Sicherheitspolitik

Programm zur Umsetzung der reteach Sicherheitspolitik

Version 1.2
Letzte Bearbeitung: 06.07.2022

Inhalt

1. Übersicht

1.1. Einleitung und Geltungsbereich

Die Richtlinie beschreibt Grundsätze für einen angemessenen Schutz von Informationen in susell GmbH. Der Geltungsbereich ist das Unternehmen susell GmbH mit Sitz in Rosenthaler Str. 38, 10178 Berlin. Unternehmenswerte von susell GmbH mit einem hohen Schutzbedarf sind z. B.

- Die E-Learning-Plattform reteach
- Software-Quellcode und andere sensible Daten
- Persönliche und andere sensible Informationen, die susell GmbH im Rahmen seiner Geschäftstätigkeit speichert und verarbeitet

Der Inhalt wird von der Geschäftsleitung geprüft und offiziell freigegeben. Die Geschäftsleitung verpflichtet sich mit Freigabe zur

- Kontinuierlichen Verbesserung im Bereich des ISMS
- Ausreichenden Ressourcenfreigabe für das ISMS
- Systematischen Analyse ISMS-relevanter Anforderungen und kontinuierlichen Verfolgung der Erfüllung dieser Anforderungen

Verantwortlich für die regelmäßige Prüfung und ggf. Aktualisierung ist der ISM-Manager. Die in Sharepoint freigegebene und veröffentliche Fassung ist die gültige und verbindliche Fassung. Druckversionen dienen nur der Information. Diese kann nach Freigabe durch den Informationssicherheitsbeauftragten auch extern anfragenden Stellen (wie z.B. Kunden) zur Verfügung gestellt werden.

Die nachfolgenden Grundsätze der Richtlinie gelten uneingeschränkt und unmittelbar.

1.2. Grundsätze der Informationssicherheit

Alle Mitarbeitende sind verpflichtet, die Informationen des Unternehmens zu schützen, damit dem Unternehmen durch die unberechtigte Nutzung von Informationen kein Schaden entsteht.

Das Informationssicherheitsmanagement (ISMS) unterstützt Mitarbeitende und Führungskräfte bei der Umsetzung aller Sicherheitsrichtlinien und führt angemessene Kontrollen durch.

Ziel ist, die Sicherheit der Informationen im Unternehmen aufrecht zu erhalten, so dass die Geschäftsinformationen bei Bedarf verfügbar sind. Dies umfasst die

- Vertraulichkeit
- Verfügbarkeit und
- Integrität der Informationen

als oberste Schutzziele der Informationssicherheit.

Auf operativer Ebene werden durch das ISMS regelmäßig Ziele auf relevanten Ebenen definiert und an die jeweils verantwortlichen Personen zur Umsetzung weitergegeben.

Durch Sicherheitsmängel verursachte Ersatzansprüche, Schadensregulierungen, Image-Schäden für die Organisation sowie Missbrauch von organisationseigenen Informationen muss verhindert werden.

1.3. Zuständigkeit & Organisation

Der ISM-Manager, der von der Geschäftsleitung von susell GmbH eingesetzt wird, stellt die Entwicklung der Informationssicherheitspolitik und der damit verbundenen Standards sicher. Der Informationssicherheitsbeauftragte und das Sicherheitsmanagement verfolgen die Umsetzung der Sicherheitspolitik und vereinbaren entsprechende Maßnahmen. Das ISMS berät in Sicherheitsfragen, überwacht das Einhalten der Sicherheitsvorschriften und ermittelt und betreibt Aufklärung im Schadensfall.

Das Sicherheitsmanagement ist verantwortlich für:

- die Eskalation etwaiger Risiken an die Geschäftsleitung.
- die Beratung der Mitarbeitende zu Fragen des ISMS.
- für die Schulung der Mitarbeitende in Fragen der Informationssicherheit.

Die zuständigen Stellen der Informationsverarbeitung:

- unterstützen die Belange der Informationssicherheit,
- schaffen organisatorische wie technische Voraussetzungen für einen ausreichenden Schutz der betrieblichen Informationen, die mittels Informationstechnologie gespeichert, verarbeitet und übermittelt werden und überwachen - zusammen mit den Funktionen der Sicherheit - die Einhaltung der Sicherheitsmaßnahmen.

