

# Inhaltsverzeichnis

- 1. Über das Verfahren ..... 2
  - 1.1. Sicherheitsprinzipien ..... 2
  - 1.2. Grundsatzaussagen ..... 2
  - 1.3. Ziel und Zweck ..... 2
  - 1.4. Geltungsbereich ..... 2
  
- 2. Allgemeines Managementsystem für Informationssicherheit (ISMS) ..... 3
  - 2.1. Vertragliche Anforderungen ..... 3
  - 2.2. Aufbau des ISMS ..... 3
  - 2.3. Einhaltung der Informationssicherheitsrichtlinien (Compliance) ..... 3
  - 2.4. Unterstützung und Schulung ..... 3
  - 2.5. Durchsetzung ..... 4
  - 2.6. Ausnahmen ..... 4
  
- 3. Informationsklassifizierung ..... 5
  - 3.1. Kennzeichnung von Informationen ..... 5
  - 3.2. Umgang mit Informationen ..... 6
  
- 4. Sicherheitskontrollmaßnahmen ..... 8
  - 4.1. Zutrittskontrolle ..... 8
  - 4.2. Zugangskontrolle ..... 8
  - 4.3. Trennungskontrolle ..... 9
  - 4.4. Datenträgerkontrolle ..... 9
  - 4.5. Transportkontrolle ..... 9
  - 4.6. Systemsicherheit ..... 9
  - 4.7. Gewährleistung der Verfügbarkeit ..... 10
  - 4.8. Sicherheitsvorfälle ..... 10
  
- 5. Anhang – Änderungshistorie ..... 11

Erstellung	Genehmigung	Datum
B. Schmalfuß	J. Lange	28.03.2024

# 1. Über das Verfahren

Es ist das Sicherheitsziel der Umfotec, dass Informationen aller Art - geschrieben, gesprochen, elektronisch erfasst oder gedruckt - gegen zufällige oder vorsätzliche unbefugte Änderung, Zerstörung oder Offenlegung über den gesamten Lebenszyklus geschützt werden. Die Schutzmaßnahmen für die Systeme und Programme, mit denen diese Informationen verarbeitet, übertragen und gespeichert werden müssen einem angemessenen Schutzniveau entsprechen.

## 1.1. Sicherheitsprinzipien

- Unsere Geschäftsprozesse und Informationen sind schützenswert.
- Unsere Sicherheitsmaßnahmen werden die Risiken für das Unternehmen reduzieren.
- Unsere Sicherheitsmaßnahmen entsprechen dem Industriestandard.
- Jeder Einzelne ist in seinem Bereich verantwortlich für die Sicherheit unserer Informationen, Anlagen und Systeme.
- Wir werden eine klare Trennung der Verantwortlichkeiten implementieren, um Interessenskonflikte zu vermeiden.
- Wir werden alle rechtlichen und regulatorischen Anforderungen einhalten.
- Wir werden sicherstellen, dass die Sicherheitsanforderungen den sich ändernden Geschäftsanforderungen angepasst werden

## 1.2. Grundsatzaussagen

Die Durchsetzung der Informationssicherheitsrichtlinien darf nur unter Beachtung der Mitbestimmungsrechte der nationalen Arbeitnehmervertretungen, sowie der Vorschriften der geltenden Betriebsvereinbarungen und örtlichen Gesetze (z. Bsp. Datenschutzgesetze) erfolgen.

## 1.3. Ziel und Zweck

Der Zweck dieser Informationssicherheitsrichtlinie ist die Gewährleistung der Geschäftskontinuität und die Schadensreduktion bei der Zusammenarbeit mit Drittfirmen (Lieferanten, Dienstleister sowie Geschäftspartner, usw.) durch die Verhinderung oder Minimierung von Sicherheitsvorfällen.

