GEMEINDEVERBAND
ALTENWOHNHEIM TELFS

DATENSCHUTZLEITLINIE

GDVBD ALTENWOHNHEIM TELFS

Gemeindeverband Altenwohnheim Telfs

Dir. Dorijan Jungic, DATB

Datenschutzbeauftragter
ZERTIFIZIERUNGS STELLE
N° DATB18I0040

WIFI WKO VALID: 05/2021

V 2.0

27.11.2018

Inhalt adaptiert auf Grundlage von Informationen und Texten der folgenden Institutionen:

WKÖ – Wirtschaftskammer Österreich

Bundesamt für Sicherheit und Informationstechnik

LEITLINIE ZUR INFORMATIONSSICHERHEIT

1 EINLEITUNG

Die Verbandsversammlung des Gemeindeverbandes Altenwohnheim Telfs verabschiedet folgende Leitlinie zur Informationssicherheit als Bestandteil ihrer Strategie:

1.1 STELLENWERT DER INFORMATIONSVERARBEITUNG

Informationsverarbeitung spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können.

Auch in Teilbereichen sind Ausfälle nicht hinnehmbar. Da unsere Kernkompetenz in der Pflege und Betreuung der uns anvertrauten Bürgerinnen und Bürger der Verbandsregion liegt, ist der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung von existenzieller Bedeutung.

1.2 ÜBERGREIFENDE ZIELE

Unsere Daten und unsere IT-Systeme in allen technikabhängigen und kaufmännischen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). Die Anforderungen an Vertraulichkeit haben ein normales, an Gesetzeskonformität orientiertes Niveau.

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden. Alle Mitarbeiter des Gemeindeverbandes Altenwohnheim Telfs halten die einschlägigen Gesetze (zB DSGVO, GuKG etc.) und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für den Verband sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter und die Direktionen sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

1.3 DETAILZIELE

Verspätete oder fehlerhafte Entscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für die Verbandsversammlung, als oberstes Gremium des Verbandes, bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungsdaten wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicher zu stellen.

Die Datenschutzgrundverordnung und die Interessen unserer Mitarbeiter verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten. Die Daten und die IT-Anwendungen der Personalabteilung werden daher einem hohen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Bewohner und Geschäftspartner.

Für den Pflegebereich ist die Aufrechterhaltung der digitalen Verfügbarkeit aller notwendigen Informationen (Durchführungsnachweise, Vitalwerte etc.) eine elementare Voraussetzung. Mangelhafte Verfügbarkeit der IT-Systeme und der Daten, aber auch Fehlfunktionen können zu weitreichenden Problemen in der Pflege führen. Die Aufrechterhaltung der Kommunikation und der ständige Zugriff auf korrekte Daten hat einen hohen Schutzbedarf.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

1.4 SICHERHEITSMAßNAHMEN

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können. Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen. IT-Benutzer nehmen regelmäßig an internen Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil.

1.5 VERBESSERUNG DER SICHERHEIT

Das Managementsystem der Informationssicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die Direktionen unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben. Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

Telfs, November 2018

DATENSCHUTZRICHTLINIE

Der Gemeindeverband Altenwohnheim Telfs („Gemeindeverband") respektiert das Persönlichkeitsrecht des Einzelnen und sein Recht auf Schutz seiner personenbezogenen Daten. Eine offene und ehrliche Kommunikation und die Erhebung von personenbezogenen und sensiblen personenbezogenen Daten sind für den Gemeindeverband nötig, um auf die Bedürfnisse einzelner Bewohner, Anwärter bzw. Interessenten und Mitarbeiter einzugehen und dem Gemeinwohl dienende Tätigkeiten ausführen zu können. Gleichzeitig erkennt der Gemeindeverband als korrelierende Notwendigkeit die Verpflichtung an, die Vertraulichkeit zu wahren und Informationen angemessen zu schützen. Wir messen der Vertraulichkeit in allen Belangen einen hohen Stellenwert bei.

Zahlreiche Länder haben Datenschutzgesetze erlassen, um das Persönlichkeitsrecht des Einzelnen zu schützen. Für den Gemeindeverband als übergeordneten Rechtsträger und Erhalter von Einrichtungen für Altenwohn- und Pflegeheime, Einrichtungen für seniorengerechtes Wohnen und Dienstleister für externe mildtätige Organisationen, war es seit jeher selbstverständlich, Persönlichkeitsrechte zu respektieren und die Vertraulichkeit zu wahren, bereits lange vor der Schaffung solcher Datenschutzgesetze. Der Gemeindeverband wird den Schutz der ihm zur Verfügung gestellter Informationen in Übereinstimmung mit seiner langjährigen Praxis weiterhin gewährleisten.

2 DATENSCHUTZGRUNDSÄTZE

Der Gemeindeverband behandelt alle personenbezogenen Daten in Übereinstimmung mit den folgenden Grundsätzen:

2.1 FAIRNESS UND RECHTMÄßIGKEIT

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise und fair erhoben und verarbeitet werden.

2.2 ZWECKBINDUNG

Personenbezogene Daten werden nur in dem Maße erhoben, verarbeitet und verwendet, wie es notwendig ist, damit der Gemeindeverband seine dem Gemeinwohl dienenden Zwecke erfüllen kann. Nachträgliche Änderung

der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung

2.3 TRANSPARENZ

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden, über:

- Die Identität der verantwortlichen Stelle
- Den Zweck der Datenverarbeitung
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

2.4 DATENVERMEIDUNG UND DATENSPARSAMKEIT

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, eine gesetzliche Bericht- und/oder Aufbewahrungspflicht sieht dies vor.

2.5 LÖSCHUNG

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde oder die Gemeinde- und/oder Landesarchive den Datenbestand auf seine Archivwürdigkeit für historische Zwecke bewerten konnten.

2.6 SACHLICHE RICHTIGKEIT UND DATENAKTUALITÄT

Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

2.7 VERTRAULICHKEIT UND DATENSICHERHEIT

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

Alle elektronisch gespeicherten Daten werden auf passwortgeschützten Computern gepflegt, deren Passwörter nur autorisierten Benutzern zur Verfügung stehen. Büros sind nach der Dienstzeit abgeschlossen; nur autorisiertes Personal hat Zugang.

Das Recht des Einzelnen auf Schutz personenbezogener und sensibler personenbezogener Daten sowie auf Korrektur oder Löschung personenbezogener und sensibler personenbezogener Daten (personenbezogene Daten besonderer Kategorien) wird nach Maßgabe der Verfahrensweisen des Gemeindeverbandes gewährt, die in der Richtlinie hinsichtlich der Verwendung personenbezogener Daten unter der Überschrift „Rechte des Nutzers“ dargelegt werden.