2. Informationssicherheit

Schäden für das Unternehmen oder Dritte können entstehen, wenn Unbefugte oder Nicht-Berechtigte Kenntnis von internen Informationen erlangen und diese zum Nachteil von susell GmbH und dessen Kunden verwenden. Daher müssen alle „Berechtigten“ einen wirkungsvollen Schutz der Informationen sicherstellen, unabhängig von der Form, in der sie vorliegen.

Beispiele:

- E-Mails, persönliche Mitteilungen, Telefonate, Schriftstücke, etc.
- Software-Quellcode, Datenbanken, Files etc.

Informationssicherheit bei susell GmbH bedeutet die Sicherheitsaufsicht, die Einhaltung und Durchsetzung der Informationssicherheit und die Durchführung von Bewertungen der Informationssicherheit.

2.1. Vorgaben

Als „Berechtigte“ dürfen alle Mitarbeitende von susell GmbH und externe Partner, die mit der Firma in einer Geschäftsbeziehung stehen, die zur Erfüllung ihrer Aufgaben erforderlichen Informationen erhalten („Need-to-know-Prinzip“). Alle Mitarbeitende sind verpflichtet, durch ihr Verhalten Informationen zu schützen, damit Schaden vom Unternehmen abgewendet wird.

2.2. Festlegung der Verantwortlichkeiten und der Vorgehensweise

- Jeder Informationsinhaber ist für den Schutz der Informationen verantwortlich, also für Kennzeichnung, Aufbewahrung, Speicherung, Verarbeitung, Weitergabe und Vernichtung.

- Führungskräfte veranlassen für ihre Aufgabenumfänge und Geschäftsprozesse Schutzmaßnahmen für die Informationen. Hierbei sind Verfügbarkeit, Integrität und Authentizität sowie die Vertraulichkeit der Informationen zu berücksichtigen.
- Der Informationsgeber stellt bei Informationen mit vertraulichem Inhalt sicher, dass der Informationsempfänger über den Grad der Vertraulichkeit und den besonderen Umgang mit einer Information Kenntnis erhält. Hierzu muss die Information unabhängig von der Art der Übermittlung entsprechend den gültigen Regeln gekennzeichnet und geschützt werden.
- Kundendaten und Informationen, die den Kunden betreffen, sind vertraulich und zweckbestimmt zu behandeln.

3. Personalsicherheit

Susell GmbH stellt hohe Ansprüche an Mitarbeitende für ethisches Geschäftsverhalten auf allen Ebenen des Unternehmens. Diese umfassen Mitarbeitende sowie Auftragnehmer und Kunden. Sie betreffen die Einhaltung rechtlicher und regulatorischer Vorschriften sowie das Geschäftsgebaren und die Geschäftsbeziehungen. Susell GmbH schult seine Mitarbeitenden in Ethik und Geschäftsgebaren alle zwei Jahre.

3.1. Schwerpunkt Sicherheit

Das Unternehmen führt laufend Initiativen durch, die dazu beitragen, Risiken im Zusammenhang mit menschlichem Versagen, Diebstahl, Betrug und Missbrauch von Einrichtungen zu minimieren. Maßnahmen die gewährleisten, dass ausschließlich vertrauenswürdiges und gut ausgebildetes Personal, das mit angemessenem Datenschutz und Informationssicherheit Bewusstsein agiert, für susell GmbH tätig ist.

3.2. Verschwiegenheit

Mitarbeitende sind verpflichtet, die Vertraulichkeit von Kundendaten zu wahren. Mitarbeitende verpflichten sich mit Eintritt in das Unternehmen Vertraulichkeit zu allen Geschäftsvorgängen zu wahren und Unternehmensrichtlinien zum Schutz vertraulicher Informationen als Teil ihrer ursprünglichen Beschäftigungsbedingungen einzuhalten. Subunternehmen und relevante Dienstleister werden von Masterplan auf Compliance zu Susell GmbH Vorgaben regelmäßig geprüft.

3.3. Ausbildung und Weiterentwicklung des Sicherheitsbewusstseins

susell GmbH fördert das Sicherheitsbewusstsein und schult seine Mitarbeitende regelmäßig.

Jeder Mitarbeitende verpflichtet sich, bei seiner Einstellung und anschließend alle zwei Jahre eine Schulung zum Thema Informationssicherheit zu absolvieren. Dieses Training schult die Mitarbeitende zur Einhaltung von Datenschutz und Sicherheitsrichtlinien und -prinzipien von susell GmbH.

3.4. Umsetzung

Es werden in regelmäßigen Abständen Sicherheitsüberprüfungen und Audits durchgeführt, um die Einhaltung der Richtlinien, Verfahren und Prozeduren der Informationssicherheit von susell GmbH zu gewährleisten.