Diese Informationssicherheitsrichtlinie ermöglicht die Benutzung von Umfotec-Informationen im externen Unternehmen unter Beachtung von:

- Vertraulichkeit
- Integrität und
- Verfügbarkeit

Mit dieser Sicherheitsrichtlinie bringt die Geschäftsleitung die Wichtigkeit der Sicherheit der Informationen und der Informationssysteme für Umfotec und für die Zusammenarbeit mit Drittfirmen zum Ausdruck.

## 1.4. Geltungsbereich

Diese Umfotec-Informationssicherheitsrichtlinie ist als "öffentliche" Information klassifiziert und wird folgenden Personenkreisen zur Verfügung gestellt:

- Lieferanten, Geschäftspartner, Dienstleister
- Geschäftskunden und Endkunden
- Vertragsnehmer, Beratern, Zeit- und Aushilfskräften
- sowie Agenturbüros, Franchisenehmer usw.

Weitere Richtlinien oder Standards können je nach Anwendungsfall mit Unterstützung des Umfotec ISMS-Teams ebenfalls einbezogen werden

Erstellung	Genehmigung	Datum
B. Schmalfuß	J. Lange	28.03.2024

## 2. Allgemeines Managementsystem für Informationssicherheit (ISMS)

### 2.1. Vertragliche Anforderungen

Wenn eine Drittfirma auf sensible Umfotec-Daten zugreifen kann oder ihr sensible Umfotec-Daten zur Verfügung gestellt werden, muss eine Geheimhaltungsvereinbarung (GHV) in den Vertrag aufgenommen werden, welche für alle Mitarbeiter der Drittfirma gilt. Dadurch wird die Vertraulichkeit der Umfotec-Daten sichergestellt.

Auch nach der Beendigung der Dienstleistung bzw. der Zusammenarbeit ist über die erlangten Informationen Stillschweigen zu vereinbaren. Dies gilt auch für die Beendigung des Arbeitsverhältnisses einer Person, welche bei einer Drittfirma eingestellt war und von diesem bei der Umfotec eingesetzt wurde

Stellt eine Drittfirma Subunternehmer für die Erbringung der Leistung ein, die mit der Umfotec vereinbart wurde, so muss dies vor Beauftragung des Subunternehmers der Umfotec gemeldet werden. Darüber hinaus muss von den durch die Umfotec beauftragten Drittfirmen (z.B. Lieferanten) sichergestellt sein, dass die Subunternehmer über die Vertragsbedingungen des Lieferanten mit der Umfotec in Kenntnis gesetzt sind und diese sich auch auf diese Bedingungen verpflichten. Damit soll erreicht werden, die Sicherheit und den Schutz der informationstechnischen Systeme sowie der in ihnen gespeicherten Daten bei der Umfotec zu gewährleisten. Die Subunternehmer müssen daher vom Lieferanten bzw. Drittfirmen auch auf die GHV der Umfotec verpflichtet werden.

### 2.2. Aufbau des ISMS

Umfotec erwartet, dass die vertraglich verbundenen Drittfirmen im Umfeld der Informationsverarbeitung von Umfotec-Daten ein Management der Informationssicherheit ausgerichtet an ISO 27001 oder TISAX Standard haben. Mit diesen Informationssicherheits-Standards wird ein risikobasierter Ansatz umgesetzt, um eine gründliche Analyse aller Informationen und informationsverarbeitenden Systeme in regelmäßigen Abständen durchzuführen. Dadurch werden die Bedrohungen und Schwachstellen für übertragene und gespeicherte Informationen anerkannt und rechtzeitig mit weiteren Sicherheitsmaßnahmen behandelt, um einen optimalen Sicherheitsniveau in der Organisation sicherzustellen.

### 2.3. Einhaltung der Informationssicherheitsrichtlinien (Compliance)

In jeder vertraglich verbundenen Drittfirma ist diese Informationssicherheitsrichtlinie einzuhalten.


Stellt eine Drittfirma einen Subunternehmer für die Erbringung einer Software- oder Hardwareleistung ein, so hat die Drittfirma, welcher mit der Umfotec in einem Vertragsverhältnis steht, dafür Sorge zu tragen, dass sich der Subunternehmer auch auf die Einhaltung der Informationssicherheitsrichtlinien der Umfotec verpflichtet.

