IT-Sicherheitskonzept

Vorwort

Dieses IT-Sicherheitskonzept ist Grundlage für den Einsatz von IT-Systemen bei Evermood.

Das IT-Sicherheitskonzept dient der Optimierung der Informationssicherheit in unserem Unternehmen und soll dazu beitragen, bestehende und künftige Prozesse weiter im Hinblick auf eine sichere Verarbeitung der Daten zu optimieren.

IT-Sicherheit stellt einen Teil der Informationssicherheit dar. Sie umfasst die Sicherheit von IT-Systemen, Netzen und Anwendungen sowie der darin gespeicherten Daten durch Realisierung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Schutzziele der IT-Sicherheit (Vertraulichkeit, Verfügbarkeit und Integrität).

Alle Beschäftigten sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten bzw. darüber zu unterrichten. Sie und sonstige relevante Personen (extern Beschäftigte und Kooperationspartner) werden systematisch und zielgruppengerecht zu Datenschutzfragen sensibilisiert und zum Umgang mit personenbezogenen Daten geschult.

Es sind technisch-organisatorische Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO zu entwickeln, um die Sicherheit der Verarbeitung der Daten sowie die Durchsetzung der Rechte der Betroffenen (Auskunft, Berichtigung, Einschränkung der Bearbeitung, Löschung sowie Mitteilungs- und Benachrichtigungspflichten) zu gewährleisten, und der Rechenschaftspflicht nachkommen zu können.

Dieses Dokument muss regelmäßig fortgeschrieben und mit der/dem zuständigen IT-Sicherheitsbeauftragten abgestimmt werden. Die Checkliste wird mindestens einmal im Jahr überprüft und ggf. angepasst.

Folgende Rahmenbedingungen sollen stets gewährleistet werden:

- Die Verfügbarkeit der Systeme (z. B. Schutz vor Diebstahl, Zerstörung, Ausfallzeiten, Verlust von Datenträgern),
- die Integrität der Software und der Daten (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen, Manipulation von Dateien),
- die Vertraulichkeit von Daten (z. B. Schutz vor unbefugter Kenntnisnahme von Dateiinhalten).

Das Sicherheitsniveau bezieht sich auf alle im Unternehmen eingesetzten technischen Systeme und Verfahrensabläufe, mit deren Hilfe personenbezogene Informationen oder Informationen zu Betriebs- und Geschäftsgeheimnissen gespeichert und weiterverarbeitet werden können.

In diesem Sicherheitskonzept werden zunächst die Räume, IT-Systeme und IT- Anwendungen (sowie ein Netzplan) aufgeführt. Diese stellen die im Unternehmen verwendeten technischen Einrichtungen dar, welche Grundlage zur Ermittlung der Schutzgegenstände, Schwachstellen und Risiken sowie zur Beschreibung der erforderlichen technischen und organisatorische Maßnahmen zum Schutz der Daten sind.

1. Bestandsanalyse

1.1. Übersicht: Räume

Grundsätzlich haben nur Mitarbeitende Zugang zu den Räumlichkeiten von Evermood. Sollten Kunden oder anderen Personen (Externe) in Ausnahmefällen Zugang zu den Räumlichkeiten erhalten, so ist der Aufenthalt der Personen zu dokumentieren und von der Person zu bestätigen.

Externe haben die Möglichkeit über WLAN auf das Internet zuzugreifen (Gast-Zugang). Ein Zugriff auf das interne Netzwerk wird durch Zugangsbeschränkungen ausgeschlossen.

Die Räume werden anhand ihrer ID, Art und Bereich nachfolgend aufgelistet:

R 1.01: Flur (Eingangsbereich)

Im Flur werden keine Datenträger oder Unterlagen mit personenbezogenen Daten aufbewahrt. Externe haben Zugang zu diesem Bereich.

R 1.02: Kleiner Besprechungsraum [Stage] (Vertraulicher Bereich)

Während Besprechungen ist die Tür zum Besprechungsraum aus Vertraulichkeitsgründen stets geschlossen zu halten.

Kundenbezogene Unterlagen sind beim Betreten und Verlassen des Raums mitzuführen.