4. Zugriffskontrolle

Die Zugangskontrollen beziehen sich auf die Richtlinien, Verfahren und Instrumente, die den Zugang zu und die Nutzung von Ressourcen regeln. Beispiele für Ressourcen sind physische Server, Dateien, Verzeichnisse, Dienste, die auf einem Betriebssystem laufen, Tabellen einer Datenbank oder Netzwerkprotokolle.

Least Privilege ist ein systemorientierter Ansatz, bei dem die Benutzerrechte und die Systemfunktionalität sorgfältig evaluiert werden und der Zugriff auf die Ressourcen beschränkt ist, die die Benutzer oder Systeme zur Erfüllung ihrer Aufgaben benötigen.

4.1. Zugriffskontrollrichtlinien und -praktiken

Die Richtlinie zur logischen Zugriffskontrolle gilt für Zugriffskontrollentscheidungen für alle Mitarbeitenden und alle informationsverarbeitenden Einrichtungen, für die susell GmbH Verwaltungsbefugnisse hat.

4.2. Verwaltung von Privilegien

Die Autorisierung hängt von einer erfolgreichen Authentifizierung ab, da die Kontrolle des Zugriffs auf bestimmte Ressourcen von der Feststellung der Identität einer Entität oder Person abhängt. Alle Autorisierungsentscheidungen von Susell GmbH für die Gewährung, Genehmigung und Überprüfung des Zugriffs basieren auf den folgenden Prinzipien:

- Need to know: Benötigt der Benutzer diesen Zugriff für seine Arbeitsfunktion?
- Trennung der Aufgaben: Führt der Zugriff zu einem Interessenkonflikt?
- Geringste Privilegien (Least Privilege): Ist der Zugang nur auf die Ressourcen und Informationen beschränkt, die für einen legitimen Geschäftszweck erforderlich sind?

4.3. Benutzer-Passwortverwaltung

Susell GmbH setzt starke Passwortrichtlinien für das Susell GmbH-Netzwerk, das Betriebssystem und die Datenbankkonten durch, um die Chancen zu verringern, dass Eindringlinge durch Ausnutzung von Benutzerkonten und zugehörigen Passwörtern Zugang zu Systemen oder Umgebungen erhalten.

4.4. Periodische Überprüfung der Zugriffsrechte

Susell GmbH überprüft regelmäßig Netzwerk- und Betriebssystemkonten im Hinblick auf die entsprechenden Zugriffsebenen der Mitarbeitende. Im Falle von Kündigungen, Todesfällen oder Rücktritten von Mitarbeitenden ergreift das Unternehmen geeignete Maßnahmen um physische & virtuelle Zugänge unverzüglich zu beenden.

4.5. Passwort-Richtlinie

Die Verwendung von Passwörtern wird in der Susell GmbH Password Policy behandelt. Mitarbeitende sind verpflichtet, Regeln für die Länge und Komplexität von Passwörtern einzuhalten und ihre Passwörter jederzeit vertraulich und sicher zu behandeln. Passwörter dürfen nicht an unbefugte Personen weitergegeben werden. Unter bestimmten Umständen können autorisierte Susell GmbH-Mitarbeitende Passwörter zum Zweck der Bereitstellung von Support-Dienstleistungen gemeinsam nutzen.

4.6. Netzwerk-Zugangsmaßnahmen

Susell GmbH hat starke Netzwerkmaßnahmen eingeführt und hält diese aufrecht, um den Schutz und die Kontrolle von Kundendaten während ihrer Übertragung von einem Endsystem zum anderen zu

gewährleisten. Die Susell GmbH-Richtlinie zur Nutzung von Netzwerkdiensten besagt, dass Endpunkte, die mit dem Susell GmbH-Netzwerk verbunden sind, gut etablierten Standards für Sicherheit, Konfiguration und Zugriffsmethode entsprechen müssen.

5. Datensicherheit

Die Klassifizierung der Information Assets von Susell GmbH bestimmt die Anforderungen des Unternehmens an die Datensicherheit von Susell GmbH-verwalteten Systemen. Susell GmbH-Richtlinien und -Standards bieten eine Anleitung für angemessene Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmensdaten in Übereinstimmung mit der Datenklassifizierung. Die erforderlichen Mechanismen sind so konzipiert, dass sie mit der Art der zu schützenden Unternehmensdaten in Einklang stehen. Beispielsweise sind die Sicherheitsanforderungen bei sensiblen oder wertvollen Daten wie Cloud-Systemen, Quellcode‘s und Beschäftigungsaufzeichnungen höher.