Die Umfotec behält es sich vor, im Rahmen der vertraglichen Vereinbarungen und der vereinbarten allgemeinen Geschäftsbedingungen Mitarbeiter der Drittfirmen sowie Drittfirmen auf die Einhaltung der GHV zu prüfen. Zusätzlich werden auch ggfs. vorhandene Zertifikate im Umfeld der Informationssicherheit abgefragt.

### 2.4. Unterstützung und Schulung

Die Umfotec Informationssicherheit und die IT-Abteilung können die Drittfirmen durch zielorientierte Schulungen unterstützen. Die grundlegenden Anforderungen an Informationssicherheit werden durch diese Informationssicherheitsrichtlinie mitgeteilt.

Erstellung	Genehmigung	Datum
B. Schmalfuß	J. Lange	28.03.2024

<b>ST06_001_Rev01</b>	<b>Informationssicherheit bei UMFOTEC</b>	
<b>Public</b> <i>öffentlich</i>		

## 2.5. Durchsetzung

Die Nichteinhaltung der Umfotec Informationssicherheitsrichtlinien und -standards oder die Missachtung angemessener Maßnahmen zum Schutz der Systeme, Daten, Informationen und Vermögenswerte kann zu rechtlichen Schritten führen.

## 2.6. Ausnahmen

Ausnahmen oder Abweichungen zu dieser Informationssicherheitsrichtlinie müssen dokumentiert, begründet und seitens der Umfotec-Geschäftsleitung freigegeben werden. Der detaillierte Ausnahmebehandlungs-Prozess ist bei der Umfotec Informationssicherheit nachzufragen. Die Kontaktdaten finden Sie in Kapitel 4.8

Erstellung	Genehmigung	Datum
B. Schmalfuß	J. Lange	28.03.2024

### 3. Informationsklassifizierung

Eine Klassifikation wird zur Gewährleistung angemessener Schutzmaßnahmen für vertrauliche Informationen eingesetzt. Unabhängig von der Klassifizierung müssen auch die Integrität und die Richtigkeit der Informationsklassifikation geschützt werden. Die zugewiesene Klassifikation und die damit verbundenen Maßnahmen müssen in Abhängigkeit von der Sensibilität der Informationen umgesetzt werden. Die sensibelsten Elemente der Information definieren den Klassifikationsgrad. Informationen, die in verschiedenen Formaten aufgezeichnet wurden (z. Bsp. gedruckte Dokumente, elektronische Sprachaufzeichnungen, elektronische Berichte), müssen unabhängig von ihrem Format die gleiche Klassifizierung haben.

Die anzuwendenden Klassifizierungsstufen sind:

Klassifikation	Potenzielle Schaden durch unautorisierte Bekanntgabe, Änderungen oder Vernichtung	Zugangsbeschränkung
Öffentlich	Zugang zu diesen Informationen beeinträchtigt das Unternehmen keinesfalls.	Informationen sind öffentlich zugänglich.
Intern	Zugang durch Dritte oder nicht vertrauenswürdige Vertragspartner kann einen geringen Schaden oder Ansehensverlust zur Folge haben.	Informationen sind allen Mitarbeitern und, wenn nötig, Vertragspartnern (mit GHV) zugänglich.
Vertraulich	Zugang zu Informationen durch Dritte oder unberechtigte Mitarbeiter kann einen erheblichen Schaden zur Folge haben.	Informationen sind nur dem vom Eigentümer festgelegten Empfängerkreis zugänglich, dieser kann auch Vertragspartner mit unterzeichneter Geheimhaltungsvereinbarung enthalten.
Streng vertraulich	Das Schadenspotenzial ist existenzbedrohend, langfristig oder nicht auf ein einzelnes Unternehmen beschränkt.	Nur namentlich genannte Personen, eingeschränkte Nutzung

#### 3.1. Kennzeichnung von Informationen

Die ordnungsgemäße Kennzeichnung ist eine Voraussetzung für den sicheren Umgang mit Informationen. Informationen sollten daher entsprechend ihrer Vertraulichkeitseinstufung gekennzeichnet werden.

