Datenschutzhandbuch der Leuchtturm - Sozialpsychiatrische Hilfen GmbH

Inhalt

A) Allgemeines

Versionshistorie für das Datenschutzhandbuch

Version	Datum	Anmerkungen	Autor
1.0	01.06.2021	Initialfassung des Datenschutzhandbuchs	GF Lars Baumhauer
1.1	10.04.2024	Aktuelle Anpassungen	GF Lars Baumhauer
1.2	02.12.2024	Anlassbezogene Prüfung und Anpassung	Datenschutzberater Rüdiger Pabst (Pabst Data – Pabst Media GmbH)
1.3	17.12.2024	Anpassung Formatierungen, Ergänzung Prüfzyklen	Datenschutzberater Rüdiger Pabst (Pabst Data – Pabst Media GmbH)

1. Zweck des Datenschutzhandbuchs

Im Datenschutzhandbuch der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** werden die im Unternehmen geltenden Regeln zum Umgang mit personenbezogenen Daten definiert. Die **Ziele** des Datenschutzes und die damit verbundene Einhaltung der Vorgaben der Datenschutz-Grundverordnung (DSGVO) sind in der **Leitlinie zu Datenschutz und Informationssicherheit** festgehalten. Die Unternehmensleitung dokumentiert mit der Leitlinie ihre Verantwortung für die Einhaltung von Datenschutz und Informationssicherheit.
Aus der Leitlinie ergibt sich auch die Aufbauorganisation für die Umsetzung des Datenschutzes. Dieses hat die Aufgabe, Maßnahmen zur Einhaltung von Datenschutzvorgaben zu planen, bei der Umsetzung mitzuwirken und die Wirksamkeit der getroffenen Maßnahmen regelmäßig zu evaluieren und erforderliche Anpassungen vorzunehmen.
Das Datenschutzhandbuch enthält die wesentlichen Richtlinien, die für den Umgang mit personenbezogenen Daten gelten. Abweichungen von den Richtlinien sind nicht vorgesehen und bedürfen der Prüfung im Einzelfall sowie der vorherigen Freigabe durch die Geschäftsführung oder durch einen von der Geschäftsführung entsprechend bevollmächtigten Mitarbeiter.

2. Geltungsbereich

Dieses Datenschutzhandbuch und die jeweils aktuelle Fassung sind für alle Mitarbeiter verbindlich. Änderungen am Datenschutzhandbuch werden den Beschäftigten in geeigneter Weise mitgeteilt.

3. Inhalte des Datenschutzhandbuchs

In diesem Datenschutzhandbuch ist die von der Unternehmensleitung verabschiedete **Leitlinie zu Datenschutz und Informationssicherheit** wiedergegeben. Die Leitlinie wird von der Geschäftsführung freigegeben.
Im Anschluss daran finden sich die einzuhaltenden Richtlinien für den Umgang mit personenbezogenen Daten bzw. „Informationen“.

4. Prüfzyklus

Das Datenschutzhandbuch und die enthaltenen sowie ggf. ergänzenden Unterlagen sind mindestens einmal jährlich auf Aktualität, Angemessenheit sowie Wirksamkeit zu prüfen.

B) Leitlinie zu Datenschutz und Informationssicherheit

1. Einleitung

Der Verantwortliche verabschiedet hiermit diese Leitlinie zu Datenschutz und Informationssicherheit in unserem Unternehmen.
Als Unternehmen verarbeiten wir eine Vielzahl von (auch personenbezogenen) Daten, um unsere Aufgaben und Pflichten gegenüber unseren Klienten, Vertragspartnern, Dienstleistern, öffentlichen Stellen und sonstigen Dritten zu erfüllen. Dabei verarbeiten wir Daten mit unterschiedlichem Schutzbedarf. Die Sicherheit der Informationsverarbeitung und der Schutz von personenbezogenen Daten spielt eine wesentliche Rolle in unserem Unternehmen. Diese Leitlinie soll die Strategie, die Organisation und Ziele von Datenschutz und Informationssicherheit in unserem Unternehmen in übersichtlicher Form darstellen.

2. Geltungsbereich

Diese Leitlinie erstreckt sich auf alle aktuellen sowie zukünftigen Standorte des Verantwortlichen und verpflichtet alle Mitarbeiter zur Einhaltung der hier festgelegten Pflichten. Die Leitlinie wird den Beschäftigten in der jeweils geltenden Fassung über das „Datenschutzhandbuch“ des Verantwortlichen zugänglich gemacht.

3. Ziele

Ziel dieser Leitlinie ist es, Datenschutz und Informationssicherheit als Vrantwortlicher zu gewährleisten. Für diesen Zweck wird das Unternehmen bei der Planung, Einführung und während des Ablaufs von Prozessen insbesondere nachfolgende Ziele berücksichtigen:

1. Rechtmäßigkeit
2. Transparenz
3. Zweckbindung
4. Datenminimierung
5. Richtigkeit
6. Speicherbegrenzung
7. Verfügbarkeit, Integrität und Vertraulichkeit, Belastbarkeit
8. Intervenierbarkeit und Verarbeitung nach Treu und Glauben („Fairness“)
9. Rechenschaftspflicht („Accountability-Prinzip“)

Die Berücksichtigung dieser Ziele wird durch gesonderte Richtlinien, vor allem den Richtlinien des Datenschutzhandbuches konkretisiert. Bei der konkreten Umsetzung der Ziele müssen die getroffenen Schutzmaßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Schutzbedarf der verarbeiteten Daten und Informationen stehen.

4. Organisation von Datenschutz und Informationssicherheit

a) Informationssicherheit
Zur Erreichung der Ziele dieser Richtlinie hat sich die Geschäftsführung mit den allgemeinen Themen der Informationssicherheit vertraut gemacht. Verantwortlich für die Sicherheitsorganisation ist die Unternehmensleitung. Zukünftig werden bei Bedarf Aufgaben der operativen Umsetzung in diesem Bereich an geeignete IT-Dienstleister ausgelagert.

b) Datenschutzbeauftragter (DSB)
Der Verantwortliche ist zum Gegenwärtigen nach herrschender Meinung aufgrund deer Organisationsgröße nicht verpflichtet, einen Datenschutzbeauftragten zu bestellen. Insoweit unterliegt die Umsetzung des Datenschutzes vorläufig der Unternehmensleitung. Diese kann jedoch jederzeit aufgrund einer gesetzlichen Pflicht oder freiwillig einen internen oder externen DSB besteelln. einen Mitarbeiter oder die Geschäftsführung al Ansprechpartner für den Datenschutz

Soweit gegenwärtig kein DSB benannt ist, hat die Unternehmensleitung dennoch insb. die Erfüllung der nachfolgend benannten Aufgaben entsprechend sicherzustellen.

Der DSB berät, kontrolliert und unterstützt die Unternehmensleitung und Beschäftigten hinsichtlich der Verarbeitung von personenbezogenen Daten im Unternehmen. Seine weiteren Aufgaben ergeben sich vor allem aus Art. 39 DSGVO.
Im Bereich der Verarbeitung von personenbezogenen Daten ist Sorge dafür zu tragen, dass eine frühe Einbindung des **DSB** bei der Planung und Einführung von neuen Prozessen, in deren Zusammenhang auch personenbezogenen Daten verarbeitet werden, erfolgt. Gleiches gilt für Änderungen an bestehenden Prozessen. Die Einbindung des DSB kann auch im Zusammenhang mit der Einbindung des DST erfolgen.
Der Datenschutzbeauftragte und der Informationssicherheitsbeauftragte informieren und unterstützen sich gegenseitig durch gegenseitigen Informationsabgleich, soweit keine gesetzlichen oder vertraglichen Pflichten entgegenstehen. Der Informationsaustausch kann über das DST erfolgen.
Im Unternehmen wird sowohl für den Bereich der Informationssicherheit als auch für den Bereich des Datenschutzes ein Managementsystem eingerichtet. Hierfür wird im Unternehmen ein Prozess der kontinuierlichen Verbesserung mit dem Ziel implementiert, die einzelnen Maßnahmen in den Bereichen Datenschutz und Informationssicherheit so zu koordinieren, dass die Ziele dieser Leitlinie erreicht werden.

Bei Bedarf ist insbesondere eine entsprechende E-Mail-Adresse für Datenschutzanfragen eingerichtet und einem etwaigen DSB Zugriff gewährt.

Die Richtlinien, insbesondere die im Datenschutzhandbuch der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** enthaltenen Richtlinien, werden von der Unternehmensleitung verbindlich gemacht, so dass sie von den jeweiligen Adressaten der Richtlinie einzuhalten sind und Verstöße ggf. sanktioniert werden können.