R 1.03: Aufenthaltsraum [Library] (Öffentlicher Bereich)

Im Aufenthaltsraum werden keine Datenträger oder Unterlagen mit personenbezogenen Daten aufbewahrt.

Externe haben Zugang zu diesem Bereich.

R 1.04: Großer Besprechungsraum [Parliament] (Öffentlicher Bereich)

Während Besprechungen ist die Tür zum Besprechungsraum aus Vertraulichkeitsgründen stets geschlossen zu halten.

Externe haben Zugang zu diesem Bereich.

Kundenbezogene Unterlagen sind beim Betreten und Verlassen des Raums mitzuführen.

R 1.05: Büroraum 1 [Base Camp] (Vertraulicher Bereich)

Dieser Raum steht vor allem den Mitarbeitenden zur Verfügung.

Unterlagen, die aktiv (d.h. nicht archiviert sind) dürfen hier grundsätzlich nur vorübergehend aufbewahrt werden.

Externe haben keinen Zugang zu diesem Bereich.

R 1.06: Küche (Öffentlicher Bereich)

Externe haben Zutritt zu diesem Bereich.

R 1.07: Toiletten (Öffentlicher Bereich)

Die Toiletten dürfen auch durch Externe genutzt werden.

R 1.08: Abstellraum (Vertraulicher Bereich)

Externe haben keinen Zugang zu diesem Bereich. Der Raum muss so weit möglich verschlossen bleiben.

1.2. Übersicht: IT-Systeme

Die IT-Systeme werden anhand ihrer ID, Art und Benennung nachfolgend aufgelistet und anhand der Grundwerte (Vertraulichkeit, Integrität und Verfügbarkeit) eingeordnet:

S1: GSuite		
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	hoch	Sämtliche Daten des Unternehmens sind hier gespeichert.
Integrität	hoch	Sämtliche Daten des Unternehmens sind hier gespeichert.

Verfügbarkeit	hoch	Ohne Zugriff zu der GSuite ist die tägliche Arbeit nicht möglich.

S2: AWS (Amazon Web Services)		
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	hoch	Sämtliche Daten der Anwendung sind hier gespeichert. Personenbezogene Daten von Nutzern sind hier gespeichert.
Integrität	hoch	Sämtliche Daten der Anwendung sind hier gespeichert. Personenbezogene Daten von Nutzern sind hier gespeichert.
Verfügbarkeit	hoch	Ohne Zugriff zu AWS ist die Anwendung nicht verfügbar.

MBx: MacBook Pro 13 Zoll (mehrere), MacOS		
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	hoch	Auf dem MacBook werden Daten von Kunden und von dem Unternehmen gespeichert (nur in Ausnahmefällen). Über das MacBook kann Zugriff auf sensible Daten mit Login-Daten für diverse Anwendungen erfolgen. Das MacBook ist durch ein Passwort zu sichern. Eine Aufbewahrung in einem unbewachten Kfz ist nicht zulässig. Wenn das MacBook unbeaufsichtigt ist, ist der Bildschirm zu sperren, so dass er nur durch Passwort-Eingabe wieder aktiviert werden kann.
Integrität	mittel	Standort: Mobil Die Datenhaltung erfolgt auf dem MacBook. Daten sind jedoch grundsätzlich in der GSuite zu speichern.
Verfügbarkeit	mittel	Ein Ausfall kann durch andere Geräte überbrückt werden.

Mx: Mobile Geräte (iPads und iPhones)		
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	hoch	Auf den Endgeräten werden Kundendaten (Mails, Termine, Adressen) gespeichert. Die Geräte sind durch eine PIN zu sichern.
Integrität	mittel	Standort: Mobil Die Datenhaltung erfolgt auf den Endgeräten. Daten sind jedoch grundsätzlich in der GSuite zu speichern.

Verfügbarkeit	mittel	Ein Ausfall kann durch andere Geräte überbrückt werden.

U1: UBIQUITI Gigabit Port Switch		
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	niedrig	Keine Daten werden auf dem Switch gespeichert.
Integrität	niedrig	Standort: R 1.04 Keine Daten werden auf dem Switch gespeichert.
Verfügbarkeit	hoch	Ohne ein funktionsfähiges Netzwerk ist der Betrieb des Unternehmens nur eingeschränkt möglich.