RICHTLINIE HINSICHTLICH DER VERWENDUNG PERSONENBEZOGENER DATEN

3 EINLEITUNG

Wir erheben, speichern und verwenden personenbezogene Daten, ausschließlich für die Zwecke, für die sie zur Verfügung gestellt worden sind, und die Aufbewahrung dieser Daten erfolgt nur solange, wie dies für den jeweiligen Zweck bzw. für andere im Sinne der Anfrage des Betroffenen zugehörigen rechtmäßigen Zwecke, die zutreffen mögen, erforderlich ist. Sollte sich ein Betroffener in diesen Situationen entscheiden, personenbezogene Daten, die erbeten werden, zurückzuhalten, kann es vorkommen, dass in diesem Fall die Erfüllung einer Bitte durch uns nicht möglich sein wird.

3.1 ONLINE

Die Inhalte der Website www.awh-telfs.at sind frei zugänglich, ohne dass man sich als Nutzer registrieren oder irgendwelche Informationen zur Verfügung stellen muss. Einige Funktionen (Ticketsystem) sind exklusiv Mitarbeitern des Gemeindeverbandes vorbehalten, stehen daher der Öffentlichkeit nicht zur Verfügung und demgemäß werden keine personenbezogenen Daten abgefragt und verarbeitet.

Es mag vorkommen, dass ein Besucher der Website seine personenbezogenen Daten (Name, Postanschrift, Telefonnummer) für eine Bewerbung als Heimbewohner, als Nutzer einer Wohnung für seniorengerechtes Wohnen oder als Mitarbeiter in einer Abteilung des Gemeindeverbandes Altenwohnheim Telfs einreichen bzw. personenbezogene Daten zu Spendenzwecken bekannt geben. In jedem Fall, in dem jemand eingeladen wird Informationen zur Verfügung zu stellen, wird der Zweck hierfür klar benannt. Wir werden keine Informationen für Zwecke nutzen, die zum Zeitpunkt der Zurverfügungstellung von Daten nicht benannt worden sind.

3.2 ZUGANG ZU PERSONENBEZOGENEN DATEN

Die in einer Anfrage oder Bewerbung zur Verfügung gestellten Daten sind den Datenverarbeitern zugänglich, die an der Erfüllung des Datenverarbeitungszwecks beteiligt sind und/oder technischen Support-Spezialisten, die

Aufgaben in Verbindung mit dem Betrieb und der Wartung des Verarbeitungssystems erfüllen. Wir werden keine personenbezogenen Daten an irgendjemand anderen herausgegeben, es sei denn (1) dies ist erforderlich zur Erbringung der vom Nutzer angefragten Dienste und wir haben dies mit einer umfassenden Information dem Nutzer mitgeteilt; (2) wir sind der Überzeugung, dass die Offenlegung solcher Information vernünftigerweise notwendig ist, um allen anwendbaren Gesetzen oder Vorschriften zu genügen; (3) dies geschieht infolge einer Aufforderung von Strafverfolgungsbehörden; (4) dies ist notwendig zur Aufdeckung und Verhinderung von Betrug aus technischen oder Sicherheitsgründen. Durch die Nutzung dieser Website willigt der Nutzer zu ausschließlich diesen Zwecken in die Offenlegung seiner personenbezogenen Daten an Dritte ein. Personenbezogene Daten, die der Nutzer zur Verfügung stellt, werden unter keinen Umständen verkauft oder vermietet, noch wird Handel damit getrieben.

3.3 BEWERBUNGEN

Möglicherweise stellen Bewerber einer Arbeitsstelle, ob initiativ oder aufgrund einer Ausschreibung, ihre personenbezogenen Daten und sensiblen personenbezogenen Daten obgleich digital und/oder in Papierform dem Gemeindeverband zur Verfügung. In diesem Fall werden die zur Verfügung gestellten Daten ausschließlich zur Prüfung und Verarbeitung der Bewerbung sowie für damit verbundene administrative Zwecke verwendet. Wenn es für die Bearbeitung der Bewerbung nötig ist, mögen die darin enthaltenen Daten auch zusammenarbeitenden verbandsinternen Gremien und/oder Gemeinden, denen der Gemeindeverband angehört, zur Verfügung gestellt werden. Bewerbungen werden sechs Monate nach nachweislichem Einlangen aufbewahrt. Wenn ein Bewerber eine längere Aufbewahrung seiner übermittelten Unterlangen wünscht, ist dies ausdrücklich anzugeben.

3.4 SPENDEN

Wir erfassen Namen, Kontaktdaten und die Bankverbindung von Spendern. Der Spendenempfänger verwahrt Aufzeichnungen über die finanziellen Transaktionen für eine Dauer von mindestens zehn Jahren. Dies umfasst Aufzeichnungen über das Datum der Spende, den gespendeten Betrag und die Zahlungsmethode. Dadurch wird es uns ermöglicht, Buchführungsvorschriften zu genügen und Fragen des Spenders während der genannten Zeitspanne zu beantworten. Wir werden keinen Spender kontaktieren, um weitere Spenden zu erbitten.

3.5 RECHTE DES NUTZERS

Wann immer wir personenbezogene Daten verarbeiten, unternehmen wir vernünftige Schritte um sicherzustellen, dass die personenbezogenen Daten des Nutzers für die Zwecke, für die sie gesammelt wurden, korrekt und aktuell gehalten werden. Der Nutzer hat die nachfolgenden Rechte hinsichtlich seiner zur Verfügung gestellten personenbezogenen Daten und personenbezogenen Daten besonderer Kategorien:

- Auskunftsrecht über die Erhebung und Verwendung seiner personenbezogenen Informationen gemäß den anwendbaren Datenschutzgesetzen
- Recht auf Auskunft, Korrektur, Löschung oder Sperrung der personenbezogenen Informationen, sofern diese unvollständig oder unrichtig sind.
- Falls jemand rechtliche Gründe dafür hat, kann er der Verarbeitung seiner personenbezogenen Informationen widersprechen und uns auffordern, seine Daten nicht weiter zu verwenden.

3.6 AUSKUNFTSBEGEHREN

Nach Erhalt des schriftlichen Antrags des Betroffenen, eines ausreichenden Identitätsnachweises und genügender Hinweise, die es uns ermöglichen, seine personenbezogenen Daten ausfindig zu machen, wird der Verantwortliche das Interesse des Einzelnen an der Datenauskunft, der Datenkorrektur oder der Datenlöschung mit dem berechtigten Interesse des Gemeindeverbandes Altenwohnheim Telfs — einschließlich der Abwägung, ob die Erfüllung gesetzliche Verpflichtungen gefährden würde — zu einem gerechten Ausgleich bringen. Wir werden auch alle Dritten, die diese Daten von uns erhalten haben, über die notwendigen Änderungen in Kenntnis setzen.