5. Maßnahmen

Die Maßnahmen zur Umsetzung dieser Leitlinien können in Form von technischen und organisatorischen Maßnahmen erfolgen. Dazu gehören auch Richtlinien, betriebliche Regelungen oder betriebliche Anweisungen. Diese sind von den Beschäftigten zu befolgen.

6. Verantwortlichkeiten

Die **Unternehmensleitung** übernimmt die Gesamtverantwortung für die **Informationssicherheit** und den **Datenschutz** im Unternehmen.
Die Verantwortlichkeiten von DSB und ISB sind bereits oben beschrieben.
Der **IT-Verantwortliche** setzt die Richtlinien und sonstigen Vorgaben zu Datenschutz und Informationssicherheit in seinem Verantwortungsbereich um. Er stimmt Maßnahmen, die Auswirkungen auf die Informationssicherheit haben, mit dem Informationssicherheitsbeauftragten ab.
Die **Administratoren** führen die technischen Maßnahmen in Abstimmung mit dem IT-Verantwortlichen durch und tragen durch Verbesserungsvorschläge zur Optimierung der Informationssicherheit bei.
Vorgesetzte mit Personalverantwortung haben die Aufgabe, sicherzustellen, dass die getroffenen technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf die die in ihrem Verantwortungsbereich tätigen Personen umgesetzt werden.
Jeder **Mitarbeiter** trägt durch sein Verhalten zur Gewährleistung von Datenschutz und Informationssicherheit bei. Alle Beschäftigten sind verpflichtet, diese Leitlinie und die Richtlinien zu Datenschutz und Informationssicherheit, insbesondere die Richtlinien aus dem Datenschutzhandbuch der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**, einzuhalten.

Um Datenschutz und Informationssicherheit im Unternehmen ist jeder Mitarbeiter verpflichtet, Störungen, Sicherheitsvorfälle und Notfälle im Bereich der Informationssicherheit unverzüglich und direkt an die Unternehmensleitung ggf. an den ISB zu melden. Vorfälle im Bereich des Datenschutzes sind von allen Beschäftigten unverzüglich nach Kenntnisnahme an die Unternehmensleitung oder den DSB zu melden. Es gelten die jeweiligen Richtlinien aus dem Datenschutzhandbuch der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.

Projekt oder Prozessverantwortliche müssen den DSB odern die für den Datenschutz verantwortliche Unternehmensleitung bei allen Projekten mit Auswirkung auf die Verarbeitung personenbezogener Daten konsultieren, um sicherzustellen, dass datenschutzrechtliche Vorschriften eingehalten werden können. Ferner sind alle Projekt- oder Prozessverantwortlichen verpflichtet,

diese/n bei allen Projekten zu konsultieren, die Auswirkung auf die Informationssicherheit im Unternehmen haben.

Lieferanten, externe Dienstleister und sonstige Auftragnehmer sind durch gesonderte Vereinbarungen zu verpflichten, die sie betreffenden Vorgaben zu Datenschutz und Informationssicherheit einzuhalten, wenn diese Daten im Auftrag verarbeiten oder die Möglichkeit der Kenntnisnahme von personenbezogenen Daten oder als nicht öffentlich klassifizierten Informationen des Unternehmens haben. Auftragsverarbeiter sind mit besonderer Sorgfalt auszuwählen und durch eine geeignete Vorabkontrolle zu prüfen. Ferner ist zwingend mit allen Auftragsverarbeitern eine Vereinbarung zur Auftragsverarbeitung (kurz AVV) nach Art. 28 mitsamt den technischen und organisatorischen Maßnahmen (TOM) sowie Liste der Unterverarbeiter zu vereinbaren. Auftragsverarbeiter sind fortlaufend in geeignetem Umfang auf die Einhaltung des Datenschutzes zu prüfen.

7. Sanktionen

Ein Verstoß gegen diese Leitlinie kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden. Für Lieferanten, externe Dienstleister und sonstige Auftragnehmer sollten bei besonderen Risiken Vertragsstrafenregelungen vereinbart werden.
Zur Umsetzung der Ziele aus der Leitlinie sind die **nachfolgenden Richtlinien** von den Beschäftigten einzuhalten. Der Geltungsbereich ergibt sich aus der jeweiligen Richtlinie.
Dieses Datenschutzhandbuch wird regelmäßig aktualisiert. Die Änderungen sind der Versionshistorie zu entnehmen. Gleiches gilt für Änderungen der Richtlinien. Es gilt die jeweils aktuelle Fassung der Richtlinien in diesem Datenschutzhandbuch.

C) Richtlinie zum Datenschutz (für Beschäftigte)

1. Einleitung

Bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** werden personenbezogene Daten verarbeitet. Die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** ist gesetzlich verpflichtet, personenbezogene Daten unter Einhaltung der jeweils geltenden datenschutzrechtlichen Vorschriften zu verarbeiten.

Einschlägige Rechtsvorschriften sind dabei die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) sowie ggf. bereichsspezifische Rechtsvorschriften.
Jeder Geschäftsprozess, der mit einer Verarbeitung personenbezogener Daten einhergeht, ist von der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** auf die Einhaltung der rechtlichen Vorgaben zu prüfen.

Zudem ist der **Datenschutzbeauftragte** oder die für den Datenschutz verantwortliche Unternehmensleitung der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** für die Überprüfung der Einhaltung der gesetzlichen Vorschriften zum Datenschutz zuständig.
Um eine rechtskonforme Verarbeitung von personenbezogenen Daten zu gewährleisten, sind auch grundsätzliche Verhaltensanweisungen für die Beschäftigten erforderlich.
Diese sind Gegenstand dieser Richtlinie. Die Verhaltensanweisungen dieser Richtlinie können durch spezifische Anweisungen für einen Umgang mit personenbezogenen Daten in besonderen Fällen (z.B. in spezifischen Projekten) ergänzt oder konkretisiert werden.

2. Geltungsbereich

Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch Beschäftigte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese Richtlinie gilt für alle aktuellen sowie zukünftigen Standorte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.

Diese Richtlinie verpflichtet alle Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

3. Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten eingehalten werden.

4. Grundsätze für den Umgang mit personenbezogenen Daten

Die nachfolgenden Grundsätze sind von allen **Beschäftigten** der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** einzuhalten:
Personenbezogene Daten werden nicht eigenmächtig verarbeitet und nur bei rforderlichkeit sowie dem Vorliegen einer Rechtsgrundlage verarbeitet werden. Es wird ausschließlich die von der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** bereitgestellte oder genehmigte Hard- und Software genutzt.

Sollte zusätzliche Verarbeitungsprozesse für die Geschäftsprozesse erforderlich werden, werden diese beim Vorgesetzten gemeldet. Der Vorgesetzte wird die Erforderlichkeit prüfen. Im Falle einer Erforderlichkeit wird der Vorgesetzte den gewünschten Verarbeitungsprozess dem DSB melden.. Der neue Verarbeitungsprozess darf erst nach Prüfung und Freigabe durch di für dn Datenschutz verantwortliche Person eingesetzt werden.

Beschäftigte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** sind verpflichtet alle sie oder ihre Tätigkeit betreffenden Richtlinienvorgaben oder Anweisungen im Umgang mit personenbezogenen Daten einzuhalten. Dies gilt insbesondere für Vorgaben, die die Sicherheit personenbezogener Daten betreffen

Beschäftigte melden mögliche **Datenschutzvorfälle** unverzüglich an die für den Datenschutz verantwortliche Person. Ein Datenschutzvorfall liegt insbesondere vor, wenn die Annahme besteht,

dass die Datensicherheit, insbesondere die Vertraulichkeit von Daten, gefährdet sein kann. Ein Datenschutzvorfall liegt auch bei jedem Sachverhalt vor, bei dem die Annahme besteht, dass Dritte unbefugt Zugriff oder Zugang zu personenbezogenen Daten haben oder hatten.

5. Ausnahmen

Die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** kann Ausnahmen von den unter Ziff. 4 genannten Grundsätzen in begründeten Einzelfällen erlauben. Ausnahmen sind vom **DSB** zu prüfen und mit der Unternehmensleitung abzustimmen. Genehmigte Ausnahmen sind inklusive einer Begründung zu dokumentieren.

6. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

D) Richtlinie zur Umsetzung von Datenschutzmaßnahmen

1. Einleitung

Bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** werden personenbezogene Daten verarbeitet. Die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** ist gesetzlich verpflichtet, personenbezogene Daten unter Einhaltung der jeweils geltenden datenschutzrechtlichen Vorschriften zu verarbeiten.