Neben dem Dokumentbesitzer müssen sowohl der Empfänger als auch der Verarbeiter der Information mit den Klassifizierungsstufen vertraut sein und daher die damit verbundenen Anforderungen an den Umgang mit der Information kennen und anwenden.

Eine korrekte Kennzeichnung ist insbesondere bei der Übermittlung vertraulicher oder streng vertraulicher Informationen zwischen Unternehmen (z. B. an Partnerfirmen und Lieferanten) unbedingt erforderlich. Bei der Kennzeichnung von Informationen müssen die Form der Information und ihr Geheimhaltungsgrad berücksichtigt werden.

Wenn Informationen nicht gekennzeichnet sind und die Klassifizierung nicht offensichtlich ist, müssen sie als "intern" betrachtet werden.

### 3.2. Umgang mit Informationen

Klassifikation	Kennzeichnung	Data at rest*	Data in transit*	Vernichtung
Öffentlich	Angabe der Vertraulichkeitsstufe in englisch / deutsch „Public“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form.	<u>Elektronische Daten:</u> keine Einschränkungen  <u>Papierunterlagen:</u> keine Einschränkungen	<u>Elektronische Daten:</u> keine Einschränkungen  <u>Papierunterlagen:</u> keine Einschränkungen	<u>Elektronisch:</u> keine Einschränkungen  <u>Physisch:</u> keine Einschränkungen
Intern	Keine / optional Angabe der Vertraulichkeitsstufe in englisch / deutsch, keine oder „Internal“ auf der ersten Seite des Dokuments	<u>Elektronische Daten:</u> Zugriff auf externe Server eingeschränkt  <u>Papierunterlagen:</u> Sollte bei Nichtgebrauch in verschlossenen Schränken/Containern gelagert werden	<u>Elektronische Daten:</u> Verschlüsselung auf externen Servern  <u>Papierunterlagen:</u> Äußerer Transport nur in verschlossenen Umschlägen	<u>Elektronisch:</u> Sicheres Löschen durch Überschreiben von Medien mit mindestens einem Schreibdurchgang mit einem festen Datenwert, z. B. nur Nullen. ODER Nutzung von, durch Sicherheitsteam freigegebenes Entmagnetisierungsgerät für die magnetische Speicherung (in Anlehnung an NIST SP 800-88 Rev. 1)  <u>Physisch:</u> Vernichtung nach ISO 21964 (DIN 66399), mind. Schutzklasse 1 Sicherheitsstufe 2
Vertraulich	Angabe der Vertraulichkeitsstufe in englisch / deutsch, „Confidential“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form.	<u>Elektronische Daten:</u> grundsätzlich zugriffsbeschränkt  <u>Papierunterlagen:</u> Eingeschlossen, wenn sie nicht direkt benutzt werden und nicht beaufsichtigt werden, nicht an öffentlichen Orten nutzen	<u>Elektronische Daten:</u> immer verschlüsselt  <u>Papierunterlagen:</u> Nur in entsprechend verschlossenen Umschlägen	<u>Elektronisch:</u> Sicheres Löschen durch Überschreiben von Medien mit mindestens einem Schreibdurchgang mit einem festen Datenwert, z. B. nur Nullen. ODER Nutzung von, durch Sicherheitsteam freigegebenes Entmagnetisierungsgerät für die magnetische Speicherung (in Anlehnung an NIST SP 800-88 Rev. 1)  <u>Physisch:</u> Vernichtung nach ISO 21964 (DIN 66399), mind. Schutzklasse 2 Sicherheitsstufe 4

