Informationssicherheits-Managementsystem (ISMS)

Version	3.1
Letzte Bearbeitung	15.07.2026
Geltungsbereich	Susell GmbH, Joachimstraße 7, 10119 Berlin (inkl. Remote-/Hybrid-Arbeitsplätze)
Freigabe GF	Dr. Andreas Bersch, Geschäftsführer
Freigabe ISM-Manager	Joscha Klopfer (Head of Engineering)
Klassifikation	keine Einschränkung

Änderungen gegenüber v3.0: EU-Aussagen an Regelbetrieb/modulgebunden-Linie angepasst (Abschnitt 2.1, 8, 9, 11); PITR-Angabe vereinheitlicht (7 Tage); S1-Erstreaktion vereinheitlicht (30 Minuten); Unterauftragnehmer-Liste aktualisiert (Bunny ergänzt, Billwerk+ → Frisbii, Phishing Tackle ergänzt, A/B-Struktur); Vertretungsberechtigte korrigiert.

1. Übersicht

1.1. Einleitung und Geltungsbereich

Die Richtlinie beschreibt Grundsätze für einen angemessenen Schutz von Informationen bei der Susell GmbH. Der Geltungsbereich umfasst:

- Die Susell GmbH mit Sitz in Joachimstraße 7, 10119 Berlin
- Alle Remote- und Hybrid-Arbeitsplätze der Mitarbeitenden
- Die E-Learning-Plattform reteach und zugehörige Infrastruktur
- Software-Quellcode und andere sensible Daten
- Persönliche und andere sensible Informationen, die Susell GmbH im Rahmen ihrer Geschäftstätigkeit speichert und verarbeitet

1.2. Normenbezug

Das ISMS der Susell GmbH orientiert sich an ISO 27001. Die vorliegende Policy bildet die oberste Leitlinie des ISMS und wird durch weiterführende Richtlinien konkretisiert.

1.3. Grundsätze der Informationssicherheit

Alle Mitarbeitenden sind verpflichtet, die Informationen des Unternehmens zu schützen, damit dem Unternehmen durch die unberechtigte Nutzung von Informationen kein Schaden entsteht. Das ISMS unterstützt Mitarbeitende und Führungskräfte bei der Umsetzung aller Sicherheitsrichtlinien und führt angemessene Kontrollen durch. Ziel ist die Aufrechterhaltung von Vertraulichkeit, Verfügbarkeit und Integrität der Informationen als oberste Schutzziele.

1.4. Zuständigkeit & Organisation

Der ISM-Manager, eingesetzt von der Geschäftsleitung der Susell GmbH, stellt die Entwicklung der Informationssicherheitspolitik und der damit verbundenen Standards sicher.

1.5. Review-Zyklus und Freigabe

Die ISM-Policy wird jährlich durch den ISM-Manager überprüft und bei Bedarf aktualisiert. Die Freigabe erfolgt durch die Geschäftsführung. Außerordentliche Reviews werden bei wesentlichen Änderungen der Bedrohungslage, Organisationsstruktur oder regulatorischen Anforderungen ausgelöst.

2. Informationssicherheit

Schäden für das Unternehmen oder Dritte können entstehen, wenn Unbefugte Kenntnis von internen Informationen erlangen. Alle Berechtigten müssen einen wirkungsvollen Schutz der Informationen sicherstellen, unabhängig von der Form, in der sie vorliegen.

2.1. Vorgaben

Als Berechtigte dürfen alle Mitarbeitenden 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).

2.2. Datenklassifikation

Susell GmbH klassifiziert Informationen in drei Stufen: Öffentlich, Intern, Vertraulich. Die Kennzeichnung und Handhabung richtet sich nach der jeweiligen Stufe und ist in der Datenklassifikationsrichtlinie im Detail beschrieben.

2.3. Verantwortlichkeiten

Jeder Informationsinhaber ist für den Schutz der Informationen verantwortlich. Führungskräfte veranlassen für ihre Aufgabenumfänge Schutzmaßnahmen. Kundendaten und kundenrelevante Informationen sind vertraulich und zweckbestimmt zu behandeln.

3. Personalsicherheit

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.