Einschlägige Rechtsvorschriften sind dabei die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz sowie ggf. bereichsspezifische Rechtsvorschriften.
Jeder Geschäftsprozess, der mit einer Verarbeitung personenbezogener Daten einhergeht, ist von der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** auf die Einhaltung der rechtlichen Vorgaben zu prüfen.

Zudem ist der **Datenschutzbeauftragte** der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** für die Überprüfung der Einhaltung der gesetzlichen Aufgaben zuständig.

Um die Rechtskonformität von Datenverarbeitungen im Unternehmen zu gewährleisten, macht die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** durch diese Richtlinie Vorgaben für die **Einrichtung, Prüfung und Durchführung von Datenverarbeitungsprozessen**. Zudem wird mit dieser Richtlinie die Erstellung und Pflege des **Verzeichnisses von Verarbeitungstätigkeiten** i.S.d. Art. 30 DSGVO unterstützt. Gleiches gilt für die Unterstützung im Zusammenhang mit der Prüfung, ob (und erforderlichenfalls wie) **Datenschutz-Folgenabschätzungen** i.S.d. Art. 35 DSGVO durchzuführen sind.

Ferner sind von der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** etwaige Meldepflichten nach Art. 33, 34 DSGVO einzuhalten.

2. Geltungsbereich

Diese Richtlinie gilt für die Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungen personenbezogener Daten bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** oder für eine Verarbeitung selbst als „Owner“/Eigentümer verantwortlich sind.
Diese Richtlinie gilt für alle Standorte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.

3. Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten eingehalten werden.

4. Grundsätze für die Einrichtung oder Änderung von Verarbeitungen personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten und auch bei der Einrichtung oder Änderung von den damit zusammenhängenden Prozessen sind folgende Grundsätze der Datenverarbeitung i.S.d. Art. 5 DSGVO einzuhalten:
Personenbezogene Daten müssen
1. auf Basis einer Rechtsgrundlage oder Einwilligung, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
2. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);
3. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
5. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);

6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit");
7. für jeden Geschäftsprozess, der die Verarbeitung personenbezogener Daten beinhaltet, muss es einen Verantwortlichen bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** geben („Owner/Eigentümer");

Beschäftigte sind lediglich dazu befugt, die Berichte mitzunehmen, die alle 2 Jahre zusammen mit den Klienten erstellt werden. Die Rechtmäßigkeit dieser Mitnahme wird durch die Erforderlichkeit des Aufgabenbereiches begründet. Alle weiteren Unterlagen werden eingescannt und gemäß deutscher DSGVO in der Cloud gespeichert. Dies Befugnis besteht lediglich solange, bis die die geplante digitale Berichterstellung über eine entsprechend gesicherte Cloudanwendung abgelöst wird.

Bei Fragen zur Anwendung und Auslegung dieser Grundsätze kann sich jeder Beschäftige an den **DSB** oder die für den Datenschutz verantwortliche Person wenden.

5. Ausnahmen

Die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** kann Ausnahmen von den unter Ziff. 4 genannten Grundsätzen in begründeten Fällen erlauben. Ausnahmen sind vom DST zu prüfen und mit der Unternehmensleitung abzustimmen. Genehmigte Ausnahmen sind inklusive einer Begründung zu dokumentieren.

6. Verzeichnis von Verarbeitungstätigkeiten

Die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** führt ein Verzeichnis von Verarbeitungstätigkeiten und – soweit die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** als Auftragsverarbeiter tätig ist – auch ein Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter i.S.d. Art. 30 Abs. 2 DSGVO.

Das Verzeichnis von Verarbeitungstätigkeiten wird vom **DSB** verantwortet. Der DSB als federführende Person für die Pflege des Verarbeitungsverzeichnisses bestimmen. Der DSB trägt Sorge dafür, dass die Verarbeitungsverzeichnisse regelmäßig aktualisiert werden.
Alle Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungen personenbezogener Daten bei der Leuchtturm - Sozialpsychiatrische Hilfen GmbH oder für eine Verarbeitung selbst als „Owner/Eigentümer" verantwortlich sind, sind bei einer geplanten Einrichtung oder Änderung von Verarbeitungen und/oder Geschäftsprozessen verpflichtet, dieses dem DSB mitzuteilen.

7. Datenschutz-Folgenabschätzung

Der DSB wird jeden neuen, gemeldeten Verarbeitungsprozess dahingehend prüfen, ob damit voraussichtlich ein hohes Risiko für personenbezogene Daten einhergeht. Gleiches gilt für die Veränderung von Verarbeitungsprozessen.
Wenn ein voraussichtlich hohes Risiko besteht, wird der DSB der Unternehmensleitung die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) empfehlen. Die Unternehmensleitung entscheidet über das „Ob" und „Wie" der Durchführung der DSFA.
Die jeweilige Verarbeitung darf grundsätzlich erst nach Durchführung der DSFA und entsprechender Freigabe durch die Unternehmensleitung begonnen werden.

Die DSFA kann vom DSB und / oder in Zusammenarbeit mit weiteren Mitarbeitern durchgeführt werden. Die DSFA kann auch durch externe, fachkundige Personen durchgeführt werden. Der DSB steht bei der Durchführung der DSFA auf Anfrage für die Beratung zur Verfügung.

Das Ergebnis der DSFA wird der Unternehmensleitung mitgeteilt. Die Unternehmensleitung entscheidet über die Freigabe des Verarbeitungsprozesses.

Sollte die DSFA ergeben, dass das mit dem Verarbeitungsprozess verbundene Risiko nicht durch technische und organisatorische Maßnahmen eingedämmt werden kann, wird die Unternehmensleitung darüber entscheiden, ob die eine vorherige Konsultation mit der Aufsichtsbehörde i.S.d. Art. 36 DSGVO durchzuführen ist.

8. Meldepflichten bei Datenschutzverletzungen

Der DSB oder die für den Datenschutz verantwortliche Person untersucht unverzüglich jeden Vorfall oder jede Meldung („Vorfälle“) einer Verletzung des Schutzes personenbezogener Daten in Zusammenarbeit mit dem jeweiligen Fachverantwortlichen.
Jeder Vorfall wird vom DSB in Textform dokumentiert. Dabei werden Zeitpunkt der Kenntnisnahme, Sachverhaltsdarstellung und getroffene Maßnahmen dokumentiert. Bei jedem Vorfall ist zunächst zu prüfen, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt und die Verletzung voraussichtlich zu einem Risiko für die Betroffenen führt. Im Falle eines Risikos muss der DSB unverzüglich die Unternehmensleitung informieren und Sorge dafür tragen, dass binnen 72 Stunden nach Kenntnis von dem Vorfall eine Meldung an die für die **Leuchtturm – Sozialpsychiatrische Hilfen GmbH** zuständige **Aufsichtsbehörde für den Datenschutz** erfolgt. Sollte die Frist von 72 Stunden bereits verstrichen sein, wird gleichwohl so schnell wie möglich eine Meldung an die Aufsichtsbehörde erfolgen. Dieser Meldung ist dann eine Begründung für die Verzögerung beizufügen.

Die Meldung ist mit der Unternehmensleitung vorab abzustimmen und enthält mind. die In Art 33 genannten und nachfolgend beschriebenen Pflichtangaben.

Die Meldung muss insbesondere beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Sollten die genannten Informationen nicht binnen der 72-Stunden-Frist ermittelt oder zusammengestellt werden können, hat gleichwohl eine Meldung an die Aufsichtsbehörde zu erfolgen. Die o.g. Inhalte sind dann unverzüglich an die Aufsichtsbehörde nachzureichen. Nach Möglichkeit ist jedoch immer mind. eine vorläufige, fristwahrende Meldung unter Angabe des voraussichtlichen Zeitpunkts der Ergänzung fehlender Angaben durchzuführen.

Wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für von dem Vorfall Betroffenen hat, so benachrichtigt der DSB die **betroffenen Personen** unverzüglich von der Verletzung. Der DSB wird die Meldungen vorab mit der Unternehmensleitung abstimmen und dabei insbesondere etwaige Ausnahmeregelungen nach Art. 34 Abs. 3 DSGVO in Erwägung ziehen. Sofern die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** personenbezogene Daten im Auftrag anderer Unternehmen oder Organisationen verarbeitet, ist eine Meldung eines Vorfalls unverzüglich an den Auftraggeber der Datenverarbeitung vorzunehmen. Bezüglich Zeitpunkt und Art der Meldung ist sofort nach Kenntnis von einem Vorfall im betreffenden Auftragsverarbeitungsvertrag mit dem Auftraggeber nachzusehen, wann und wie die Meldung an den Auftraggeber zu erfolgen hat.