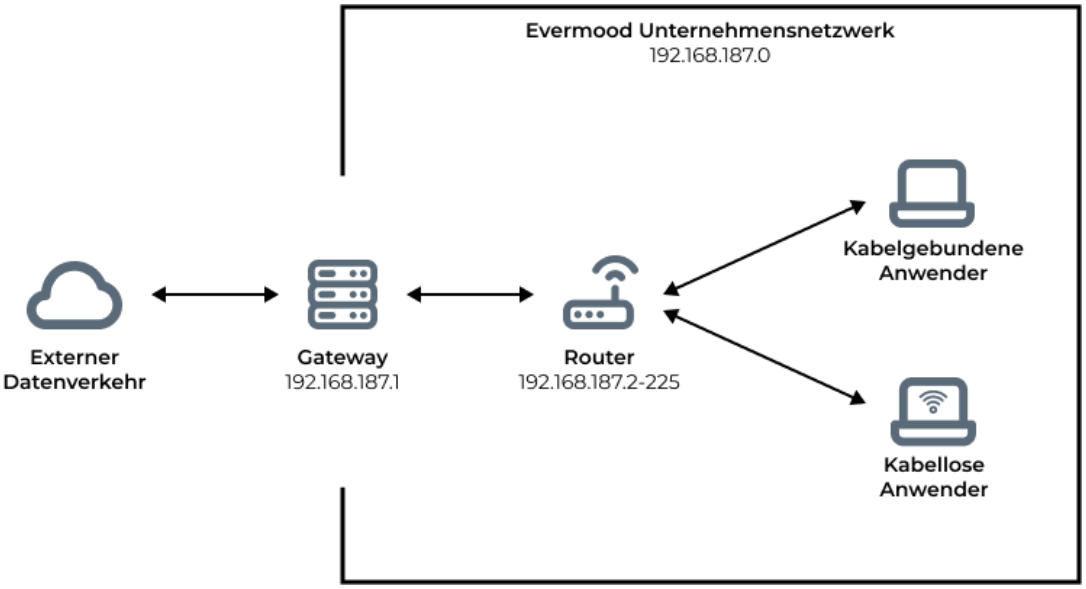
N1: Fritzbox WLAN/ DSL Router		
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	niedrig	Die Zugangsdaten des Unternehmens sind auf dem Router gespeichert. Der Router ist die Verbindung zum Internet.
Integrität	niedrig	Standort: R 1.04 Die Zugangsdaten des Unternehmens sind auf dem Router gespeichert. Der Router ist die Verbindung zum Internet.
Verfügbarkeit	hoch	Ohne ein funktionsfähiges Netzwerk ist der Betrieb des Unternehmens nur eingeschränkt möglich.

1.3. Übersicht: IT-Anwendungen

Nr.	Bezeichnung	Zwecke
A1	Slack	Interner Kommunikationskanal des Unternehmens
A2	Notion	Dokumentation und Unternehmens-Wiki der Unternehmensprozesse
A3	ClickUp	Aufgaben- & Team-Management
A4	Figma	Erstellung von Skizzen und Layouts der Softwarelösung
A5	CircleCI	Feedback Anwendung für Figma
A6	AppSignal	Ressourcenverwaltung der Komponenten der Softwarelösung
A7	Github	Code-Management der Softwarelösung

A8	Sentry	Fehler-Management der Softwarelösung
A9	Zoom	Videokonferenzen mit Kunden
A10	Google Hangouts	Videokonferenzen mit Kunden

1.4. Übersicht: Netzwerkplan



2. Schwachstellen-/Risikoanalyse & Maßnahmen

Die Schwachstellen- & Risikoanalyse erfolgt zusammen mit der Benennung der jeweiligen Maßnahme zur Risikominimierung. Die Risiken werden jeweils in Frageform gestellt:

Sind die Nutzer (einschließlich der Vertreter) von IT-Systemen aufgabenspezifisch geschult?