Wir weisen darauf hin, dass die Daten nicht gelöscht werden mögen, wenn die Verarbeitung gesetzlich vorgeschrieben ist oder wenn die Daten aufgrund einer anderen Rechtsgrundlage aufbewahrt werden können. Löschungsanfragen unterliegen allen auf uns anwendbaren gesetzlichen Berichtspflichten oder Aufbewahrungspflichten von Dokumenten. Ein Nutzer kann eine Beschwerde bei der Datenschutzbehörde einreichen hinsichtlich der Verarbeitung der Daten, die er mittels dieser Website zur Verfügung gestellt hat.

VERWENDUNG PERSONENBEZOGENER DATEN - DIENSTNEHMER

4 EINLEITUNG

Wer Dienstnehmer des Gemeindeverbandes Altenwohnheim Telfs ist, anerkennt, dass der Gemeindeverband als Dienstgeber – einschließlich der Verbandsgemeinden – rechtmäßig personenbezogene Daten in Übereinstimmung mit den berechtigten Interessen verwendet.

Dienstnehmer mögen dem Gemeindeverband zusätzliche personenbezogene Daten zur Verfügung stellen, wenn sie an internen und/oder externen Tätigkeiten bzw. Veranstaltungen teilnehmen.

Die Daten schließen möglicherweise Informationen ein, die sensible Daten (personenbezogene Daten besonderer Kategorien) beinhalten. Verwendung personenbezogener Daten kann das Erheben, Erfassen, Organisieren, Ordnen und Speichern von Daten bedeuten sowie vergleichbare Datenverarbeitungsvorgänge sein.

5 DATENVERARBEITUNG IM RAHMEN DES ARBEITSVERHÄLTNISSES

Die Verarbeitung und Übermittlung der Daten erfolgt für die Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zum Beispiel Korrespondenz) in diesen Angelegenheiten. Dies gilt auch für alle freiwilligen Sozialleistungen des Dienstgebers sowie für externe Bildungs- und Weiterbildungsangebote.

Eine Übermittlung der im jeweiligen Einzelfall relevanten Daten erfolgt auf Grundlage der gesetzlichen Bestimmungen bzw. vertraglicher Vereinbarung an folgende Stellen:

- Lohnverrechnung (extern)
- Sozialversicherungsträger;

- Bundesamt für Soziales und Behindertenwesen (Sozialministeriumsservice) zB gemäß § 16 BEinstG;
- Finanzamt;
- Betriebliche Vorsorgekassen (BV-Kassen) gemäß § 11 Abs 2 Z 5 und § 13 BMSVG;
- Lehrlingsstelle gemäß §§ 12 und 19 BAG und Berufsschulen;
- Arbeitsmarktservice;
- Arbeitsinspektorat, Verkehrs-Arbeitsinspektion, insbesondere gemäß § 8 Arbeitsinspektionsgesetz;
- Gemeindebehörden und Bezirksverwaltungsbehörden in verwaltungspolizeilichen Agenden (Gewerbebehörde, Zuständigkeiten nach ASchG usw.);
- gesetzliche Interessenvertretungen;
- Betriebsärzte;
- Bildungs- und Weiterbildungsanbieter;
- Amt der Tiroler Landesregierung;
- Portal Tirol (portal.tirol.gv.at);
- ARGE – Arbeitsgemeinschaft Tiroler Altenheime
- Organe der betrieblichen Interessenvertretung (insbesondere Betriebsrat § 89 ArbVG, Sicherheitsvertrauensperson nach § 10 ASchG, Jugendvertrauensperson gemäß § 125 ff ArbVG und Behindertenvertrauensperson gemäß § 22a BEinstG);
- Rechtsvertreter;
- Gerichte;
- Gläubiger der betroffenen Person sowie sonstige an der allenfalls damit verbundenen Rechtsverfolgung Beteiligte, auch bei freiwilligen Gehaltsabtretungen für fällige Forderungen;
- mit der Auszahlung an die betroffene Person oder an Dritte befasste Banken;
- vom Arbeitnehmer angegebene Gewerkschaft, mit Einwilligung der betroffenen Person;
- Mitversicherte;
- Pensionskassen;
- Versicherungsanstalten im Rahmen einer bestehenden Gruppen- oder Einzelversicherung;

6 DATENVERARBEITUNG FÜR ZWECKE DER VERWALTUNG UND SICHERHEIT DES SYSTEMS

Aufgrund der geltenden gesetzlichen Datensicherheitsbestimmungen werden eine Reihe von Daten für die Verwaltung und Sicherheit des Systems verarbeitet, wie etwa zur Verwaltung von Benutzerkennzeichen, die Zuteilung

von Hard- und Software an die Systembenutzer sowie für die Sicherheit des Systems. Dies schließt automationsunterstützt erstellte und archivierte Textdokumente (wie zB Korrespondenz) in diesen Angelegenheiten mit ein. Ohne diese Datenverarbeitung ist ein sicherer Betrieb des Systems und damit eine Beschäftigung im Gemeindeverband nicht möglich. Eine Reihe von Daten werden zur Erbringung von zum Beispiel Help-Desk-Diensten, Cloud-Diensten, etc. an einen Auftragsverarbeiter weitergegeben.

Personalisierte E-Mail-Adressen sind ausschließlich der betrieblichen Nutzung vorbehalten, eine Privatnutzung ist ausgeschlossen. Personalisierte E-Mail-Adressen werden nach Ausscheiden des Dienstnehmers aus dem Gemeindeverband drei Monate bestehen bleiben; elektronische Postnachrichten dem logisch folgenden Mitarbeiter bzw. der Abteilung weitergeleitet.

6.1 VERÖFFENTLICHUNG BERUFLICHER KONTAKTDATEN AUF DER WEBSITE WWW.AWH-TELFS.AT

Zur Kontaktaufnahme durch Kunden und Lieferanten werden berufliche Kontaktdaten von Mitarbeitern mit Außenkontakt im Internet veröffentlicht. Dies erfolgt aus unserem berechtigten Interesse an einem reibungslosen Geschäftsablauf.

6.2 DATENVERARBEITUNG IM FALLE VON ARBEITSRECHTSSTREITIGKEITEN

Kommt es während des aufrechten Dienstverhältnisses oder nach Beendigung zu einer gerichtlichen Auseinandersetzung, werden die für die zweckentsprechende Rechtsverfolgung notwendigen Daten an Rechtsvertreter und Gerichte übermittelt.