9. Schulungsmaßnahmen

Alle Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** sind zeitnah nach Beginn der Aufnahme ihrer Tätigkeit für die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** und sodann regelmäßig (mindestens jährlich) in **Datenschutzschulungen** mit den Rechtsvorschriften zur Verarbeitung personenbezogener Daten vertraut zu machen.

Alle Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungen personenbezogener Daten bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** verantwortlich sind, tragen Sorge dafür, dass alle Beschäftigten, die über diese Verarbeitungen Zugang zu personenbezogenen Daten haben, zuvor zum Datenschutz geschult wurden.

Der DSB wird ein Schulungskonzept entwickeln, dass die richtlinienkonforme Schulung der Beschäftigten gewährleistet, und der Unternehmensleitung vorlegen. Die Unternehmensleitung wird über die Durchführung des Schulungskonzeptes entscheiden und geeignete Schulungsmaßnahmen anordnen. Soweit kein DSB bestellt ist, kann die Schulung hilfsweise von der Geschäftsführung, vorzugsweise jedoch von einem geeigneten und qualifizierten externen Dienstleister durchgeführt werden.

10. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

E) Richtlinie für die Umsetzung von Betroffenenrechten

1. Einleitung

Die Datenschutz-Grundverordnung (DSGVO) sieht in den Art. 12 ff. DSGVO Rechte der von einer Verarbeitung personenbezogener Daten betroffenen Personen vor, die von der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** einzuhalten sind. Dies bedarf der Umsetzung von Maßnahmen bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.

2. Geltungsbereich

Diese Richtlinie gilt für alle Standorte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese Richtlinie verpflichtet alle Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

3. Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften für die Wahrung der Rechte der betroffenen Personen eingehalten werden.

4. Informationspflichten

Der DSB führt das Verzeichnis der Verarbeitungstätigkeiten regelmäßig in Zusammmenarbeit mit dem jeweiligen Fachverantwortlichen. Der DSB trägt Sorge dafür, dass für jede Verarbeitung im Verarbeitungsverzeichnis seitens der „Owner/Eigentümer“ der Verarbeitung Sorge dafür getragen wurde, dass Datenschutzinformationen für die betroffenen Personen im erforderlichen Umfang vorliegen und auch den betroffenen Personen in geeigneter Weise zur Verfügung gestellt werden. Die Informationen sind auch bei Änderungen der Verarbeitung auf ihre Aktualität vom „Owner/Eigentümer“ zu prüfen.
Art und Umfang der Informationserteilung sind mit dem DST abzusprechen.

5. Rechte auf Auskunft, Löschung, Widerspruch und weitere Betroffenenrechte gem. Artt. 15-22 DSGVO

Jede Person kann seine Betroffenenrechte nach den Art. 15-22 DSGVO gegenüber der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** geltend machen.
Dies beinhaltet insbesondere das Recht auf **Auskunft, Berichtigung** und **Löschung** von personenbezogenen Daten sowie das Recht auf **Einschränkung der Verarbeitung** sowie das Recht auf **Widerspruch** gegen eine Verarbeitung von Daten (z.B. auch gegen die Verwendung von Daten für Werbezwecke).
Alle Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** sind verpflichtet, einen von einem Betroffenen geltend gemachten Anspruch auf Auskunft, Berichtigung, Löschung oder einen Widerspruch unverzüglich nach Zugang der Mitteilung an den DSB weiterzuleiten. Die Weiterleitung kann z.B. auch per E-Mail an die E-Mail-Adresse des DSB / der für den Datenschutz verantwortlichen Person erfolgen.

Der DSB wird die Anfrage dokumentieren und unverzüglich, spätestens aber binnen **innerhalb eines Monats** nach Eingang der Mitteilung des Betroffenen bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** gegenüber dem Betroffenen beantworten.
Der DSB wird die Unternehmensleitung über schwierige oder umfangreiche Anfragen von Betroffenen informieren.

Das DST hat bei der Beantwortung von Anfragen von Betroffenen sicherzustellen, dass vor der Erteilung von Information an den Betroffenen sichergestellt wurde, dass die Person diejenige ist, für die sich ausgibt, um zu verhindern, dass personenbezogene Daten an Unbefugte gelangen. Im Fall einer Auskunftserteilung per E-Mail ist von dem Betroffenen vorab die Zustimmung einzuholen, dass die Informationen per E-Mail zur Verfügung gestellt werden. Bei Fehlen einer Zustimmung ist die Auskunft schriftlich zu erteilen.

6. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

F) IT-Richtlinie für Nutzer

1. Einleitung

Die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** verfügt über eine IT-Infrastruktur, die den Beschäftigten im Zusammenhang mit ihrer Tätigkeit für die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** als Arbeitsmittel zur Verfügung steht. Die IT-Infrastruktur ist unerlässlich für den Geschäftsbetrieb der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.

2. Geltungsbereich

Diese IT-Richtlinien gelten für die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**. Sie gelten für alle Standorte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese IT-Richtlinien sind von allen Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** einzuhalten.

3. Ziele

Um die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Systeme auf Dauer zu gewährleisten, sind die nachfolgenden IT-Richtlinien von allen Beschäftigten einzuhalten.

4. Allgemeine Nutzungsrichtlinien für IT-Systeme

Sofern nachfolgend von **IT-Systemen** die Rede ist, sind darunter ausnahmslos alle Geräte oder Anwendungen (Hard- und Software) zu verstehen, mit denen Informationen elektronisch verarbeitet oder übertragen werden können. Dazu gehören insbesondere PCs, Notebooks/Laptops, Tablet PCs (z.B. iPad), Telefone, Mobiltelefone, Server, Speichermedien, Netzwerktechnologie, Softwareprodukte und Drucker.
Die Nutzung der IT-Systeme und Applikationen im Unternehmen ist ausschließlich zu dienstlichen Zwecken und in jeweils erlaubten Umfang zur Aufgabenerledigung 28

zulässig. Abweichungen hiervon bedürfen der Erlaubnis des Arbeitgebers. Es darf nur die Software auf IT-Systemen des Unternehmens installiert werden, die vom Arbeitgeber oder der IT-Abteilung freigegeben worden ist.
Die Benutzung privater Hard-und Software zu dienstlichen Zwecken ohne Genehmigung ist nicht zulässig.

Die Nutzung von IT-Systemen bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** erfolgt grundsätzlich nur für berufliche Zwecke. Eine private Nutzung von IT-Systemen der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** ist grundsätzlich untersagt, sofern nicht diese oder eine andere Unternehmensrichtlinie ausdrückliche Ausnahmen hiervon regelt. Zur Umsetzung einheitlicher Vorgaben aus dem Datenschutz sowie der IT-Sicherheit, sind Ausnahmen jedoch ausdrücklich nicht zu empfehlen.

5. Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme und Applikationen bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** sind von den Beschäftigten die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie sonstige Rechtsvorschriften und Unternehmensrichtlinien einzuhalten. Sollten Beschäftigte unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren Vorgesetzten zur Klärung zu wenden.

6. Schulung

Das Unternehmen trägt Sorge dafür, dass die Beschäftigten die erforderlichen Schulungen und Instruktionen/Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen und/oder Applikationen erforderlich sind.

7. Generelle Vorgaben zur Minimierung von Risiken

Für die Minimierung der Risiken von Datenverlust und von IT-Notfällen sind die folgenden Vorgaben zu befolgen:

- Die Datenhaltung sowie der Betrieb von geschäftsrelevanten IT-Systemen erfolgt ausschließlich in den in der Richtlinie für Speicherorte festgelegten Speicherorten/-bereichen.
- Bei der Inanspruchnahme von externen Dienstleistern ist die Richtlinie mit „Regelungen für Lieferanten und sonstige Auftragnehmer“ zu befolgen. Eine Inanspruchnahme von externen Dienstleistern, die entweder Daten im Auftrag verarbeiten oder Kenntnis von Daten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** erhalten könnten, ist zwingend mit dem **DSB** abzustimmen.

8. Vorgaben zur Gestaltung des Arbeitsplatzes

Der Arbeitsplatz ist von den Beschäftigten so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein. So sind Büros nach dem Verlassen des Arbeitsplatzes grundsätzlich zu verschließen.
Beim Verlassen des Arbeitsplatz-PCs muss der jeweilige Mitarbeiter sich „abmelden“ bzw. seinen PC „sperren“, so dass vor der erneuten Nutzung des IT-Systems und/oder der Applikation(en) eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

In Bereichen mit Publikumsverkehr sind die IT-Systeme – insbesondere die Bildschirme – so auszurichten, dass das Risiko der Kenntnisnahme durch Besucher oder Dritte nach Möglichkeit ausgeschlossen wird. Insbesondere sind in Meetingräumen die Verbindungen zu den Bildschirmen in den Pausen und am Ende des Meetings zu trennen und der Präsentationsrechner ist zu sperren. Informationen in Papierform sind so abzulegen, dass Besucher oder sonstige Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

9. Richtlinien für den Passwort-Gebrauch

Soweit technisch möglich sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers nutzbar. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Soweit möglich oder angeordnet, werden Zwei-Faktor-Authentifizierungs-Systeme (2FA) verwendet.