3.2. Verschwiegenheit

Mitarbeitende sind verpflichtet, die Vertraulichkeit von Kundendaten (insbesondere Personaldaten von Kunden) zu wahren. Mitarbeitende verpflichten sich mit Eintritt in das Unternehmen, Vertraulichkeit zu allen Geschäftsvorgängen zu wahren. Subunternehmen und relevante Dienstleister werden von Susell GmbH auf Compliance zu den Unternehmensvorgaben regelmäßig geprüft.

3.3. Ausbildung und Sicherheitsbewusstsein

Alle Mitarbeitenden müssen bei Einstellung und anschließend jährlich eine Schulung zum Thema Informationssicherheit absolvieren. Ergänzend werden laufend Phishing-Simulationen durchgeführt.

4. Zugriffskontrolle

Die Zugangskontrollen beziehen sich auf die Richtlinien, Verfahren und Instrumente, die den Zugang zu und die Nutzung von Ressourcen regeln. Es gilt das Prinzip der geringsten Privilegien (Least Privilege).

4.1. Multi-Faktor-Authentifizierung (MFA)

Für alle geschäftskritischen Systeme ist Multi-Faktor-Authentifizierung verpflichtend.

4.2. Verwaltung von Privilegien

Alle Autorisierungsentscheidungen basieren auf den Prinzipien Need-to-know, Aufgabentrennung und Least Privilege.

4.3. Passwort-Richtlinie

Mindestlänge: 16 Zeichen. Komplexität: Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen. Rotation: Keine erzwungene Rotation bei Nutzung von MFA. Die Nutzung eines vom Unternehmen bereitgestellten und zentral verwalteten Passwort-Managers ist verpflichtend.

4.4. Periodische Überprüfung der Zugriffsrechte

Susell GmbH überprüft regelmäßig Netzwerk- und Betriebssystemkonten. Bei Ausscheiden von Mitarbeitenden werden physische und virtuelle Zugänge unverzüglich deaktiviert.

4.5. Netzwerk-Zugangsmaßnahmen

Susell GmbH hat starke Netzwerkmaßnahmen eingeführt, um den Schutz und die Kontrolle von Kundendaten während ihrer Übertragung zu gewährleisten. Endpunkte müssen etablierten Standards für Sicherheit, Konfiguration und Zugriffsmethode entsprechen.

5. Datensicherheit

5.1. Endgerätesicherheit

Auf allen Endgeräten werden Antiviren-, IPS- und Firewall-Software eingesetzt, soweit technisch möglich. Automatisierte Sicherheitsupdates und Virensignaturen müssen aktiviert sein.

5.2. Patch-Management

Sicherheitsupdates werden durch das Engineering auf Dringlichkeit und Relevanz geprüft. Kritische Updates werden innerhalb 24h nach Information eingespielt.

5.3. Logging und Monitoring

Logs und Traces der Infrastruktur sowie Applikationen werden zentral erfasst und für 7 Tage gespeichert.

5.4. Schutz vor bösartigem Code

Mitarbeitende sind dafür verantwortlich, dem Helpdesk umgehend jeden Virus oder vermuteten Virenbefall zu melden. Die Deaktivierung oder Entfernung von Antiviren-Software ist untersagt.

5.5. Endgeräte-Verschlüsselung

Zum Schutz sensibler Informationen setzen Mitarbeitende genehmigte Verschlüsselungssoftware auf ihren Endgeräten ein.

5.6. Physische und umgebungsbezogene Sicherheit

Susell GmbH verfolgt einen risikobasierten Ansatz für physische Sicherheit. Der physische Zugang zu Einrichtungen ist auf Mitarbeitende, Auftragnehmer und autorisierte Besucher beschränkt.

5.6.1. Sicherheit im Rechenzentrum

Die reteach-Plattform läuft in Rechenzentren, die den ANSI/TIA-942-A Tier 3- oder Tier 4-Standards entsprechen.

Amazon Web Services (Standort eu-central-1 – Frankfurt am Main): Zertifizierungen: ISO 27001:2022, SOC 2 Type II, CSA STAR, PCI-DSS. Verschlüsselung: SSE-KMS. Backup: Datenbank 7-Tage-PITR plus 180-Tage-Backup auf AWS S3 (verschlüsselt). Recovery-Übungen im 90-Tage-Rhythmus. File-Storage: 180 Tage Versionierung inkl. Löschungen.