6.3 RECHTSGRUNDLAGE

In Österreich findet folgendes Datenschutzgesetz Anwendung:

- Datenschutzgesetz (DSG)
- Datenschutzgrundverordnung (EU) 2016/679

7 VERARBEITUNG FREIWILLIGER ANGABEN

Dienstnehmer stimmen auf Grundlage dieses Datenschutzgesetzes ausdrücklich der Verwendung ihrer personenbezogenen Daten durch den Gemeindeverband zu, einschließlich der nachfolgenden:

1. Zurverfügungstellung von personenbezogenen Daten an die gewählte Personalvertretung, soweit dafür nicht bereits eine Rechtsgrundlage besteht;
2. Übernahme von Aufgaben oder das Erfüllen gewisser Funktionen („Heute hat Dienst"-Tafel), was einschließt, dass der Name des Mitarbeiters und seine Aufgabe ausgehängt wird;
3. Anfertigung, Hinterlegung und Verwendung des eigenen Lichtbildes in der Personaldatenbank (CareCenter), zur Erstellung des Dienstausweises und gegebenenfalls Publizierung auf der Website www.awh-telfs.at;
4. Anfertigung, Hinterlegung und Verwendung von Einzel- und Gruppenbildern bei Veranstaltungen, zur Dokumentation von Aktivitäten mit Bewohnern und öffentlicher Darstellung auf internen Monitoren;
5. Führen von Aufzeichnungen betreffend des Kfz-Kennzeichens zur Erstellung von Parkberechtigungen;
6. Verarbeitung des Religionsbekenntnisses, wenn entsprechende Rechte in Anspruch genommen werden möchten;
7. Verarbeitung der Gewerkschaftszugehörigkeit, soweit der Gewerkschaftsbeitrag über den Dienstgeber abgeführt wird;
8. Verarbeitung von Notfallkontakten, soweit vom Dienstnehmer gewünscht;
9. Datenverarbeitung im Zuge von außerbetrieblichen Veranstaltungen, zum Beispiel Betriebsausflug, Weihnachtsfeier, etc.;
10. Verarbeitung von relevanten Gesundheitsdaten, soweit Personalessen genutzt wird;
11. Zustellung von betrieblichen Informationen mittels Newsletter per Mail;
12. Zustellung von betrieblichen Informationen mittels SMS;

8 RECHTE DES DIENSTNEHMERS

Personenbezogene Daten werden auf nicht näher bestimmte Zeit gespeichert, solange die oben genannten Zwecke oder andere berechtigte Interessen bestehen. Mitarbeiter haben hinsichtlich ihrer personenbezogenen Daten, die der Gemeindeverband speichert, das Recht auf Auskunft und Berichtigung unrichtiger Daten sowie um Löschung oder Einschränkung der Verarbeitung zu ersuchen. Mitarbeiter können hinsichtlich bestimmter zukünftiger Verwendung ihrer personenbezogenen Daten ihre Einwilligung jederzeit widerrufen. Ein Widerruf hat zur Folge, dass Daten ab diesem Zeitpunkt zu dem widerrufenen Zweck nicht weiter verarbeitet werden, und somit entsprechende Rechte, Vorteile, etc. nicht mehr in Anspruch genommen werden können.

Falls ein Dienstnehmer seine Einwilligung in die Verwendung seiner personenbezogenen Daten zurückzieht, mag der Gemeindeverband als Dienstgeber auf Grundlage seiner berechtigten Interessen zur Pflege und Verwaltung oder eines anderen im Datenschutzgesetz verankerten Rechtsgrundes berechtigt sein, einige dieser personenbezogenen Daten ohne eine solche Einwilligung weiter zu verwenden. Dienstnehmer sind sich bewusst, dass sie das Recht haben, eine Beschwerde bei der Datenschutzbehörde einzureichen.

Der Gemeindeverband Altenwohnheim Telfs hat in Übereinstimmung mit dem Datenschutzgesetz verschiedene technische und organisatorische Sicherheitsmaßnahmen ergriffen, um personenbezogene Daten zu schützen. Dienstnehmer sind sich darüber im Klaren, dass nur einer begrenzten Anzahl von autorisierten Personen zur Erfüllung der oben genannten Zwecke Zugriff auf ihre personenbezogenen Daten gewährt wird.

9 ANFRAGEN

Anfragen an den Datenschutzbeauftragten (siehe „Kontakt Datenschutzbeauftragter“) können schriftlich, fernmündlich oder persönlich (bei ausreichender Identitätsfeststellung) gestellt werden.

10 ÄNDERUNG DER VERWENDUNG PERSONENBEZOGENER DATEN

Es kann sein, dass sich die Vorgehensweise des Gemeindeverbandes bezüglich Daten von Zeit zu Zeit ändern kann, zum Beispiel aufgrund Änderung, Wegfall oder Neueinführung von Prozessen oder aufgrund von Gesetzen oder Technik. Sollte es jemals notwendig werden, beschriebenen Inhalt zu ändern, werden diese Änderung auf online auf www.awh-telfs.at und mittels interner Kundmachung veröffentlicht, damit Dienstnehmern immer bewusst ist, welche Informationen seitens des Gemeindeverbandes erfasst und wie sie verwendet werden.

VERWENDUNG PERSONENBEZOGENER DATEN – BEWOHNER UND DEREN ANGEHÖRIGE

11 EINLEITUNG

Wer Bewohner des Gemeindeverbandes Altenwohnheim Telfs ist, anerkennt, dass der Gemeindeverband– einschließlich der Verbandsgemeinden – rechtmäßig personenbezogene Daten in Übereinstimmung mit den berechtigten Interessen verwendet.

Die Daten schließen möglicherweise Informationen ein, die sensible Daten (personenbezogene Daten besonderer Kategorien) beinhalten. Verwendung personenbezogener Daten kann das Erheben, Erfassen, Organisieren, Ordnen und Speichern von Daten bedeuten sowie vergleichbare Datenverarbeitungsvorgänge sein.

12 DATENVERARBEITUNG IM RAHMEN EINES HEIM- UND/ODER NUTZUNGSVERTRAGES

Die Verarbeitung und Übermittlung der Daten erfolgt für Gebührenverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen oder Normen kollektiver Rechtsgestaltung jeweils erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zum Beispiel Korrespondenz) in diesen Angelegenheiten.