Passwörter müssen eine Mindestlänge von 12 Zeichen haben. Das Passwort ist komplex zu gestalten und muss mindestens 3 der nachfolgenden 4 Kategorien enthalten:
1. Großbuchstaben
2. Kleinbuchstaben
3. Sonderzeichen
4. Ziffern

Soweit technisch möglich ist jeder Mitarbeiter verpflichtet, sein Initial-Passwort unverzüglich zu ändern.

Die Passwörter sind so zu wählen, dass sie nicht durch Dritte leicht zu erraten sind. Vor-und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345678).
Passwörter sollten grds. nur anlassbezogen gewechselt werden. Gründe für einen Wechsel können, mangelnde Komplexität / Länge, mögliche Kenntnisnahme durch Dritte oder sonstige Sicherheitsrisiken sein. Bereits genutzte Passwörter dürfen nicht noch einmal wiederverwendet werden.

10. Schutz vor Schad-Inhalten

Zum Schutz vor Schad-Inhalten werden im Unternehmen Virenschutzprogramme und mind. in Endgeräten wie PCs, Notebooks vorhandene Software Firewalls eingesetzt. Die Umsetzung des Virenschutzes erfolgt durch die IT-Administration oder einen geeigneten IT-Dinstleister.

Zudem kommen Systeme zum Einsatz, mit denen E-Mails mit unverlangter Werbung gefiltert werden. Entsprechende E-Mails werden in einem gesonderten Ordner abgelegt. Die Beschäftigten sind

verpflichtet, diesen Ordner regelmäßig – mindestens 1x täglich – im Hinblick auf falsch eingeordnete E-Mails zu sichten.

11. Richtlinie zur Nutzung von E-Mail/Internet

Beschäftigte erhalten einen dienstlichen E-Mail Account. Die Nutzung von E-Mail darf nur für dienstliche Zwecke erfolgen.

12. Verhalten bei Sicherheitsvorfällen

Sollte ein Mitarbeiter merken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, hat dieser sich unverzüglich an den DSB und die Unternehmensleitung zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

13. Weisungen

Die Mitarbeiter sind verpflichtet, den Weisungen der IT-Abteilung / des IT-Verantwortlichen in Bezug auf den Umgang mit IT-Systemen Folge zu leisten. Sofern Zweifel an der Richtigkeit oder der Sinnhaftigkeit von Weisungen bestehen, kann der DSB sowie die Geschäftsführung eingebunden werden.

14. Definition Notfall und Notfallplan

Ein Notfall kann den Geschäftsbetrieb nachhaltig gefährden. 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. Im Falle eines Notfalls gelten die Richtlinien des Notfallplans mit dem Zweck, den Geschäftsbetrieb aufrechtzuerhalten bzw. unverzüglich wieder einen Zustand einer funktionsfähigen IT-Infrastruktur herzustellen.
Der Notfallplan ist in einem separaten Dokument geregelt und beschreibt diese Punkte.

15. Protokollierung

In der IT-Infrastruktur werden verschiedene Informationen protokolliert, um Störungen, Ausfälle und Sicherheitsvorfälle schnell identifizieren und beheben zu können. Dabei werden die einschlägigen datenschutzrechtlichen Bestimmungen eingehalten und die Persönlichkeitsrechte der Mitarbeiter gewahrt.

Während des Regelbetriebs der IT-Infrastruktur werden von verschiedenen Systemen (insbesondere von Servern und Firewalls) Verbindungsdaten (Datum, Uhrzeit, Adressen von Absender und Empfänger, die Art der übertragenen Daten, das übertragene Datenvolumen usw.) protokolliert.
Im Zuge der Nutzung der IT-Infrastruktur werden Daten protokolliert, aus denen auch das Nutzerverhalten ganz oder in Teilen nachvollzogen werden kann (Zeitpunkt der An- und Abmeldung an IT-Systemen, Datum und Uhrzeit von Änderungen in Dateien, usw.).
Um gesetzliche Anforderungen zu erfüllen, archiviert das Unternehmen alle ein- und ausgehenden E-Mails mindestens für die Dauer gesetzlicher Aufbewahrungspflichten. Diese können bis zu zehn Jahre betragen.
Das Erheben dieser Protokolldaten ist für den sicheren und rechtskonformen Betrieb der IT-Infrastruktur notwendig.

Die Protokolldaten werden ausschließlich zu folgenden Zwecken verwendet:

- Analyse und Korrektur von Störungen, Ausfällen und Sicherheitsvorfällen
- Gewährleistung der Sicherheit der IT-Infrastruktur
- Optimierung der IT-Infrastruktur
- für Statistiken über die Nutzung der IT-Infrastruktur sowie für
- nicht personenbezogene Stichprobenkontrollen sowie Auswertungen gemäß dieser Richtlinie (siehe Abschnitt „Missbrauchskontrolle“)
- Die Protokolldaten werden nicht zur Leistungs- und Verhaltenskontrolle der Mitarbeiter eingesetzt.

16. Missbrauchskontrolle

Für das Erkennen von Störungen, Ausfälle und Sicherheitsvorfällen findet eine nicht-personenbezogene Auswertung der Protokolldaten durch einen gesondert beauftragten Mitarbeiter statt. Eine personenbezogene Auswertung der Protokolldaten findet nur statt, wenn aufgrund einer Stichprobenkontrolle, einer Meldung oder anderer Verdachtsmomente ein konkreter Verdacht auf eine missbräuchliche, unerlaubte oder strafbare Nutzung der IT-Infrastruktur besteht.

In diesem Falle ist folgende Vorgehensweise verbindlich:

- Eine personenbezogene Überprüfung der Protokolldaten erfolgt nur bei einem gewichtigen Missbrauchsverdacht, Bagatellfälle rechtfertigen die Überprüfung nicht.
- Sie wird nach dem Prinzip der Datensparsamkeit durchgeführt.
- Sie erfolgt unter zwingender Beteiligung des Datenschutzbeauftragten.
- Wird der Verdacht durch die Überprüfung nicht bestätigt, so werden die für die Überprüfung erhobenen Daten und Aufzeichnungen unverzüglich gelöscht. Der nicht bestätigte Verdacht darf keinerlei weitere Folgemaßnahmen – insbesondere keine gezielten Stichproben gegen den Mitarbeiter – nach sich ziehen.
- Bei Gefahr im Verzug werden durch die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** weitere gefährdende oder strafbare Handlungen – eventuell unter Einschaltung der Strafverfolgungsbehörden – unmittelbar unterbunden, insbesondere werden die erforderlichen technischen Abwehrmaßnahmen ohne Verzögerung ergriffen, auch wenn hierbei personenbezogene Daten erhoben oder eingesehen werden müssen. Dr DSB wird schnellstmöglich über die Vorgänge informiert.

17. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

G) Richtlinie für Speicherorte

1. Einleitung

Bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** können Daten auf verschiedenen IT-Systemen gespeichert werden („Speicherorte“). Um die Verfügbarkeit, Integrität und Vertraulichkeit von Daten zu gewährleisten, macht diese Richtlinie Vorgaben für Beschäftigte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**, aus denen sich ergibt, wo Daten zu speichern sind.

2. Geltungsbereich

Diese Richtlinie gilt für die Speicherung von Daten im Zusammenhang mit der Tätigkeit für die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese Richtlinie gilt für alle Standorte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese Richtlinie verpflichtet alle Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

3. Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen durch eine Vorgabe von Speicherorten gewährleistet wird.

4. Grundsätze der Speicherung von Daten

Grundsätzlich sind Daten nicht auf lokalen Festplatten oder Datenspeichern von Endgeräten zu speichern. Hintergrund ist neben der dann fehlenden Verfügbarkeit der Daten vor allem auch, dass dann eine Sicherung der Daten nicht in hinreichender Weise erfolgt. Dies führt auch bei Diebstahl oder sonstiger Zerstörung von lokaler Hard- und Software zu erheblichen Risiken für die Sicherheit und Vrfügbrkeit von perseonenbezogenen Daten.

