationssicherheit und gibt sie den Mitarbeitern bekannt. Sie stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher.

8.2. Mitarbeiter

Diese Leitlinie gilt für alle Mitarbeiter der DATOlution ohne Ausnahme. Es gibt keine Rechtfertigung für Abweichungen.

8.3. Externe Leistungserbringer

Personen und Unternehmen, die nicht zur DATOlution GmbH gehören, für diese aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie und einer zusätzlichen Richtlinie zur Informationssicherheit für Fremdfirmen einzuhalten. Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung.

9. MASSNAHMEN BEI VERSTÖSSEN

Verstöße gegen diese Leitlinie sowie Richtlinien und sonstige Vorschriften können zu erheblichen negativen Konsequenzen für die DATOlution GmbH führen. Deshalb ist bei vorsätzlichen und grob fahrlässigen Handlungen, die einen Verstoß darstellen, mit arbeitsrechtlichen Konsequenzen zu rechnen. Darüber hinaus können derartige Zuwiderhandlungen auch straf- oder zivilrechtliche Schritte nach sich ziehen.

Dr. Verena Schraner

Digital unterschrieben
von Dr. Verena Schraner
Datum: 2023.01.23
13:15:03 +01'00'

_____

Ort | Datum | Unterschrift der Geschäftsleitung