Eine Übermittlung der im jeweiligen Einzelfall relevanten Daten erfolgt auf Grundlage der gesetzlichen Bestimmungen bzw. vertraglicher Vereinbarung an folgende Stellen:

- Vertrauensperson nach § 30 Heimvertrag
- Hausarzt; behandelnde Ärzte, Therapeuten
- Apotheken
- Vorsorgebevollmächtigte oder an gewählte/gesetzliche/gerichtliche Erwachsenen-vertreter

- Weiterführende betreuende Einrichtungen und Organisationen (wie zum Beispiel Rehabilitationseinrichtungen)
- Lohnverrechnung (bei Betriebs- und/oder Gemeindepensionen)
- Sozialversicherungsträger;
- Bundesamt für Soziales und Behindertenwesen (Sozialministeriumsservice) zB gemäß § 16 BEinstG;
- Finanzamt;
- Gemeindebehörden und Bezirksverwaltungsbehörden
- gesetzliche Interessenvertretungen (wie zum Beispiel Heimanwaltschaft Tirol)
- Amt der Tiroler Landesregierung;
- ARGE – Arbeitsgemeinschaft Tiroler Altenheime
- Rechtsvertreter;
- Gerichte;
- Gläubiger der betroffenen Person sowie sonstige an der allenfalls damit verbundenen Rechtsverfolgung Beteiligte, auch bei freiwilligen Gehaltsabtretungen für fällige Forderungen;
- mit der Auszahlung an die betroffene Person oder an Dritte befasste Banken;
- Mitversicherte;
- Pensionskassen;
- Ausländische Behörden und Pensionskassen, soweit ein Datenaustausch auf Grund von Gesetzen erfolgt (zum Beispiel Lebendbescheinigungen, usw.)

12.1 DATENVERARBEITUNG FÜR ZWECKE DER VERWALTUNG UND SICHERHEIT DES SYSTEMS

Aufgrund der geltenden gesetzlichen Datensicherheitsbestimmungen werden eine Reihe von Daten für die Verwaltung und Sicherheit des Systems verarbeitet. Dies schließt automationsunterstützt erstellte und archivierte Textdokumente (wie zB Korrespondenz) in diesen Angelegenheiten mit ein. Ohne diese Datenverarbeitung ist ein sicherer Betrieb des Systems nicht möglich. Eine Reihe von Daten werden zur Erbringung von zum Beispiel Help-Desk-Diensten, Cloud-Diensten, etc. an einen Auftragsverarbeiter weitergegeben.

12.2 RECHTSGRUNDLAGE

In Österreich findet folgendes Datenschutzgesetz Anwendung:

- Datenschutzgesetz (DSG)
- Datenschutzgrundverordnung (EU) 2016/679

12.3 VERARBEITUNG FREIWILLIGER ANGABEN

Bewohner stimmen auf Grundlage dieses Datenschutzgesetzes ausdrücklich der Verwendung ihrer personenbezogenen Daten durch den Gemeindeverband zu, einschließlich der nachfolgenden:

1. Anfertigung, Hinterlegung und Verwendung des eigenen Lichtbildes in der Bewohnerdatenbank (CareCenter);
2. Anfertigung, Hinterlegung und Verwendung von Einzel- und Gruppenbildern bei Veranstaltungen, zur Dokumentation von Aktivitäten mit Bewohnern und öffentlicher Darstellung auf internen Monitoren;
3. Aushang des eigenen Namens am Türschild;
4. Verarbeitung des Religionsbekenntnisses, wenn seelsorgerische Betreuung gewünscht ist;
5. Verarbeitung von Notfallkontakten, soweit vom Bewohner gewünscht;
6. Datenverarbeitung im Zuge von Veranstaltungen, zum Beispiel Bewohnerausfüge, Weihnachtsfeiern, etc.
7. Zurverfügungstellung von personenbezogenen Daten an externe Dienstleister (zum Beispiel Fußpflege, Frisör);
8. Zustellung von Informationen mittels Newsletter per Mail;
9. Zustellung von Informationen mittels SMS;
10. Zustellung von Informations-SMS bei Posterhalt an Vertrauenspersonen oder Erwachsenenvertreter

12.4 SCHWEIGEPFLICHT

Bewohner stimmen auf Grundlage dieses Datenschutzgesetzes ausdrücklich zu, dass der behandelnde Arzt die für die Pflege und Betreuung erforderlichen Informationen den Mitarbeitern des Gemeindeverbandes Altenwohnheim Telfs und den Mitarbeitern seiner ärztlichen Ordination zur Verfügung stellt und die Mitarbeiter des Gemeindeverbandes Altenwohnheim Telfs wiederum dem behandelnden Arzt die für die Behandlung erforderlichen Informationen zur Verfügung stellen dürfen.

- Der Bewohner (Leistungsempfänger) entbindet insoweit die Mitarbeiter des Gemeindeverbandes Altenwohnheim Telfs, die behandelnden Ärzte und Therapeuten widerruflich von ihrer Schweigepflicht.

12.5 BEZUG VON MEDIKAMENTEN UND SONSTIGEN ARZNEIEN

Bewohner stimmen auf Grundlage dieses Datenschutzgesetzes ausdrücklich zu, dass die Apotheke personenbezogene Daten sowie Daten der bezogenen Arzneimittel (Dosierung, Einnahmezeitpunkt), Medizinprodukte, diätetischen Lebensmittel und Nahrungsergänzungsmittel sowie relevante medizinische Informationen in einer Patientendatei zur Erkennung und Lösung arzneimittel- und gesundheitsbezogener Probleme mit dem Ziel der Optimierung der Arzneimitteltherapie verarbeitet/speichert und in der Folge Mitarbeitern des Gemeindeverbandes Altenwohnheim Telfs wiederum die für die Behandlung erforderlichen Informationen zur Verfügung stellen darf.

- Der Bewohner (Leistungsempfänger) stimmt widerruflich zu, von Apotheken mit verschreibungspflichtigen und nichtverschreibungspflichten Medikamenten und Arzneiwaren versorgt zu werden, die ausschließlich mit dem Gemeindeverband Altenwohnheim Telfs zusammenarbeiten. Wahl und Wechsel der Apotheke obliegt dem Gemeindeverband Altenwohnheim Telfs.

12.6 RECHTE DES BEWOHNERS

Personenbezogene Daten werden auf nicht näher bestimmte Zeit gespeichert, solange die oben genannten Zwecke oder andere berechtigte Interessen bestehen. Bewohner haben hinsichtlich ihrer personenbezogenen Daten, die der Gemeindeverband speichert, das Recht auf Auskunft und Berichtigung unrichtiger Daten sowie um Löschung oder Einschränkung der Verarbeitung zu ersuchen. Bewohner können hinsichtlich bestimmter zukünftiger Verwendung ihrer personenbezogenen Daten ihre Einwilligung jederzeit widerrufen. Ein Widerruf hat zur Folge, dass Daten ab diesem Zeitpunkt zu dem widerrufenen Zweck nicht weiter verarbeitet werden, und somit entsprechende Rechte, Vorteile, etc. nicht mehr in Anspruch genommen werden können.