Die Sicherheitsmaßnahmen von Susell GmbH lassen sich in drei Kategorien einteilen: administrative, physische und technische Sicherheitsmaßnahmen.

- Administrative Maßnahmen, einschließlich logischer Zugriffskontrolle und Personalprozesse.
- Physische Maßnahmen, die den unbefugten physischen Zugang zu Servern und Datenverarbeitungsumgebungen verhindern sollen.
- Technische Maßnahmen, einschließlich sicherer Konfigurationen und Verschlüsselung für Daten im Ruhezustand und bei der Übertragung (Data at Rest, Data in Motion).

Darüber hinaus verfügt Susell GmbH über formelle Programme, um die Entwicklung der Plattform zu steuern. Diese umfasst jede Phase des Produktentwicklungs-Lebenszyklus und ist die Methodik für den Einbau von Sicherheit in das Design, den Aufbau, das Testen und die Wartung seiner Plattform.

5.1. Sicherheitspolitik für Endgeräte (Stationär und mobil)

Die susell GmbH-Richtlinie schreibt den Einsatz von Antiviren-, IPS und Firewall-Software auf Endgeräten - soweit möglich - vor. Darüber hinaus müssen auf allen Endgeräten automatisierte Sicherheitsupdates und Updates der Virensignaturen aktiviert sein. Endgeräte, die Daten von susell GmbH oder Kundendaten verarbeiten, werden mit zugelassener Software verschlüsselt.

5.2. Schutz vor bösartigem Code

Mitarbeitende müssen die E-Mail-Anweisungen von Susell GmbH befolgen und sind dafür verantwortlich, dem Helpdesk für Susell GmbH-Mitarbeitende umgehend jeden Virus oder vermuteten Virenbefall zu melden, der nicht durch Antiviren-Software behoben werden kann.

Den Mitarbeitenden ist es untersagt, Antiviren-Software und den Sicherheits-Update-Service von jedem Computer aus zu verändern, zu deaktivieren oder zu entfernen. Jeder Mitarbeitende, der gegen diesen Standard verstößt, kann Disziplinarmaßnahmen bis hin zur Kündigung des Arbeitsverhältnisses unterworfen werden.

5.3. Endgeräte Verschlüsselung

Zum Schutz sensibler Informationen müssen die Mitarbeitenden von susell GmbH genehmigte Verschlüsselungssoftware auf ihren Endgeräten installieren.

5.4. Physische und Umgebungsbezogene Sicherheit

5.4.1. Risikobasierter Ansatz

Globale physische Sicherheit verwendet einen risikobasierten Ansatz für physische und umgebungsbezogene Sicherheit. Ziel ist es, Prävention, Erkennung, Schutz und Reaktion in ein Gleichgewicht zu bringen und gleichzeitig ein positives Arbeitsumfeld aufrechtzuerhalten, das Innovation und Zusammenarbeit zwischen Mitarbeitenden, Kunden und Partnern fördert. Susell GmbH führt regelmäßig Risikobewertungen durch, um zu bestätigen, dass die korrekten und wirksamen Maßnahmen zur Risikominderung vorhanden sind und aufrechterhalten werden.

5.4.2. Präventive Maßnahmen: Schutz von Assets und Mitarbeitenden

Susell GmbH hat die folgenden Protokolle implementiert:

- Der physische Zugang zu den Einrichtungen ist auf Susell GmbH-Mitarbeitende , Auftragnehmer und autorisierte Besucher beschränkt.
- Besucher sind verpflichtet, begleitet und/oder beobachtet zu werden, wenn sie sich in den Räumlichkeiten von Susell GmbH aufhalten, und/oder an die Bedingungen einer Vertraulichkeitsvereinbarung mit Susell GmbH gebunden zu sein.
- Susell GmbH überwacht den Besitz von Schlüsseln/Zugangskarten und die Möglichkeit des Zugangs zu Einrichtungen. Mitarbeitende, die aus dem Arbeitsverhältnis mit Susell GmbH ausscheiden, müssen Schlüssel/Karten zurückgeben, und Schlüssel/Karten werden bei Kündigung deaktiviert.