6. Secure Development Lifecycle (SDLC)

Susell GmbH integriert Sicherheit in jede Phase des Produktentwicklungs-Lebenszyklus. Alle Code-Änderungen werden durch mindestens zwei Engineers geprüft. Eingesetzte Abhängigkeiten werden automatisiert auf bekannte Schwachstellen geprüft (Dependabot); Container-Images werden über AWS-Scanning geprüft. Penetrationstests durch externe Dienstleister finden jährlich statt.

7. Nutzung von KI-Tools und Cloud-Diensten

Susell GmbH regelt die Nutzung von KI-basierten Tools in einer separaten KI-Acceptable-Use-Policy. Grundsätzlich gilt:

- Kundendaten und vertrauliche Informationen dürfen nicht in öffentliche KI-Tools eingegeben werden
- Es dürfen nur von der IT freigegebene KI-Tools verwendet werden
- Die Verarbeitung personenbezogener Daten durch KI-Tools muss den DSGVO-Anforderungen entsprechen

8. Lieferanten- und Dienstleister-Management

Susell GmbH führt ein Verzeichnis kritischer Dienstleister und Unterauftragnehmer. Die Sicherheitskonformität wird regelmäßig durch die Geschäftsführung geprüft.

9. Business Continuity und Disaster Recovery

Susell GmbH verfügt über einen Business-Continuity-Plan, der die Wiederherstellung geschäftskritischer Systeme regelt. Applikationen sind stateless und innerhalb von Minuten wiederherstellbar.

- RPO: unter 10 Minuten (Point-in-Time-Recovery)
- RTO: unter 4 Stunden
- Datenbank-Backup: Point-in-Time-Recovery für 7 Tage (minutengenau), anschließend tägliche verschlüsselte Backups für 180 Tage
- File-Storage: Versionierung aller Dateien für 180 Tage, einschließlich Änderungen und Löschungen
- Recovery-Tests: Alle 90 Tage vollständige Wiederherstellung in Testumgebung

10. Reaktion auf Vorfälle

Susell GmbH bewertet und reagiert auf Ereignisse, die den Verdacht auf unbefugten Zugriff oder Umgang mit Kundendaten begründen.

10.1. Severity-Klassifikation und Reaktionszeiten

Stufe	Bezeichnung	Erstreaktion	Kundeninfo
S1 (Kritisch)	Bestätigter Data Breach, Ransomware	Unter 30 Minuten	Unverzüglich, spätestens 48h ab Kenntnis
S2 (Hoch)	Verdacht auf Kompromittierung	Unter 4 Stunden	Nach Bestätigung
S3 (Mittel)	Schwachstelle ohne Ausnutzung	Unter 24 Stunden	Bei Bedarf
S4 (Niedrig)	Sicherheitsrelevante Beobachtung	Unter 72 Stunden	Nicht erforderlich

10.2. Benachrichtigungen

Im Falle eines Sicherheitsvorfalls benachrichtigt Susell GmbH unverzüglich alle betroffenen Kunden, spätestens 48 Stunden ab eigener Kenntnis, damit diese ihre Meldepflicht nach Art. 33 DSGVO (72 Stunden) erfüllen können. Die Meldung enthält: Art des Vorfalls, betroffene Datenkategorien, ergriffene und geplante Maßnahmen.

10.3. Sicherheitslücken melden

Um eine Sicherheitslücke an Susell GmbH zu melden: sicherheit@reteach.com

11. Datenschutz und DSGVO

Datenschutz wird von der Geschäftsführung verantwortet. Die Susell GmbH ist gemäß § 38 BDSG nicht verpflichtet, einen Datenschutzbeauftragten zu bestellen. Relevante Dokumente: Verzeichnis der Verarbeitungstätigkeiten (VVT), Vereinbarung zur Auftragsverarbeitung (AVV).

12. Risikomanagement

Die Zuständigkeit für die regelmäßige Ermittlung und Bewertung der Risiken verbleibt beim jeweiligen Prozesseigentümer. Die Rahmenbedingungen sind im Risikomanagement-Handbuch detailliert beschrieben.