Falls ein Bewohner seine Einwilligung in die Verwendung seiner personenbezogenen Daten zurückzieht, mag der Gemeindeverband als übergeordneter Rechtsträger und Erhalter von Einrichtungen für Altenwohn- und Pflegeheime, Einrichtungen für seniorengerechtes Wohnen und Dienstleister für externe mildtätige Organisationen auf Grundlage seiner berechtigten Interessen zur Pflege und Verwaltung oder eines anderen im Datenschutzgesetz verankerten Rechtsgrundes berechtigt sein, einige dieser personenbezogenen Daten ohne eine solche Einwilligung weiter zu verwenden. Bewohner sind sich bewusst, dass sie das Recht haben, eine Beschwerde bei der Datenschutzbehörde einzureichen.

Der Gemeindeverband Altenwohnheim Telfs hat in Übereinstimmung mit dem Datenschutzgesetz verschiedene technische und organisatorische Sicherheitsmaßnahmen ergriffen, um personenbezogene Daten zu schützen. Bewohner sind sich darüber im Klaren, dass nur einer begrenzten Anzahl von autorisierten Personen zur Erfüllung der oben genannten Zwecke Zugriff auf ihre personenbezogenen Daten gewährt wird.

12.7 ANFRAGEN

Anfragen an den Datenschutzbeauftragten (siehe „Kontakt Datenschutzbeauftragter") können schriftlich, fernmündlich oder persönlich (bei ausreichender Identitätsfeststellung) gestellt werden.

12.8 ÄNDERUNG DER VERWENDUNG PERSONENBEZOGENER DATEN

Es kann sein, dass sich die Vorgehensweise des Gemeindeverbandes bezüglich Daten von Zeit zu Zeit ändern kann, zum Beispiel aufgrund Änderung, Wegfall oder Neueinführung von Prozessen oder aufgrund von Gesetzen oder Technik. Sollte es jemals notwendig werden, beschriebenen Inhalt zu ändern, werden diese Änderung auf online auf www.awh-telfs.at und mittels interner Kundmachung veröffentlicht, damit Bewohnern immer bewusst ist, welche Informationen seitens des Gemeindeverbandes erfasst und wie sie verwendet werden.

SICHERHEITSHINWEISE BENUTZER

13 EINLEITUNG

Durch den zunehmenden Einsatz und die daraus resultierende Abhängigkeit von der Informationstechnologie können Bedrohungen für den Gemeindeverband Altenwohnheim Telfs entstehen. Neben dem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität persönlicher, vertraulicher und weiterer sensibler Informationen durch IT-Fehlfunktionen und durch menschliches Fehlverhalten (bewusst oder unbewusst) kann das ganze System Ziel von Angriffen sein (von innen und außen).

14 VERANTWORTUNG

Jeder Benutzer von IT-Diensten ist verpflichtet, geltende, einschlägige Gesetze (Datenschutzgrundverordnung, Datenschutzanpassungsgesetz, Gesundheitstelematikgesetz etc.) und interne Regelungen zu beachten. Folgende Richtlinien sind zu beachten:

- Leitlinie zur Informationssicherheit
- Sicherheitsrichtlinie zur IT-Nutzung
- Sicherheitsrichtlinie zur Internetnutzung

Diese Sicherheitshinweise sind allen Mitarbeitern des Gemeindeverbandes Altenwohnheim Telfs verfügbar. Die Gesamtheit der enthaltenen Regelungen hat verbindlichen Charakter, so dass Verstöße gegen die Inhalte der Richtlinie zu arbeitsrechtlichen Konsequenzen führen können.

Alle Mitarbeiter sind im eigenen Interesse angehalten, an angebotenen Schulungen zu Programmnutzung und Sicherheitsmaßnahmen vor der Nutzung von IT-Diensten teilzunehmen.

Bei Fragen zur IT-Nutzung und zur Informationssicherheit stehen die Verwaltungsdirektion bzw. von ihr namhaft gemachte Mitarbeiter (zB Administratoren etc.) zur Verfügung.

15 ALLGEMEINE REGELUNGEN

Die Nutzung der erlaubten Dienste ist ausschließlich zu dienstlichen Zwecken und im ausdrücklich erlaubten Umfang zur Erledigung der Aufgaben gestattet.

Nur freigegebene Software darf verwendet werden.

Die Benutzung privater Hard- und Software zu dienstlichen Zwecken ist ohne Genehmigung nicht zulässig.

Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderungen an der Konfiguration etc.) sind nur durch den Administrator zulässig.

Informationsträger (Dokumente, Durchführungsnachweise etc.) mit vertraulichen Informationen sind in einem Shredder zu vernichten. Nicht mehr benötigte Datenträger (USB-Sticks, CD, DVD etc.) sind sicher zu löschen oder zu vernichten.

16 ZUTRITT UND ZUGANG

Es sind die Zugangsregelungen und die vergebenen Berechtigungen zu beachten. Das Ausprobieren von weiteren Diensten und Zugriffsrechten als den explizit Erlaubten ist verboten.

16.1 ALLGEMEINE ZUTRITTS- UND ZUGANGSREGELUNGEN

Der Arbeitsplatz ist „aufgeräumt" zu hinterlassen, so dass Unbefugte keinen Zugriff auf Informationen und IT-Anwendungen ermöglicht wird. Hierzu sind Räume falls möglich zu verschließen. IT-Geräte sind zum Schutz von unbefugten Personen mit einem passwortgeschützten Bildschirmschoner ausgestattet. Dieser muss bei Verlassen des Arbeitsplatzrechners oder nach 5 Minuten automatisch aktiviert werden.

In Bereichen mit Publikumsverkehr sind Monitore, Drucker und Faxgeräte so aufzustellen, dass das Risiko der Einsichtnahme Dritter möglichst ausgeschlossen wird.

Die Weitergabe von eigenen Benutzerkennungen und sonstigen Authentisierungshilfsmitteln an Dritte ist unzulässig.

Wenn der Verdacht besteht, dass die eigenen Zugangs- und Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist das Passwort umgehend zu ändern und der Administrator oder Datenschutzbeauftragte um Rat zu fragen.

16.2 PASSWORT-REGELN

Folgende Regeln sind zu beachten:

1. Passwörter sind nirgends zu notieren und niemandem mitzuteilen.
2. Das Passwort darf nur dem Benutzer bekannt sein.

3. Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.
4. Passwörter dürfen nicht leicht zu erraten sein. Vor- und Familiennamen oder Geburtstage sind beispielsweise nicht zur Bildung von Passwörtern geeignet. Es dürfen niemals Trivialpasswörter verwendet werden (z. B. 4711; 12345 oder andere nebeneinanderliegende Tasten).
5. Die Passwörter sind spätestens alle 90 Tage zu wechseln.
6. Sofern Gruppenpasswörter zwingend erforderlich sind, gilt: Gruppenpasswörter sind umgehend zu ändern, wenn die Zusammensetzung der Gruppe sich verändert. Gleiches gilt, wenn Passwörter unautorisierten Personen bekannt geworden sind.
7. Einmal genutzte Passwörter sind nicht wieder zu verwenden.
8. Benutzer haben den Empfang von Initial-Passwörtern immer zu bestätigen und müssen diese sofort wechseln.
9. Alle IT-Systeme sind zum Schutz vor unbefugten Personen mit einem passwortunterstützten Bildschirmschoner ausgestattet, dieser ist auch immer zu benutzen.