Alle Mitarbeitenden erhalten nach ihrer Einstellung eine Einweisung in die verwendeten IT- Systeme und Anwendungen, soweit deren Anwendung (wie z.B. bei Standard-Software) nicht als bekannt unterstellt werden kann. Für die Bedienung der Fachanwendungen werden Mitarbeitende eine Einweisung von einem/einer MentorIn erhalten. Die wichtigsten systemspezifischen Aufgaben inkl. Hinweise zur Durchführung sind im betriebsinternen Unternehmens-Wiki dokumentiert.

Sind Hard- und Software inventarisiert und im Geräteverzeichnis aufgenommen?

Neben einer Dokumentation der Hardware in der Anlagenbuchhaltung gibt es eine Übersicht über alle IT-Arbeitsplätze sowie die obenstehenden Übersichten in dieser Datei über IT-Systeme und Anwendungen. Diese Aufzeichnungen werden durch den Datenschutzbeauftragten geführt und regelmäßig aktualisiert.

Werden bei Abwesenheit der Benutzer die Räume verschlossen?

Alle Mitarbeitenden sind über die IT-Richtlinie dazu verpflichtet, die Unternehmensräume nach dem Verlassen des letzten Mitarbeitenden zu verschließen. Alle Mitarbeitenden müssen sich beim Verlassen ihres Arbeitsplatzes von ihren Rechnern abmelden und den Rechner ausschalten. Die Unternehmensräume können nur mittels eines digitalen Transpondersystems geöffnet und verschlossen werden, sodass der Zutritt aller Mitarbeitenden dokumentiert wird.

Werden die Programme einschließlich der Betriebssysteme und der systemnahen Software sowie die Datenbestände regelmäßig gesichert?

Die Datenspeicherung erfolgt überwiegend in der GSuite und/oder AWS. Vorübergehend gespeicherte Daten (z.B. auf dem Desktop der Mitarbeitenden) sind am Ende eines jeden Arbeitstages in die jeweilige Cloud-Anwendung zu überführen.

Daten in der GSuite bzw. AWS werden täglich durch Backups geschützt und zum Schutz vor Vernichtung automatisch in mehreren Datenzentren archiviert.

Wird bei mobilen Geräten, die für dienstliche Zwecke außerhalb der Geschäftsräume eingesetzt werden, eine Dateiverschlüsselung eingesetzt?

Alle Laptops werden mit FileVault, der vorinstallierten Festplattenverschlüsselung von Apple verschlüsselt und durch Passwort und/oder PIN gesichert. Da die Mitarbeitenden in der Regel nur über die GSuite bzw. AWS auf personenbezogene Daten zugreifen, ist der Umfang der Daten auf den mobilen Clients auf ein Minimum beschränkt (in der Regel E-Mails, Termine und Adressen).

Wird Software vor deren Einsatz genehmigt bzw. freigegeben?

Neue Software wird nur nach Freigabe durch die Geschäftsführung eingesetzt.

Kann die Benutzung des IT-Systems nur nach Eingabe einer individuellen Nutzerkennung und der Authentifizierung durch ein Passwort erfolgen?

Jedes IT-System ist erst nach Eingabe eines Benutzernamens mit dem dazugehörigen Passwort nutzbar. Ein Zugriff auf personenbezogene Daten ohne vorherige Authentifizierung ist nicht möglich. Soweit möglich ist eine Zwei-Faktor Authentifizierung zu verwenden.

Für die Anwendungen, in der personenbezogene Daten gespeichert werden, ist ebenfalls eine weitere Anmeldung mit einem separaten Benutzernamen und einem separaten Passwort notwendig. Alle Mitarbeitenden sind verpflichtet, nicht das initiale Standard-Passwort zu verwenden (Änderung bei der ersten Anmeldung). Die Mitarbeitenden dürfen ihr Passwort nicht an Kollegen weitergeben.

Für bestimmte Fachanwendungen (bspw. Vollmachtsdatenbank) ist aus Sicherheitsgründen nur ein unternehmensweit gültiger Nutzer und ein unternehmensweit gültiges Passwort möglich.

Werden die Funktionen der Benutzer von IT-Systemen und der IT-Administratoren getrennt?