<b>Streng vertraulich</b>	Angabe der Vertraulichkeitsstufe in englisch / deutsch, „Strictly Confidential“ auf jeder Seite des Dokuments	<p><u>Elektronische Daten:</u>          grundsätzlich Zugriffsbeschränkt, individuell verschlüsselte Dateien, Nachrichten oder Datenbanken, Speicherung auf physisch unsicheren Geräten (Cloud, mobile Datenspeicherung, Laptop, Telefon) nur mit expliziter Freigabe</p> <p><u>Papierunterlagen:</u>          Eingeschlossen, wenn sie nicht direkt benutzt werden und nicht beaufsichtigt werden, Standort eingeschränkt, nicht an öffentlichen Orten zu benutzen</p>	<p><u>Elektronische Daten:</u>          Ende-zu-Ende-Verschlüsselung</p> <p><u>Papierunterlagen:</u>          Nur Sonderkurierdienst</p>	<p><u>Elektronisch:</u>          Sicheres Löschen durch Überschreiben von Medien mit mindestens einem Schreiddurchgang mit einem festen Datenwert, z. B. nur Nullen. ODER Nutzung von, durch Sicherheitsteam freigegebenes Entmagnetisierungsgerät für die magnetische Speicherung (in Anlehnung an NIST SP 800-88 Rev. 1)</p> <p><u>Physisch:</u>          Vernichtung nach ISO 21964 (DIN 66399), mind. Schutzklasse 3          Sicherheitsstufe 5</p>
---------------------------	---	---	--	--

\*Ausnahmen möglich mit unterschriebener Risikoakzeptanz von Business Owner

Erstellung	Genehmigung	Datum
B. Schmalfuß	J. Lange	28.03.2024

Änderungshistorie im Anhang

## 4. Sicherheitskontrollmaßnahmen

Der physische und logische Zugriff auf vertrauliche und interne Informations- und Datenverarbeitungssysteme wird kontrolliert. Um einen angemessenen Zugriffslevel sicherzustellen, werden vom zuständigen Informationssicherheitsbeauftragten verschiedene Sicherheitsmaßnahmen vorgegeben.

### 4.1. Zutrittskontrolle

Alle externen Organisationen, die UMFOTEC-Gebäude betreten, werden mit einem Ausweis ordnungsgemäß identifiziert.

Das Betreten oder Umhergehen im UMFOTEC-Gebäude, insbesondere (ohne Begleitung von autorisiertem Personal) in Bereichen mit beschränktem Zugang für Externe ist nicht gestattet, es sei denn, sie werden von autorisiertem UMFOTEC-Personal begleitet und haben eine GHV unterzeichnet.

Eine externe Zugangstür zum allgemeinen Lager ist für den Ein- und Ausgang von Waren bestimmt und darf nicht von Kunden oder anderen externen Personen benutzt werden.

Externes Personal der Transportunternehmen hat nur zu administrativen Zwecken Zugang zum Büro des Lagers. Die Drittfirmen sollten an ihren Standorten über eine angemessene Gebäudesicherheit und ein geregeltes Besuchermanagement verfügen.

### 4.2. Zugangskontrolle

Die Geschäftsanforderungen an Zugriffe auf UMFOTEC-Informationssysteme sind vor deren Freigabe zu definieren und zu dokumentieren. Die Zugangsvoraussetzungen orientieren sich an den geschäftlichen Erfordernissen.

Der Informationseigentümer und der Systemverantwortliche autorisieren den Zugang zu Daten und IT-Dienstleistungen in Übereinstimmung mit den Geschäftsanforderungen und Sicherheitsvorgaben. Die Informationssysteme der UMFOTEC werden nur für autorisierte dienstliche Zwecke eingesetzt, sofern keine abweichenden Vereinbarungen gelten. Alle relevanten Sicherheitsvorfälle werden dokumentiert, einschließlich einer Aufzeichnung der erfolgreichen und nicht erfolgreichen Anmeldeversuche.