Die Speicherung von Daten hat grundsätzlich in den Verzeichnissen/Ordnern von Servern bzw. IT-Systemen zu erfolgen, die für den Benutzer freigegeben sind. Bei der Verwendung von mobilen IT-Systemen und mobilen Datenträgern sind die insoweit geltenden Richtlinien zu beachten. Mobile Geräte müssen dabei immer geschützt und keinesfalls unbeaufsichtigt an einem für Dritte einsehbaren oder gar zugänglichen Ort aufbewahrt werden. So dürfen dienstliche Geräte wie Notebooks und Smartphones unter keinen Umständen unbeaufsichtigt im Fahrzeug liegen gelassen werden.

5. Datensicherung

Die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** stimmt mit ihren Administratoren / IT-Dienstleister ab, welche Daten in welchem Rhythmus und auf welchen Medien bzw. an welchen Orten gesichert werden. Die Datensicherungsstrategie ist von den zuständigen Administratoren zu dokumentieren.
Inkrementelle Datensicherungen sind mindestens täglich anzufertigen. Darüber hinaus ist auch eine wöchentliche Vollsicherung und eine monatliche Vollsicherung nach Möglichkeit umzusetzen.

6. Regelungen für Administratoren

Die Administratoren sind verpflichtet, alle für die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** bereitgestellten Speicherorte zu dokumentieren und mit dem jeweiligen Zweck des Verzeichnisses in ein Verzeichnis aufzunehmen. In dem Verzeichnis sind ggf. auch die erforderlichen Berechtigungen (Gruppen/Rollen) zu hinterlegen.

Wenn neue Speicherstrukturen durch Administratoren erstellt werden, ist dies mit der Unternehmensleitung abzustimmen.

7. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

H) Richtlinie für die Nutzung mobiler IT-Systeme

1. Einleitung

Die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** verfügt über eine IT-Infrastruktur, die den Beschäftigten im Zusammenhang mit ihrer Tätigkeit für die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** als Arbeitsmittel zur Verfügung steht. Bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** sind auch mobile IT-Systeme im Einsatz. Um den besonderen Risiken aus der Nutzung von mobilen IT-Systemen Rechnung zu tragen, wird die Nutzung dieser Systeme durch diese Richtlinie gesondert geregelt.

2. Geltungsbereich

Diese Richtlinie gilt für die Nutzung von mobilen IT-Systemen der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**. Diese Richtlinie gilt für alle Standorte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese Richtlinie verpflichtet alle Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

3. Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen auf mobilen IT-Systemen gewährleistet ist.

4. Grundsätze der Nutzung von mobilen IT-Systemen

Mobile IT-Systeme bergen das Risiko in sich, dass unbefugte Dritte in Besitz von Informationen der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** oder Kunden und/oder Geschäftspartnern der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** kommen können.
Daher sind mobile IT-Systeme grundsätzlich nur von den Mitarbeitern einzusetzen, die aufgrund ihrer Tätigkeit bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** auf die Nutzung eines mobilen IT-Systems angewiesen sind.

Grundsätzlich sind auf mobilen IT-Systemen nur dann Daten zu speichern, wenn dies für die Aufgabenerfüllung des Nutzers im Zusammenhang mit seiner Tätigkeit für die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** oder für Zwecke der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH zwingend** erforderlich ist.

Soweit technisch möglich, sind Daten auf den mobilen IT-Systemen stets verschlüsselt zu speichern. Bei der Umsetzung der Verschlüsselung ist vom Nutzer Sorge dafür zu tragen, dass eine Entschlüsselung der Daten für die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** jederzeit möglich ist. Der Mitarbeiter kann sich bei Fragen der Umsetzung an die IT-Abteilung wenden.
Der Nutzer darf das ihm zur Verfügung gestellte mobile IT-System nicht anderen Personen zur Nutzung überlassen.

Im Hinblick auf die Installation von Software auf den mobilen IT-Systemen gilt die „IT-Richtlinie für Nutzer“.

Mobile Datenträger (Festplatten, USB-Sticks, DVDs etc.) und Papierdokumente dürfen nur in begründeten Ausnahmefällen benutzt und mitgeführt werden. Hierfür ist die vorherige Zustimmung in Textform der Unternehmensleitung erforderlich.

5. Verwendung von mobilen IT-Systemen außerhalb des Betriebsgeländes

Werden mobile IT-Systeme außerhalb des Betriebsgeländes der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** verwendet, hat der Nutzer in besonderem Maße Sorge dafür zu tragen, dass Dritte keine Kenntnis von Informationen erhalten können, die mit dem mobilen IT-System verarbeitet werden.

Besonders schutzbedürftige Informationen sollten nach Möglichkeit nur an Orten verarbeitet werden, die von Dritten nicht einzusehen sind. Sollte dies nicht möglich sein, muss der Nutzer einen Ort bzw. Platz zur Verarbeitung von Daten wählen, der gewährleistet, dass der Bildschirm nicht von Dritten eingesehen werden kann. Dabei sollte das mobile IT-System nach Möglichkeit mit Sichtschutzvorrichtungen ausgestattet sein (z.B. Sichtschutzfolie bei Notebooks).

Mobile Geräte müssen dabei immer geschützt und keinesfalls unbeaufsichtigt an einem für Dritte einsehbaren oder gar zugänglichen Ort aufbewahrt werden. So dürfen dienstliche Geräte wie Notebooks und Smartphones unter keinen Umständen unbeaufsichtigt im Fahrzeug liegen gelassen werden.

Mobile Endgeräte dürfen im öffentlichen Raum genutzt werden, aber nur mit dem eigenen mobilen Netz verbunden sein. Die Anmeldung in fremden WLANs ist nicht gestattet.

Jeder Mitarbeiter hat dies im Rahmen seiner Pflichten zu gewährleisten. Ein Etwaiger Diebstahl, Verlust oder sonstiges Abhandenkommen von mobilen Geräten ist umgehend ab Kenntnisnahme dem DSB und / oder der Geschäftsführung mitzuteilen.

6. Datensicherung

Der Nutzer hat Sorge dafür zu tragen, dass Daten, die ausschließlich auf dem Gerät gespeichert werden, bei nächster Gelegenheit auf Datenspeicher übertragen werden, die die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** üblicherweise für die Speicherung von Unternehmensdaten verwendet.
Bei Fragen zu der Vorgehensweise der Übertragung der Daten hat sich der Nutzer an die IT-Abteilung zu wenden.

7. Diebstahl und Verlust

Ein Etwaiger Diebstahl, Verlust oder sonstiges Abhandenkommen von mobilen Geräten ist umgehend ab Kenntnisnahme dem DSB und / oder der Geschäftsführung mitzuteilen. Die Meldung muss so schnell wie möglich erfolgen, da in diesen Fällen gesetzliche Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen bestehen können, die im Falle einer zu späten Meldung Bußgelder in erheblicher Höhe nach sich ziehen können. Die Mitteilung muss so erfolgen, dass der Mitarbeiter eine Kenntnisnahme durch den DSB / die Unternehmensleitung sicherstellen kann.

8. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

I) Richtlinie Regelungen für Lieferanten und sonstige Auftragnehmer

1. Einleitung

Bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** können auch Lieferanten oder sonstige Auftragnehmer für die Durchführung von Leistungen beauftragt werden. Um die Verfügbarkeit, Integrität und Vertraulichkeit von Daten zu gewährleisten, macht diese Richtlinie Vorgaben für Beschäftigte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**, aus denen sich ergibt, ob und wie Lieferanten oder sonstige Auftragnehmer im Hinblick auf die Wahrung der Vertraulichkeit und des Datenschutzes beauftragt werden können.

2. Geltungsbereich

Diese Richtlinie gilt für die Beauftragung von Lieferanten oder sonstigen Auftragnehmern durch die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese Richtlinie gilt für alle Standorte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese Richtlinie verpflichtet alle Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

3. Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen bei Erbringung von Leistungen durch Lieferanten oder sonstige Auftragnehmer gewährleistet wird.

4. Grundsätze der Inanspruchnahme von Lieferanten oder sonstigen Auftragnehmern

Wenn Lieferanten oder sonstige Auftragnehmer im Zusammen mit ihrer Tätigkeit für die **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** Zugriff auf Informationen des Unternehmens und oder personenbezogene Daten, die vom Unternehmen verarbeitet werden, erhalten können, ist die Beauftragung vorher von der Unternehmensleitung zu genehmigen. Hierbei ist stets der DSB bzw. die für den Datenschutz verantwortliche Person in Verbindung setzen, um die datenschutzrechtliche Zulässigkeit und rechtliche Absicherung der Inanspruchnahme des Lieferanten oder sonstigen Auftragnehmers zu prüfen und zu klären.