13. Unabhängige Prüfung

Die Einhaltung dieser Policy wird regelmäßig in internen Audits überprüft.

14. Verstöße

Als Verstöße gelten beabsichtigte oder grob fahrlässige Handlungen, die den Ruf der Susell GmbH kompromittieren, die Sicherheit von Mitarbeitenden, Kunden oder Vermögen gefährden, oder die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen beeinträchtigen. Die Nichteinhaltung führt zu disziplinarischen oder arbeitsrechtlichen Folgen.

Kontakt: datenschutz@reteach.com | sicherheit@reteach.com

Anlage: Informationssicherheit, Datenschutz und Infrastruktur

1. Einführung

Als Betreiber der Lernplattform reteach sind wir uns unserer Verantwortung bewusst, die Daten Ihrer Mitarbeitenden auf unserem System zu schützen. Dieses Dokument gibt einen Überblick über die Sicherheitsmaßnahmen, die wir zum Schutz Ihrer Daten implementiert haben. Es richtet sich als Information ohne rechtliche oder vertragliche Wirkung an IT-Sicherheitsverantwortliche, Datenschutzbeauftragte und Einkaufsabteilungen. Es gelten unsere AGB sowie die mit unseren Kunden separat abgeschlossene AVV.

2. Plattform-Architektur und Hosting

2.1. Hosting-Standort

Die reteach-Plattform wird auf Amazon Web Services (AWS) in der Region eu-central-1 (Frankfurt am Main, Deutschland) betrieben. Die Kerninfrastruktur – Datenbank, Datei-Speicher und Videoauslieferung – liegt vollständig in der EU. Im Regelbetrieb verarbeiten sämtliche Unterauftragnehmer ausschließlich in der EU; ein Drittlandtransfer findet nicht statt. Eine Verarbeitung außerhalb der EU ist nur möglich, wenn der Kunde ein optionales Modul oder eine optionale Funktion nutzt (siehe Abschnitt 9). AWS Frankfurt ist zertifiziert nach ISO 27001:2022, SOC 2 Type II, CSA STAR und PCI-DSS.

2.2. Mandantentrennung

Die reteach-Plattform setzt eine logische Mandantentrennung auf Anwendungs- und Datenbankebene um. Die Zugehörigkeit wird bereits bei der Authentifizierung aus dem verifizierten JWT-Token abgeleitet und auf Anwendungsebene konsequent durchgesetzt: Jede Datenbankabfrage wird automatisch um eine mandantenspezifische Filterbedingung ergänzt. Ergänzend sichern Fremdschlüssel-Constraints und mandantenbezogene Unique-Constraints auf Datenbankebene die referenzielle Integrität und verhindern Datenkollisionen zwischen Mandanten.

2.3. Applikationsarchitektur

Die reteach-Applikationen laufen containerisiert auf Kubernetes (AWS EKS). Die Applikationsschicht ist stateless, was eine schnelle Skalierung und Wiederherstellung ermöglicht. Der File-Storage wird über AWS S3 mit serverseitiger Verschlüsselung bereitgestellt.

3. Verschlüsselung

Data at Rest: Alle Datenbanken und Dateien werden serverseitig mit AES-256 über den AWS Key Management Service (SSE-KMS) verschlüsselt. Die Schlüsselverwaltung erfolgt über AWS KMS mit kontrolliertem Zugriff.

Data in Transit: Sämtliche Datenübertragungen zwischen Client und Server sowie zwischen internen Services erfolgen über TLS 1.2 oder höher. HTTPS wird für die Web-Applikation und alle API-Endpunkte erzwungen.