5.4.3. Sicherheit im Rechenzentrum

Die reteach-Plattform läuft in Rechenzentren die dazu beitragen, die Sicherheit und Verfügbarkeit von Kundendaten zu schützen. Dieser Ansatz beginnt mit dem Standortauswahlverfahren von susell GmbH. Die Rechenzentren entsprechen den ANSI/TIA-942-A Tier 3- oder Tier 4-Standards des Uptime Institute and Telecommunications Industry Association (TIA). Rechenzentren, die susell GmbH Plattform beherbergen, verwenden redundante Stromquellen und unterhalten Generator-Backups für den Fall eines weit verbreiteten Stromausfalls. Diese werden genau auf Lufttemperatur und Luftfeuchtigkeit überwacht, und es sind Brandbekämpfungssysteme vorhanden. Das Personal des Rechenzentrums ist in der Reaktion auf Vorfälle und in Eskalationsverfahren geschult, um auf mögliche Sicherheits- und Verfügbarkeitsereignisse reagieren zu können.

Folgende Rechenzentren werden von susell GmbH für den Betrieb der reteach-Plattform verwendet:

- **DigitalOcean**
  (Standort „fra1“ – Frankfurt am Main, Deutschland)

  Zertifizierungen: ISO 27001:203, SOC 2 Type II, PCI-DSS (Mehr Infos)
  Verwendung: Datenbank, Cloud-Server für die Applikationen (Kubernetes), File-Server

  Verschlüsselung:
  Alle Daten, die permanent in Datenbanken gespeichert sind, werden mit LUKS (Linux Unified Key Setup) serverseitig verschlüsselt. Alle Dateien, die permanent in DigitalOcean Spaces gespeichert sind, werden serverseitig verschlüsselt. Auf die Schlüssel hat DigitalOcean und in Teilen unser Infrastruktur-Team Zugriff.

Backup:
Die Datenbank kann für 7 Tage rückwirkend minutengenau wiederhergestellt werden. Zusätzlich dazu wird täglich ein Backup erstellt und für 180 Tage in AWS S3 verschlüsselt gespeichert. Recovery-Übungen werden im 90 Tage-Rhythmus wiederholt.
Der File-Storage Spaces hält alle Versionen einer Datei für 180 Tage gespeichert. Dies schließt sowohl Änderungen als auch Löschungen von Dateien ein.

- **Amazon Web Services - AWS**
  (Standort „eu-central-1“ – Frankfurt am Main, Deutschland)

  Zertifizierungen: ISO 27001:2015, CSA STAR CCM v3.0.1 (Mehr Infos)
  Verwendung: File-Server, E-Mail-Versand

  Verschlüsselung:
  Alle Dateien, die permanent bei AWS gespeichert werden, sind dort serverseitig verschlüsselt. Die Schlüssel liegen im AWS Key Management Service (SSE-KMS) auf welchen unser Infrastruktur-Team und AWS Zugriff hat.

  Backup:
  Der File-Storage S3 ist hält alle Versionen einer Datei für 180 Tage gespeichert werden. Dies schließt sowohl Änderungen als auch Löschungen von Dateien ein.

6. Reaktion auf Vorfälle

Susell GmbH bewertet und reagiert auf Ereignisse, die den Verdacht auf unbefugten Zugriff auf oder im Umgang mit Kundendaten begründen, unabhängig davon, ob sich die Daten auf Susell GmbH-Hardware-Assets oder auf den persönlichen Hardware-Assets von Susell GmbH-Mitarbeitenden befinden. Susell GmbH’s Information Security Incident Reporting and Response Policy definiert Anforderungen für die Berichterstattung und Reaktion auf Vorfälle. Diese Richtlinie autorisiert Sicherheitsorganisation, als Hauptansprechpartner für die Reaktion auf Sicherheitsvorfälle zu fungieren und die allgemeine Richtung für die Vorbeugung, Identifizierung, Untersuchung und Lösung von Vorfällen vorzugeben.

Die Unternehmensanforderungen für Vorfallreaktionsprogramme und Einsatzteams werden pro Vorfallart definiert:

- Validierung, dass ein Vorfall aufgetreten ist
- Kommunikation mit relevanten Parteien und Benachrichtigungen
- Beweissicherung
- Dokumentieren eines Vorfalls selbst und der damit verbundenen Reaktionsaktivitäten
- Eindämmen eines Vorfalls
- Beseitigung eines Vorfalls
- Eskalieren eines Vorfalls

Bei Entdeckung eines Vorfalls definiert susell GmbH einen Vorfall-Reaktionsplan für eine schnelle und effektive Untersuchung, Reaktion und Wiederherstellung des Vorfalls. Es wird eine Ursachenanalyse durchgeführt, um Möglichkeiten für angemessene Maßnahmen zu identifizieren, die die Sicherheitshaltung und -abwehr im Detail verbessern. Formale Verfahren und zentrale Systeme

werden eingesetzt, um während der Untersuchung eines Vorfalls Informationen zu sammeln und eine Beweismittelkette zu unterhalten. Susell GmbH ist in der Lage, bei Bedarf die rechtlich zulässige forensische Datenerfassung zu unterstützen.