17 KOMMUNIKATIONSSPEZIFISCHE REGELUNGEN

Bei der Nutzung von Internet und E-Mail sind Virenschutzprogramme zu nutzen. Vom Administrator voreingestellte Konfigurationen dürfen nicht vom IT-Benutzer deaktiviert oder geändert werden.

Eine Weitergabe von vertraulichen Informationen bedarf der Zustimmung des Informationseigentümers. Beim Datenaustausch ist eine geeignete Versandart zu nutzen. Die Vertraulichkeit ist beim Versand zu gewährleisten:

- E-Mails und/oder deren Anhänge mit vertraulichem Inhalt, die extern versendet werden, sind zu verschlüsseln. Verschlüsselungspasswörter sind dem Empfänger gesondert zuzustellen, zum Beispiel mittels zweiter E-Mail, SMS oder mündlich (Zwei-Faktor-Authentifizierung).
- Es sind keine vertraulichen Nachrichten auf Anrufbeantworter zu sprechen.
- Die vom Faxgerät auf der Gegenseite vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wählfehlern die Übertragung unverzüglich abgebrochen werden kann.
- Beim Faxversand schutzbedürftiger Dokumente ist ein Sendezeitpunkt mit der Gegenseite abzustimmen bzw. alternativ sind voreingestellte Sendenummern zu programmieren und regelmäßig auf deren Aktualität zu

überprüfen (§ 27 Abs 10 Z 1 bis 3 und Abs 12 Z 1 bis 5 Gesundheitstelematikgesetz)

- Ausdrucke mit vertrauliche Informationen sind umgehend aus dem Drucker zu entfernen. Soweit möglich, ist eine Benutzerauthentifizierung vor Ausdruck einzurichten.

Des Weiteren ist die "Sicherheitsrichtlinie für die Internetnutzung zu beachten.

NOTFALLVORSORGE SENSIBILISIERUNG

18 DATENVERFÜGBARKEIT

Zur Sicherstellung der Verfügbarkeit ist folgendes sicherzustellen:

- Daten sind so aufzubewahren, dass sie problemlos wiedergefunden werden können.
- Um das Risiko eines Datenverlusts zu reduzieren, sind regelmäßig Datensicherungen durchzuführen.

19 VERSCHLÜSSELUNG

Grundsätzlich sind vertrauliche Informationen verschlüsselt zu speichern und zu übertragen. Mobile Datenträger sind sicher aufzubewahren. Das gleiche gilt für mobil genutzte IT-Systeme (Smartphones).

20 VIRENSCHUTZ

Durch einen Computer-Virenbefall ist die Verfügbarkeit ganzer IT-Systeme gefährdet. Viren können Festplatten unbrauchbar machen, so dass es zu Fristversäumnissen durch eine verzögerte Bearbeitung von Aufträgen aufgrund nicht funktionsfähiger IT-Systeme kommt oder es kommt zu erschwerten Bedingungen im Pflegeprozess aufgrund mangelnder Einsicht in die zu leistende Durchführungen. Des Weiteren können finanzielle Schäden durch den Verlust von Daten entstehen, da diese unter Umständen nur mit erheblichem Aufwand rekonstruiert werden können.

Ein Viren-Befall kann darüber hinaus zum Verlust der Integrität der Daten oder des IT-Systems führen. Dadurch können beispielsweise aufgrund einer falschen Datenbasis oder durch einen fehlerhaften Programmablauf fehlerhafte Ergebnisse generiert werden. Dies kann in gleicher Weise auch für komprimierte Dateien gelten, wenn das Viren-Schutzprogramm nicht geeignet ist.

Durch ein Trojanisches Pferd kann die Vertraulichkeit von Daten gefährdet werden, indem persönliche oder weitere vertrauliche Informationen „gestohlen“ werden. Der Verlust personenbezogener Daten oder Zugangsdaten kann zudem einen Verstoß gegen Datenschutzgesetze darstellen.

Wenn Computer-Viren an Kunden/Bürger oder Geschäftspartner weitergegeben werden, kann einen Imageschaden entstehen. Darüber hinaus können Imageschädigungen dadurch eintreten, dass Geschäftsprozesse oder einzelne Dienstleistungen nicht aufrechterhalten werden können und somit Verzögerungen entstehen.

20.1 INFEKTIONSWEGE

IT-Systeme können durch Viren auf verschiedene Weisen infiziert werden. Nachfolgend sind die häufigsten Infektionswege aufgezeigt. Die Reihenfolge der dargestellten Wege orientiert an der Wahrscheinlichkeit bzw. der Häufigkeit des Auftretens. Die größte Gefahr besteht in der Öffnung der internen Netze nach außen, so dass die Gefahren insbesondere aus externer E-Mail-Kommunikation, dem Internetzugang und dem Austausch von Datenträgern resultieren. Das interne Netz kann die Ausbreitung in der Institution „begünstigen".

E-MAIL

E-Mail dient immer öfter als Ersatz oder als Ergänzung zu anderen Bürokommunikationswegen. Mit Hilfe von Attachments (Anhängen) können Dateien effizient transportiert und E-Mail als Groupware-Lösung genutzt werden. Die angehängten Dateien können mit einem Virus infiziert sein und mittels E-Mail von außen in die Institution eingebracht und dort weiterverbreitet werden.

INTERNET

Doch auch durch die immer größere Verbreitung von aktiven Inhalten auf WWW-Seiten entsteht die Gefährdung der Viren-Infektion. Momentan ist hiermit Java, ActiveX und JavaScript gemeint, künftig könnten auch noch weitere Techniken hinzukommen.

Auch können über Plug-Ins aus dem Browser heraus andere Programme gestartet werden. Auch Dateien und Programme, die aus dem Internet heruntergeladen werden, können infiziert sein.

Gefährlich sind Schadprogramme, die sich über das Internet verbreiten und technisch so konstruiert sind, dass sie über eine nicht geschlossene Sicherheitslücke eines Programms (z. B. Browser oder Betriebssystem) direkt den Rechner infizieren.

INTERNES NETZ

Der interne Austausch von E-Mails und die Vernetzung der Rechner können die Ausbreitung eines Computer-Virus oder anderer Schadprogramme innerhalb der Institution herbeiführen. Sofern eine standortübergreifende Vernetzung vorhanden ist (zum Beispiel Virtual Private Network) wird hierdurch die Verbreitung auch auf andere Standorte ermöglicht.