4. Zugriffskontrolle und Authentifizierung

Der Zugriff auf Kundendaten folgt dem Prinzip der geringsten Privilegien (Least Privilege) und dem Need-to-know-Prinzip:

- Multi-Faktor-Authentifizierung (MFA) ist für alle geschäftskritischen Systeme verpflichtend
- Der Zugriff auf Infrastruktur-Secrets ist rollenbasiert beschränkt und erfordert MFA
- Zugriffsrechte werden regelmäßig überprüft und bei Personalwechsel unverzüglich entzogen
- Ein verpflichtender Passwort-Manager wird für die Verwaltung aller Credentials eingesetzt
- Alle Firmengeräte werden über Mobile Device Management (MDM) zentral verwaltet
- Es werden ausschließlich Firmengeräte eingesetzt. BYOD ist nicht gestattet

5. Backup und Disaster Recovery

Parameter	Wert
Recovery Point Objective (RPO)	Unter 10 Minuten (Point-in-Time-Recovery)
Recovery Time Objective (RTO)	Unter 4 Stunden
Datenbank-Backup	Point-in-Time-Recovery für 7 Tage (minutengenau), danach tägliche Backups für 180 Tage (verschlüsselt auf AWS S3)
File-Storage-Backup	Versionierung aller Dateien für 180 Tage, einschließlich Änderungen und Löschungen
Recovery-Tests	Alle 90 Tage wird die vollständige Wiederherstellung aus Backup in einer Testumgebung verifiziert
Architektur-Vorteil	Applikationen sind stateless und können innerhalb von Minuten neu deployt werden

6. Incident Response und Benachrichtigung

Susell GmbH verfügt über einen formalen Incident-Response-Plan mit definierten Severity-Stufen und Reaktionszeiten:

Stufe	Bezeichnung	Erstreaktion	Kundeninfo
S1 Kritisch	Bestätigter Data Breach, Ransomware	Unter 30 Minuten	Unverzüglich, spätestens 48h ab Kenntnis
S2 Hoch	Verdacht auf Kompromittierung	Unter 4 Stunden	Nach Bestätigung
S3 Mittel	Schwachstelle ohne Ausnutzung	Unter 24 Stunden	Bei Bedarf
S4 Niedrig	Sicherheitsrelevante Beobachtung	Unter 72 Stunden	Nicht erforderlich

Bei einem Sicherheitsvorfall mit Auswirkungen auf Kundendaten benachrichtigt Susell GmbH betroffene Kunden unverzüglich, spätestens 48 Stunden ab eigener Kenntnis, damit diese ihre Meldepflicht nach Art. 33 DSGVO (72 Stunden) erfüllen können.

7. Softwareentwicklung und Qualitätssicherung

- Code Reviews: Alle Code-Änderungen werden durch mindestens zwei Engineers geprüft
- Dependency-Scanning: Automatisierte Prüfung eingesetzter Abhängigkeiten auf bekannte Schwachstellen (Dependabot)
- Container-Scanning: Automatisierte Prüfung von Container-Images (AWS ECR Scanning)
- Penetrationstests: Jährlich durch einen spezialisierten externen Dienstleister
- Patch-Management: Kritische Sicherheitsupdates innerhalb von 24 Stunden nach Bekanntwerden
- Monitoring: Kontinuierliche Überwachung (Datadog). Protokolldaten für 7 Tage gespeichert

8. Datenschutz und DSGVO-Konformität

Susell GmbH verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Kunden (Auftragsverarbeitung gem. Art. 28 DSGVO). Eine Vereinbarung zur Auftragsverarbeitung (AVV) wird mit jedem Kunden vor Beginn der Datenverarbeitung geschlossen.

Zentrale Datenschutz-Maßnahmen:

- Im Regelbetrieb der Plattform verarbeiten sämtliche Unterauftragnehmer ausschließlich in der EU; ein Drittlandtransfer findet nicht statt. Eine Verarbeitung in Drittländern ist nur bei Nutzung optionaler Module möglich (siehe Abschnitt 9)
- Vollständige Mandantentrennung auf Anwendungs- und Datenbankebene
- Verschlüsselung aller Daten at rest (AES-256) und in transit (TLS 1.2+)
- Formale Datenklassifikation (3 Stufen: Öffentlich, Intern, Vertraulich)
- Mitarbeitende sind vertraglich zur Vertraulichkeit verpflichtet

• Recht auf Löschung: Kundendaten werden nach Vertragsende auf Weisung gelöscht

9. Unterauftragnehmer

Abschnitt A – Regelbetrieb der Plattform. Die folgenden Unterauftragnehmer verarbeiten ausschließlich in der EU:

Dienstleister	Zweck	Standort	Zertifizierungen
Amazon Web Services	Cloud-Infrastruktur, Datenbank, File-Storage, E-Mail-Versand	Frankfurt am Main (eu-central-1)	ISO 27001:2022, SOC 2 Type II, CSA STAR, PCI-DSS
BunnyWay d.o.o. (Bunny)	Videohosting und CDN	Ljubljana, Slowenien (EU)	–
Streamdiver GmbH	Videoverarbeitung und -hosting	Österreich (EU)	ISO 27001 (RZ)
Datadog, Inc.	Betriebsüberwachung, Fehleranalyse	EU	ISO 27001, SOC 2 Type II
Mixpanel, Inc.	Produktanalytik (nur pseudonyme Nutzer-ID)	Eemshaven, NL (EU)	ISO 27001, SOC 2 Type II

Abschnitt B – Modulgebundene Unterauftragnehmer. Die folgenden Unterauftragnehmer werden nur eingesetzt, wenn der Kunde das jeweilige Modul oder die jeweilige Funktion nutzt:

Dienstleister	Zweck / Modul	Standort	Transfergrundlage
Kombo Technologies GmbH	HR-System-Integration (HRIS-Synchronisation)	Berlin (EU)	EU – kein Drittlandtransfer
Rustici Software, LLC	SCORM-Verarbeitung (nur bei SCORM)	Franklin, TN (USA)	DPF, hilfsweise SCC
Stripe, Inc.	Zahlungsabwicklung (eCommerce-Modul)	USA / EU	DPF, hilfsweise SCC
Phishing Tackle Limited	Phishing Awareness	Vereinigtes Königreich	Angemessenheitsbeschluss UK, hilfsweise SCC

Die nach AVV relevanten Unterauftragnehmer sind Teil der AVV (Anlage 2). Alle Änderungen werden Kunden vier Wochen im Voraus mitgeteilt.

Eigene Dienstleister (keine Unterauftragnehmer im AVV-Sinne): HubSpot (CRM und Marketing), Frisbii Germany GmbH, ehem. Billwerk+ (Abonnementverwaltung). Diese Dienste verarbeiten keine personenbezogenen Daten der Nutzer unserer Kunden.

10. Organisatorische Maßnahmen

- ISMS: orientiert sich an ISO 27001, jährliche Überprüfung durch die Geschäftsführung
- Schulung: bei Einstellung und danach jährlich, ergänzt durch laufende Phishing-Simulationen
- Zugangsrichtlinien: Remote-Arbeit, Endgerätesicherheit, Passwort-Management und KI-Nutzung
- Business Continuity: formaler Plan mit definierten RPO/RTO-Zielen
- Incident Response: formaler Plan mit Severity-Klassifikation und Eskalationswegen

11. Sicherheitsmaßnahmen im Überblick

Bereich	Maßnahme
Hosting & Standort	AWS eu-central-1 (Frankfurt). Im Regelbetrieb ausschließlich EU-Datenverarbeitung; Drittlandtransfer nur bei optionalen Modulen.
Verschlüsselung (at rest)	AES-256 über AWS KMS (SSE-KMS)
Verschlüsselung (in transit)	TLS 1.2+ für alle Übertragungen. HTTPS erzwungen.
Authentifizierung	MFA für alle kritischen Systeme und Administrationszugänge
Zugriffskontrolle	Need-to-know, Least Privilege. Rollenbasierte Beschränkung. Sofortige Deaktivierung bei

	Offboarding.
Backup & Recovery	PITR (RPO <10 Min). Tägliche Backups für 180 Tage. Recovery-Tests alle 90 Tage.
Incident Response	S1–S4. Erstreaktion S1: <30 Min. Kundenbenachrichtigung: spätestens 48h ab Kenntnis.
Endgerätesicherheit	Nur Firmengeräte, MDM, Festplattenverschlüsselung, Endpoint Protection.
Softwareentwicklung	Code Reviews (4-Augen), Dependabot, Container-Scanning, jährliche Pentests.
Passwort-Management	Keeper verpflichtend. 16 Zeichen Mindestlänge.
Mitarbeiterschulung	Bei Einstellung + jährlich. Laufende Phishing-Simulationen.