UMFOTEC-Daten, die bei Drittfirmen gespeichert oder verarbeitet werden, sind so zu verwenden, dass keine Unbefugten diese Daten einsehen oder darauf zugreifen können. Vertrauliche und streng vertrauliche Dokumente dürfen niemals unbeaufsichtigt liegen gelassen werden, um Einsichtnahme durch Unberechtigte zu verhindern.

Dasselbe gilt auch für UMFOTEC IT-Geräte oder Systeme, die bei Drittfirmen im Einsatz sind. Die zur Verfügung gestellten Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen. Besondere Vorsicht ist bei der Verwendung mobiler Systeme geboten.

Unbefugte Nutzung der UMFOTEC datenverarbeitenden Systeme oder verbundener externen Systeme soll wie folgt verhindert werden:

- Die Anmeldung im Netzwerk/am PC erfolgt nur mit einem gültigen Account, die Nutzererkennung ist personalifiziert.
- Die Verwendung der Benutzererkennung oder des Kontos einer anderen Person ist nicht gestattet.
- Die Weitergabe von Identifikationsmitteln (z. B. SmartCards oder SecurID-Karten) ist nicht gestattet.
- Die Verwendung eines individuellen und sicheren Passwortes nach Stand der Technik ist gewährleistet.
  
- Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten, ausschließlich zu den von ihren Zugangsberechtigungen umfassten Daten Zugang haben.
- Rechte und Rollen werden dem „Need to know“-Prinzip folgend vergeben, wobei die jeweiligen Berechtigungen auf die Rolle zugeschnitten sind (least privilege).
- Zugriffe werden exakt dokumentiert.
- Nicht mehr benötigte Berechtigungen werden im Rahmen eines Nutzer-Identifikationsmanagements zeitnah entfernt.
- Der Zugriff von außen ist nur über eine verschlüsselte Kommunikation (VPN-Tunnel) möglich.



### 4.3. Trennungskontrolle

Wenn die Drittfirmen auch mit anderen Kunden arbeiten, muss eine Mandantenfähigkeit entsprechend den Anforderungen der Umfotec oder des Umfotec-Kunden logisch und physikalisch sichergestellt sein.

Eine Systemtrennung für Test und Produktion muss implementiert sein, basierend auf einer Risiko-Abschätzung.

### 4.4. Datenträgerkontrolle

Datenträger (wie z. B. CDs, DVDs, USB-Sticks und Festplatten) sind vor Verlust, Zerstörung und Verwechslung sowie vor unbefugtem Zugriff zu schützen.

Nicht mehr benötigte Datenträger sind auf sichere Weise nach Kap. 3.2 zu entsorgen. Ein Transport von Datenträgern mit UMFOTEC Daten zu einem zertifizierten Aktenvernichtungsunternehmen darf nur in geschlossenen Behältnissen und in „geschlossenen“ Fahrzeugen durchgeführt werden, sodass kein Material verloren gehen kann.

### 4.5. Transportkontrolle

Es wird gewährleistet, dass bei der Übermittlung von Informationen die Vertraulichkeit und die Integrität der Daten geschützt werden.

Datenverkehr, welcher UMFOTEC Daten transportiert, z. B. E-Mail, Webzugriff, wird verschlüsselt. Datenübertragungen werden verschlüsselt, z. B. S-FTP, VPN. Eine unautorisierte Weitergabe von Daten findet nicht statt.

Faxnummern und E-Mail-Adressen sind aktuellen Verzeichnissen zu entnehmen oder beim Empfänger zu erfragen, um fehlerhafte Übertragungen zu vermeiden. Für den Inhalt und die Verteilung einer E-Mail ist der Absender verantwortlich. Für die weitere Verarbeitung und Verteilung ist der Empfänger verantwortlich. Die Erstellung und der Versand von Ketten-E-Mails sind unzulässig.

Bei allen Gesprächen (einschließlich Telefonaten, Video- und Webkonferenzen), die vertraulichen oder streng vertraulichen Informationen betreffen oder enthalten, ist sicherzustellen, dass diese nicht unberechtigt mitgehört oder aufgezeichnet werden können.