Die zum Einsatz kommenden Systeme, mit denen auch die Nutzerberechtigungen umgesetzt werden, trennen Nutzer und Administratoren.

Sind Vertreter des IT-Administrators in ausreichender Zahl vorhanden?

Derzeit sind zwei Administratoren im Einsatz (1 x CEO, 1 x CTO). Im Falle eines z.B. krankheits- oder urlaubsbedingten Ausfalls ist ein ordnungsgemäßer Betrieb der IT-Systeme dennoch gewährleistet.

Werden Systemaktivitäten nachvollziehbar protokolliert?

Das Server-Betriebssystem protokolliert alle Änderungen an Richtlinien im Verzeichnisdienst, das Anlegen, Ändern und Löschen von Benutzern sowie die Änderung von Berechtigungen.

Sind die Zugriffsberechtigungen auf die Anwendungssoftware so weit wie möglich differenziert?

Das Berechtigungskonzept für Anwendungen sieht grundsätzlich vor, dass jeder Nutzer nur die Rechte erhält, die er zur Erfüllung seiner Aufgaben benötigt. Zeigt sich, dass Berechtigungen nicht ausreichend sind, können entsprechende Rechte zusätzlich im Rahmen der Erforderlichkeit eingeräumt werden.

Besteht eine Dokumentation der Benutzer- und Rechteverwaltung?

Die Benutzerrechte sind im Server-Betriebssystem bzw. dem Verzeichnisdienst und in den Administrationstabellen dokumentiert und können jederzeit ausgedruckt werden.

Sind IT-Systeme so platziert, dass eine unbefugte Kenntnisnahme von dargestellten oder ausgedruckten Informationen (z. B. durch Besucher oder sonstige Nichtbeteiligte) ausgeschlossen wird?

Die Mitarbeitenden sind durch die IT-Richtlinie angewiesen, ihre Arbeitsplätze so zu gestalten, dass Externe nicht unbefugt Kenntnis von personenbezogenen Daten erhalten können.

Dies wird insbesondere dadurch sichergestellt, dass die Räumlichkeiten des Unternehmens in einen öffentlichen und einen vertraulichen Bereich unterteilt sind. Externe haben keinen Zutritt zum vertraulichen Bereich. Im öffentlichen Bereich dürfen keine vertraulichen Unterlagen mit Zugriffsmöglichkeit für Dritte aufbewahrt werden (siehe Räumlichkeiten).

Werden die Tätigkeiten von Dienstleistern (Installation, Wartung, Servicetechniker) beaufsichtigt und protokolliert?

Jede Wartung von IT-Systemen wird durch mindestens einen Mitarbeitenden überwacht.

Sind die Zutrittsberechtigungen zum Serverraum geregelt?

Es existiert kein Serverraum in den Räumlichkeiten des Unternehmens.

Werden die Daten der Fachverfahren ausschließlich auf den zentralen IT-Systemen gespeichert?

Die lokale Speicherung von personenbezogenen Daten ist zu vermeiden.

3. Auftragsverarbeitung von Daten

Die Auftragsverarbeitung von Daten ist in unserem Auftragsverarbeitungs-Vertrag (AVV) geregelt.

4. Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen sind Teil unseres AVVs.

5. Notfallplan

Falls es zu Notfällen kommt, die die Funktionsfähigkeit der IT-Systeme beeinträchtigen, kommt ein Notfallplan zur Anwendung. Im Notfallplan ist eine Notfalldefinition, eine Angabe der Verantwortlichen, die Benachrichtigungen sowie die Notfallmaßnahmen definiert.

Der Notfallplan ist im Unternehmens-Wiki dokumentiert. Eine ausgedruckte Version liegt in den Räumlichkeiten des Unternehmens vor.

6. Geltung, Evaluierung & Anpassung dieses IT-Sicherheitskonzepts

Das Sicherheitskonzept ist bei jeder Änderung der aktuellen örtlichen und personellen Gegebenheiten und aus sonstigen Anlässen, die Auswirkungen auf das Sicherheitskonzept haben, fortzuschreiben und spätestens nach einem Jahr zu überprüfen.

Stand: Februar 2020