Wenn eine Kenntnisnahme von personenbezogenen Daten durch den Lieferanten oder sonstigen Auftragnehmer nicht möglich ist, so sollte gleichwohl eine Geheimhaltungsverpflichtung mit dem jeweiligen Auftragnehmer abgeschlossen werden. Eine entsprechende Vorlage für eine solche Erklärung ist bei der Unternehmensleitung zu erhalten. Ferner ist zwingend mit allen Auftragsverarbeitern (weisungsgebundene Verarbeitung personenbezogener Daten) eine Vereinbarung zur Auftragsverarbeitung (kurz AVV) nach Art. 28 mitsamt den technischen und organisatorischen Maßnahmen (TOM) sowie Liste der Unterverarbeiter zu vereinbaren. Auftragsverarbeiter sind fortlaufend in geeignetem Umfang auf die Einhaltung des Datenschutzes zu prüfen.

5. Regelungen für Lieferanten und sonstige Auftragnehmer

Um die IT-Infrastruktur vor Störungen zu schützen und die Sicherheit der in ihr verarbeiteten, gespeicherten und übertragenen Informationen zu gewährleisten, sind Lieferanten und sonstige Auftragnehmer, die Zugriff auf IT-Systeme der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** haben, zwingend auf nachfolgende Regelungen zu verpflichten:

- Das unrechtmäßige Abrufen oder Verbreiten von Inhalten, die urheberrechtlich geschützt sind, ist untersagt.
- Ebenfalls untersagt ist das Abrufen oder Verbreiten von strafrechtlich relevanten oder sittenwidrigen Inhalten.
- in der IT-Infrastruktur eingesetzte Hard- und Software wird vor ihrem Einsatz erst nach Prüfung durch den Informationssicherheitsbeauftragten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** freigegeben.
- Das eigenmächtige Herunterladen von Software sowie die Installation oder Verwendung nicht freigegebener Hard- und Software ist den Lieferanten oder sonstigen Auftragnehmern nicht gestattet.

- Der Zugriff auf das Internet oder auf Netzwerke die nicht vom Unternehmen betrieben werden, erfolgt grundsätzlich nur über die vom Unternehmen speziell dafür bereitgestellten Zugänge.
- Zugangskennungen für die Nutzung der IT-Infrastruktur (wie z. B. Passwörter) sind von einem Lieferanten oder sonstigen Auftragnehmer geheimzuhalten und dürfen grundsätzlich nicht an Dritte weitergegeben werden. Auch innerhalb der jeweiligen Organisation des Lieferanten oder sonstigen Auftragnehmers ist dieser verpflichtet, die Daten vor anderen Beschäftigten des Auftragnehmers geheimzuhalten. Ausnahmen hiervon können gemacht werden, wenn die Leistungen des Auftragnehmers von einem Team von Personen für **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** durchgeführt werden.
- Die **private Nutzung** von IT-Systemen der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** ist jedem Lieferanten oder Auftragnehmer untersagt.
- Bei einem Einsatz von IT-Dienstleistern sind stets folgende Punkte zu berücksichtigen: IT-Systeme des Dienstleisters müssen über grundlegende Sicherheitsmaßnahmen verfügen: o Das IT-System muss ausreichend vor Schadsoftware gesichert sein. Es ist ein Virenscanner zu verwenden, der eine tagesaktuelle Versorgung mit Updates von Virendefinitionen gewährleistet. Der Virenscanner muss permanent aktiviert sein.

Die Betriebssysteme auf den IT-Systemen müssen auf dem jeweils aktuellen Stand von Sicherheitsupdates des jeweiligen Betriebssystemanbieters sein. Es sind nur Betriebssysteme zu verwenden, die vom Hersteller noch unterstützt und gepflegt werden („Support“)

6. Sanktionen
Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.
Die Verträge mit den Lieferanten oder sonstigen Auftragnehmern sollten ebenfalls Sanktionsmöglichkeiten für Verstöße der Auftragnehmer gegen die jeweils vereinbarten Pflichten im Zusammenhang mit Datenschutz und Informationssicherheit vorsehen.

J) Richtlinie für Störungen und Ausfälle

1. Einleitung

Diese Richtlinie regelt den Umgang mit Störungen und Ausfällen von IT-Systemen bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH.**

2. Geltungsbereich

Diese Richtlinie gilt für die gesamte IT-Infrastruktur der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** und gilt für alle Standorte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese Richtlinie verpflichtet alle Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

3. Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen der IT-Infrastruktur der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** gewährleistet ist.

4. Grundsätze

Die **IT-Infrastruktur** der Leuchtturm - Sozialpsychiatrische Hilfen GmbH umfasst ausnahmslos alle Geräte, die auf elektronischem Wege Informationen verarbeiten, übertragen oder speichern wie z.B. Arbeitsplatz-PCs, Server, Drucker, Speichermedien, Telefone, Fax-Geräte, mobile Telefone, Smartphones, Tablet-PCs u.ä.

Eine Störung ist eine Situation, in der Prozesse oder Ressourcen der Leuchtturm - Sozialpsychiatrische Hilfen GmbH nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind häufig als *gering* einzustufen. Die Beseitigung einer Störung kann meist im allgemeinen Tagesgeschäft vorgenommen werden.

Ein Ausfall liegt vor, wenn ein Teil oder Teile der IT-Infrastruktur ihre Funktionsfähigkeit verloren haben. Die Behebung dauert meist mehrere Tag oder länger und hat meist komplexe Ursachen.

5. Meldung

Störungen und Ausfälle beeinträchtigen die Funktionsfähigkeit des Unternehmens und können zu Kosten und weiteren Schäden führen. Wenn Störungen und Ausfälle nicht oder zu spät gemeldet werden, kann diese zu Folgeschäden führen, die zu vermeiden sind.
Um Störungen und Ausfälle schnell beheben zu können, ist eine unverzügliche Meldung entsprechender Vorfälle notwendig.

Jeder Mitarbeiter meldet mögliche Störungen und Ausfälle an einen **Administrator**. Sollte ein Administrator nicht zur Verfügung stehen, erfolgt die Meldung an den Vorgesetzten / die Unternehmsleitung. Dieser wird die Meldung entsprechend an einen Administrator oder die Unternehmensleitung weiterleiten.

Bei gravierenden Ausfällen wird die Unternehmensleitung ebenfalls sofort von dem Mitarbeiter informiert. Ein Ausfall gilt als gravierend, wenn eines der folgenden Merkmale zutreffend ist:

- Verletzung von Leib oder Leben von Menschen
- Störung der Finanzbuchhaltung
- Störung der Auftragsbearbeitung
- Es besteht ein Verstoß gegen Gesetze, Verträge oder Normen und es sind Haftungsrisiken entstanden, die für das Unternehmen oder für einzelne Verantwortliche beträchtlich sind, insbesondere mögliche Verstöße im Bereich des Datenschutzes.

6. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

K) Richtlinie für Sicherheitsvorfälle

1. Einleitung

Diese Richtlinie regelt den Umgang mit Sicherheitsvorfällen bei der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH.**

2. Geltungsbereich

Diese Richtlinie gilt für die gesamte IT-Infrastruktur der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** und gilt für alle Standorte der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH**.
Diese Richtlinie verpflichtet alle Beschäftigten der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

3. Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen der IT-Infrastruktur der **Leuchtturm - Sozialpsychiatrische Hilfen GmbH** gewährleistet ist.

4. Grundsätze

Die **IT-I**nfrastruktur der Leuchtturm - Sozialpsychiatrische Hilfen GmbH umfasst ausnahmslos alle Geräte, die auf elektronischem Wege Informationen verarbeiten, übertragen oder speichern wie z.B. Arbeitsplatz-PCs, Server, Drucker, Speichermedien, Telefone, Fax-Geräte, mobile Telefone, Smartphones, Tablet-PCs u.ä.

Ein Sicherheitsvorfall ist ein unerwünschtes Ereignis, das Auswirkungen auf die Informationssicherheit und/oder den Schutz von personenbezogenen Daten hat und in der Folge große Schäden nach sich ziehen kann.

5. Meldung

Sicherheitsvorfälle können erhebliche, negative Konsequenzen für das Unternehmen haben. Schon bei einem Verdacht eines Sicherheitsvorfalles muss sofort eine Meldung durch Mitarbeiter erfolgen, die den Sicherheitsvorfall bemerken.
Ausnahmen hierzu gibt es nur, wenn dem jeweiligen Mitarbeiter sicher bekannt ist, dass der Sicherheitsvorfall bereits von einem anderen Mitarbeiter gemeldet worden ist. Im Zweifel muss immer eine Meldung erfolgen.
Sicherheitsvorfälle sind **vorrangig**. Das bedeutet, dass die Meldung von Sicherheitsvorfällen stets dem Tagesgeschäft oder sonstigen aktuellen Arbeiten vorgeht.
Die Meldung erfolgt an den DSB und die Unternehmensleitung.