### 4.6. Systemsicherheit

Informationen sollen vor unbeabsichtigter oder beabsichtigter Veränderung oder Zerstörung geschützt werden.

Es müssen Maßnahmen wie Protokollierung umgesetzt werden, die nachträglich überprüft und feststellt, ob und von wem Informationen in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Eine Übertragung der Informationen muss ausschließlich anhand der jeweiligen vertraglichen Vereinbarungen stattfinden. Diese Übertragung muss auch protokolliert werden. Das Netzwerk/die PCs sind durch ein Firewall-System gegenüber unberechtigten Zugriffen von außen, sowie durch ein Zonenkonzept von innen geschützt. Es erfolgt eine Überprüfung auf Aktualität.

Es muss sichergestellt sein, dass gespeicherte Informationen nicht durch Fehlfunktionen des Systems beschädigt werden können. Systemzustände werden kontinuierlich und automatisiert überwacht, um Fehlfunktionen frühzeitig zu erkennen. Eine regelmäßige Wartung muss auch festgelegt werden, um die Integrität von z. B. Datenbanken zu überprüfen. Nur autorisierte und fachkundige Mitarbeiter dürfen an Systeme während des Änderungsprozesses Veränderungen durchführen und Fehlfunktionen beheben.

Erstellung	Genehmigung	Datum
B. Schmalfuß	J. Lange	28.03.2024

<b>ST06_001_Rev01</b>	<b>Informationssicherheit bei UMFOTEC</b>	
<b>Public</b> <i>öffentlich</i>		

Die Sicherheitsanforderungen an ein Informationssystem gelten über den gesamten Lebenszyklus, die Verantwortung für die Einhaltung liegt beim zuständigen Business-Management. Die Einführung neuer Technologien darf das Sicherheitsniveau der UMFOTEC nicht gefährden

#### 4.7. Gewährleistung der Verfügbarkeit

Informationen und Dienstleistungen sollen durch ordnungsgemäße Archivierung, einen Einsatz von einem Virenschutzkonzept, eine unterbrechungsfreie Stromversorgung und ein angemessenes Backupkonzept sowie Recovery-Konzept stets verfügbar sein, wenn sie benötigt werden.

Die Verantwortlichen der Informationssysteme entwickeln, pflegen und testen regelmäßig Pläne zur Aufrechterhaltung des Betriebs kritischer Informationssysteme entsprechend regulatorischen, vertraglichen oder anderen Business-Vorgaben.

#### 4.8. Sicherheitsvorfälle

Jeder tatsächliche oder vermutete Sicherheitsvorfall muss so schnell wie möglich gemeldet werden:

Bei Datenschutzvorfällen → [helpdesk@umfotec.de](mailto:helpdesk@umfotec.de) muss in der Betreffzeile der Begriff: „**DSB**“ stehen.

Bei Informationssicherheitsvorfällen → [helpdesk@umfotec.de](mailto:helpdesk@umfotec.de) muss in der Betreffzeile der Begriff: „**ISB**“ stehen.

Alle Mitarbeiter und externen Vertragspartner müssen über das Verfahren zur Meldung von Sicherheitsvorfällen informiert sein.

Der zuständige Informationssicherheitsbeauftragte überprüft regelmäßig die gemeldeten Sicherheitsvorfälle, der Rückmeldungen und der getroffenen Maßnahmen.

Erstellung	Genehmigung	Datum
B. Schmalfuß	J. Lange	28.03.2024

## 5. Anhang – Änderungshistorie

Rev-Stand	Datum	Erstellung/ Änderung durch	Genehmigung durch	Beschreibung der Änderung
00	26.11.2023	B. Schmalfuß	J. Lange	Dokumentenerstellung
01	28.03.2024	B. Schmalfuß	J. Lange	Dokument umbenannt + div. Änderungen von IT etc. eingepflegt
02				
03				
04				
05				
06				
07				
08				
09				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				