6.1. Benachrichtigungen

Für den Fall, dass Susell GmbH feststellt, dass ein Sicherheitsvorfall eingetreten ist, benachrichtigt susell GmbH unverzüglich alle betroffenen Kunden oder andere Dritte in Übereinstimmung mit seinen vertraglichen und gesetzlichen Verpflichtungen. Informationen über böswillige Versuche oder vermutete Vorfälle sind susell GmbH vertraulich und werden nicht nach außen weitergegeben. Die Vorfallhistorie wird nicht nach außen weitergegeben.

6.2. Sicherheitslücken

Um eine Sicherheitslücke an Susell GmbH zu melden, verwenden Sie bitte folgende E-Mail-Adresse: security@reteach.io

7. Weiterführende Vorgaben des ISMS

Alle Policies, Anweisungen und Leitlinien von suell GmbH sind auf Sharepoint zur Verfügung gestellt. Neben den Maßnahmen und Regelungen zur Informationssicherheit werden hier auch Anweisungen für besonders schützenswerte Informationen sowie nützliche Hilfsmittel für alle Mitarbeitende angegeben. Das Dokument Informationssicherheitspolitik ist auf Sharepoint hinterlegt und für jeden Mitarbeitende jederzeit einsehbar. Verbindliche Verfahrens- und Arbeitsanweisungen und die Organisationsstruktur sind ebenfalls auf Sharepoint hinterlegt und für jeden Mitarbeitenden jederzeit einsehbar.

Gesetzliche, behördliche und vertragliche Anforderungen sind von allen Mitarbeitenden einzuhalten.

8. Risikomanagement

Die Zuständigkeit für die regelmäßige Ermittlung und Bewertung der Risiken verbleibt beim jeweiligen Prozesseigentümer, der die aktuellen Gegebenheiten sowie speziellen Änderungen innerhalb der Geschäftsprozesse in seinem Einflussbereich berücksichtigt.

Das Risikomanagement wird entsprechend des „kombinierten Ansatzes“ durchgeführt. Die Rahmenbedingungen sind im Risikomanagement-Handbuch detailliert beschrieben.

Die vorgabenkonforme Durchführung wird durch das ISMS-Team gewährleistet. Die Gesamtverantwortung trägt die Geschäftsleitung.

9. Unabhängige Prüfung

Die Einhaltung dieser Policy sowie der darunter liegenden Vorgaben wird regelmäßig in internen Audits. Gegenstand einer Prüfung sind insbesondere

- Kontrollen im Zusammenhang mit den Informationen,
- Zugriffsmöglichkeit zu den Informationen,
- Verwaltung der Informationen, einschließlich der Trennung von Rollen und unabhängige Genehmigung/Überprüfung relevanter Vorgänge,
- Maßnahmen zur Wiederherstellung von Informationen und Verfahren.

10. Verstöße

Als Verstöße gelten beabsichtigte oder grob fahrlässige Handlungen, die

- eine Kompromittierung des Rufes von suell GmbH darstellen,
- die Sicherheit der Mitarbeitenden, Kunden, Vertragspartner, Berater und des Vermögens von susell GmbH kompromittieren,
- die Sicherheit von Informationen hinsichtlich deren Verfügbarkeit, Integrität und Vertraulichkeit gefährden.
- die dem tatsächlichen oder potenziellen finanziellen Verlust einbringen - durch die Kompromittierung der Sicherheit von Daten oder Geschäftsinformationen,
- den unberechtigten Zugriff auf Informationen, deren Preisgabe und/oder Änderung beinhalten,
- die Nutzung von Unternehmensinformationen für illegale Zwecke beinhalten.

Die Nichteinhaltung oder bewusste Verletzung der Informationssicherheitspolitik führt zu einer der nachfolgenden Aktionen, ist aber nicht auf diese beschränkt:

- disziplinarische oder arbeitsrechtliche Folgen,
- straf- und/oder zivilrechtliche Verfahren.
- Haftung und Regressforderungen

11. Ansprechpartner

ISM-Manager:

Markus Aurich
markus@reteach.io
030/235939582