6. Behandlung des Sicherheitsvorfalls

Der DSB wird in Zusammenarbeit mit Der Unternehmensleitung und dem Fachverantwortlichen n Sicherheitsvorfall unverzüglich analysieren und – soweit erforderlich – alle Sofortmaßnahmen treffen, die zur Gewährleistung der Integrität, Verfügbarkeit und Vertraulichkeit der Informationen erforderlich sind.
Die weitere Analyse und das Treffen von weiteren Maßnahmen wird mit der Unternehmensleitung abgestimmt.

7. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

L) Notfallplan

1. Definition Notfall

Ein Notfall ist ein unerwünschtes, zeitlich nicht vorhersehbares Ereignis, das den Geschäftsbetrieb nachhaltig gefährden kann. Zur Bewältigung des Notfalls Im Falle eines Notfalls gelten die nachfolgenden Richtlinien mit dem Zweck, den Geschäftsbetrieb aufrechtzuerhalten bzw. unverzüglich wieder einen Zustand einer funktionsfähigen IT-Infrastruktur herzustellen.

2. Generelles Verhalten

Beim Auftreten eines Notfalles ist ein besonnenes Vorgehen besonders geboten. Vorrangig ist in einem Notfall Ruhe zu bewahren. Die Situation ist unverzüglich zu analysieren, und der Meldeplan ist unbedingt einzuhalten.
Bei einem reinen Verdacht auf Unregelmäßigkeiten, die auf einen Notfall oder sich ankündigenden Notfall hindeuten, ist in jedem Fall der Vorgesetzte und im Zweifel auch die IT-Abteilung zu informieren.

3. Feuer

In allen Räumen, in denen sich IT-Systeme befinden, die für den laufenden Geschäftsbetrieb zwingend erforderlich oder kritisch sind, sind Rauchmelder und/oder Brandmeldeanlagen in Betrieb. Darüber hinaus befinden sich in allen Gebäuden an mehreren Stellen die erforderlichen Feuerlöscher. Diese sind gut sichtbar angebracht und im Bedarfsfall zu nutzen. Im Falle eines Brandes ist zudem unverzüglich die Feuerwehr zu informieren.
Ferner ist die Unternehmensleitung und der DSB zu informieren.
Im Falle eines größeren Brandereignisses werden die Beschäftigten an den jeweiligen Betriebsstätten umgehend evakuiert. Fluchtwegepläne hängen in jedem Gebäude an gut sichtbarer Stelle aus.

4. Wasser

Größere Wasserschäden, die die für den Geschäftsbetrieb erforderlichen, kritischen IT-Systeme negativ beeinträchtigen könnten, stellen an allen Betriebsstätten aufgrund der Lage nur ein sehr geringes Risiko dar. Es ist regelmäßig nicht damit zu rechnen, dass ein Wasserschaden zu einer Beeinträchtigung der kritischen IT-Systeme führt. Die IT-Systeme befinden sich an Orten, an denen kein Hochwasser zu befürchten ist. Auch Schäden durch Wasserleitungen sind aufgrund der räumlichen Gegebenheiten eher unwahrscheinlich.
Sollte dennoch ein Wasserschaden auftreten, der eine Gefahr für die kritischen IT-Systeme oder andere IT-Systeme darstellen könnte, sind sofort die Unternehmensleitung und der IT-Verantwortliche. Diese werden dann nach Sichtung der Lage eine Risikobewertung und die weiter erforderlichen Maßnahmen vornehmen.

5. Stromausfall

Alle kritischen IT-Systeme wie Cloudserver, die für den Geschäftsbetrieb unerlässlich sind, verfügen über eine unterbrechungsfreie Stromversorgung (USV). Diese tragen Sorge dafür, dass Stromausfälle von mehreren Minuten überbrückt und im Falle eines längeren Stromausfalls die IT-Systeme geordnet heruntergefahren werden können, um die Integrität der Daten zu gewährleisten.
Der wesentliche Teil der kritischen IT-Systeme befindet sich in einem Rechenzentrum, das über Generatoren mit alternativer Stromerzeugung im Falle eines Stromausfalls verfügt und so auch bei längeren Stromausfällen eine Verfügbarkeit der IT-Systeme gewährleistet.

6. Ausfall von IT-Systemen

Alle kritischen IT-Systeme unterliegen einem Monitoring, mit dem die Verfügbarkeit und etwaige Störungen überwacht werden.
Im Falle eines Ausfalls wird der diensthabende IT-Mitarbeiter automatisch informiert. Dieser wird unverzüglich den Vorfall prüfen und bei nicht nur kurzen, vorübergehenden Störungen unverzüglich den Vorgesetzten informieren.

Der Grund für den Ausfall ist umgehend zu beheben. Bei kritischen IT-Systemen ist Sorge dafür zu tragen, dass immer ausreichend Ersatzteile und/oder Ersatzsysteme vorrätig sind, mit denen der Ausfall kurzfristig überbrückt bzw. beseitigt werden kann.

7. Angriffe von außen

Alle Server-IT-Systeme und alle kritischen IT-Systeme werden durch Firewall-Technologie gesichert und überwacht. Ein Zugriff unbefugter Dritter von außen wird auf diese Weise wesentlich erschwert. Die Firewall-Technologie wird regelmäßig gewartet und aktualisiert, um eine Anpassung an neue Gefahrenlagen zu gewährleisten.

8. Einbruch und Diebstahl

Alle Büro- und Geschäftsräume sind vor dem Zutritt unbefugter Dritter gesichert. Dies gilt insbesondere für den Zutritt zu Gebäuden außerhalb der Büro- und Geschäftszeiten.
Alle kritischen IT-Systeme befinden sich in besonders gesicherten Räumlichkeiten (z.B. Rechenzentren), die nur nach entsprechender Authentifizierung betreten werden können.
Für den Fall, dass ein Einbruch und/oder ein Diebstahl von IT-Systemen oder Geräten bemerkt wird, hat er jeweilige Mitarbeiter unverzüglich die Unternehmensleitung und den IT-Verantwortlichen zu informieren. Ferner ist der DSB unverzüglich zu informieren.

9. Ausfall von IT-Administratoren

Im Unternehmen verfügen zwar nur wenige Personen über Administrator-Rechte. Diese Personen sind entsprechend geschult und ausgebildet. Im Falle eines Ausfalls eines IT-Administrators (z.B. durch Krankheit) ist Sorge dafür getragen worden, dass mindestens ein weiterer Mitarbeiter mit Administrator-Rechten sofort erreichbar ist, um ggf. erforderliche Administrator-Handlungen durchzuführen.

10. Notfall-Verantwortlicher

Im Unternehmen gibt es einen Notfall-Verantwortlichen, der bei Vorliegen eines Notfalles für die Veranlassung der jeweils vorgesehenen und gebotenen Maßnahmen verantwortlich ist.
Hierbei handelt es sich um den Informationssicherheitsbeauftragten.

11. Wiederanlaufplan

Der IT-Verantwortliche trägt Sorge dafür, dass für kritische IT-Systeme stets die erforderlichen Ersatzteile bzw. Alternativsysteme vorrätig sind und Wiederanlaufpläne vorliegen. Die Wiederanlaufpläne sind in jedem Fall auch in Papierform zu dokumentieren und an einer Stelle zu hinterlegen, die im Falle eines Notfalls schnell zugänglich ist und sicherstellt, dass die in den Wiederanlaufpläne aufgezeigten Aktionen unverzüglich begonnen werden können.
Im Falle eines Funktionsausfalles eines IT-Systems wird die Ursache des Vorfalls unverzüglich untersucht. Parallel dazu werden sofort Maßnahmen in die Wege geleitet, um einen Wiederanlauf des IT-Systems oder eines Alternativsystems kurzfristig zu ermöglichen.

Der IT-Verantwortliche wird dahingehend geschult, Funktionsauswahl zu untersuchen und ein Wiederanlaufen der kritischen IT-Systeme schnellstmöglich vorzunehmen. Dabei ist in besonderer Weise dafür Sorge zu tragen, dass die Integrität der Daten gewährleistet ist.

12. Adressliste / Meldeliste

Hier finden Sie eine Übersicht der verantwortlichen Personen für die genannten Bereiche:

Funktion	**Name**	**Telefon / E-Mail**	**Handynummer ggf. Privat**
Geschäftsführerin	Monika Lemanczyk-Baumhauer	baumhauer@leuchtturm-norden.de	04121-8526111
Prokurist, Notfälle, Datenschutz und Dienstleister	Lars Baumhauer	verwaltung@leuchtturm-norden.de	04121-8526111