Auch Rechner, die nur temporär in das Netz eingebunden sind, sind durch Viren bedroht. So können durch fehlende oder mangelhafte Anpassungen an Veränderungen des IT-Systems Sicherheitslücken entstehen.

WECHSELDATENTRÄGER

Über Wechseldatenträger (Disketten, CDs, DVDs, USB-Sticks etc.) können Dateien oder Programme mit Computer-Viren IT-Systeme infizieren.

20.2 ERFASSUNG DER BEDROHTEN IT-SYSTEME

Für ein effektives und effizientes Computer-Viren-Schutzkonzept sind die potentiell von Computer-Viren bedrohten IT-Systeme zu identifizieren, um angemessene Maßnahmen zu veranlassen. Es ist eine Übersicht aller IT-Systeme zu erstellen, die im Einsatz sind oder deren Einsatz geplant ist. Eine Auflistung aller IT-Systeme ist im Zuge der Verfahrensverzeichnisse nach DSGVO ohnehin zu erstellen und somit Stand der Dinge. Daraus können die IT-Systeme herausgefiltert werden, für die Viren eine Bedrohung darstellen oder über die Viren verteilt werden können.

Prinzipiell sind alle IT-Systeme sind durch Computer-Viren gefährdet. Man kann die IT-Systeme zum besseren Verständnis in vier Gruppen einteilen:

- E-Mail-Server/Gateway
- Laptops; weil sie teils im Intranet, teils mobil ohne Netzanschluss verwendet werden und dadurch besonderen Gefahren unterliegen.
- vernetzte Systeme (Client/Server)
- Stand-Alone-Systeme, die nicht ans Intranet angeschlossen sind und daher zum Beispiel eine Sonderrolle bei der Softwareverteilung einnehmen, die wesentlich aufwendiger ist.

SICHERHEITSMAßNAHMEN

- Es ist ein zentraler Virenschutz durch die Installation eines zentralen, residenten Computer-Viren-Schutzprogramms sicherzustellen. In der Regel genügt es, nur ausführbare Dateien, Skripte, Makrodateien etc. zu überprüfen. Ein vollständiges Durchsuchen aller Dateien empfiehlt

sich trotzdem in regelmäßigen Abständen (zum Beispiel vor einer Tages- oder Monatssicherung).

- Es dürfen grundsätzlich keine Rechner ohne residenten Virenschutz betrieben werden (dies schließt Laptops mit ein).
- Ein- und ausgehende E-Mails sind zentral am Gateway auf Computer-Viren hin zu prüfen.
- Die Internetnutzung ist sicher zu gestalten, indem aktive Inhalte möglichst vermieden werden. Aktive Inhalte sind nur auf separaten, nicht an das interne Netz angeschlossenen sogenannten Internet PCs zu ermöglichen.
- Dateien und Programme sind nur durch Berechtigte von vertrauenswürdigen Quellen herunterzuladen. Dies ist technisch zu unterstützen.
- Es ist auf den Servern eine Firewall zu installieren, die aktive Inhalte filtert. Gleiches gilt für Laptops, wenn sie auch mobil genutzt und ans Internet angeschlossen werden. Seiten mit aktiven Inhalten können vom Administrator einzeln zugelassen werden, wenn der Betreiber vertrauenswürdig ist und der Zugang aus dienstlichen Gründen erforderlich ist.
- Es ist für einen Dialerschutz zu sorgen, wenn Modems oder eine ISDN-Anlage/Karte genutzt werden. Kritische Nummernbereiche können zum Beispiel zentral an der ISDN-Anlage gesperrt werden. Auf Laptops können Dialer-Schutzprogramme installiert werden.
- Es ist eine Testumgebung festzulegen, um übersandte Dateien mit dem jeweiligen Anwendungsprogramm auf Makro-Viren zu untersuchen. Das automatische Ausführen von Makros ist in der Normalumgebung zu verhindern.
- Die Funktion des Browsers, heruntergeladene Daten automatisch zu öffnen, ist zu deaktivieren. Aktive Inhalte dürfen bei der Anzeige in E-Mail-Clients nicht automatisch ausgeführt werden (Vorschaufunktion deaktivieren).
- Innerhalb der Default-Einstellungen ist sicher zu stellen, dass Datei-Endungen nicht unterdrückt werden. Andernfalls wird es dem Nutzer erschwert, Dateiarten (zum Beispiel Textverarbeitungs- oder Anwendungsdateien) zu unterscheiden und Gefährdungspotentiale einzuschätzen.

BIOS-SICHERHEITSEINSTELLUNGEN

Für das BIOS sind Sicherheitsmaßnahmen erforderlich, weil nahezu alle technischen Viren-Schutzmaßnahmen erst nach Starten des Betriebssystems aktiv werden.

BIOS-Einstellungen sind dabei nur durch den autorisierten Administrator durchzuführen.

PASSWORTSCHUTZ

Es ist zu verhindern, dass Unbefugte die BIOS-Einstellungen ändern. Hierfür ist das Setup- oder Administrator-Passwort oder mindestens der Passwortschutz für die Zugriffe auf die BIOS-Einstellungen zu aktivieren.

BOOT-REIHENFOLGE

Die Boot-Reihenfolge beim Betriebssystemstart ist so umzustellen, dass generell zuerst von der Festplatte und dann erst von einem externen Medium (CD, USB-Sticks oder online Inhalte) gestartet wird. Dies schützt vor der Infektion mit Boot-Viren, falls versehentlich oder absichtlich ein bootfähiger Datenträger im Laufwerk vergessen wird.

20.3 SCHULUNG/SENSIBILISIERUNG

Die Benutzer werden vor der erstmaligen Nutzung der jeweiligen IT-Dienste hinsichtlich der Gefahren sensibilisiert und auf die Sicherheitsmaßnahmen geschult. Schulungsinhalte sind:

- Sensibilisierungsmaßnahmen: „Warum ist das IT-System so wichtig für mich und meinen Arbeitgeber?“
- Beschreibung der verschiedenen Computer-Viren
- Gefährdungspotential durch Computer-Viren „Welche Gefahren bestehen für mich und meinen Arbeitgeber durch Viren-Befall?“
- Schulung auf das Erkennen von Computer-Viren „Wie erkenne ich einen Viren-Befall?“
- Korrekte Nutzung des Computer-Viren-Schutzprogramms
- Nutzung des transienten Computer-Viren-Schutzprogramms „Wann und wie muss ich das Programm nutzen?“
- Nutzung des residenten Computer-Viren-Schutzprogramms „Verbot der Deaktivierung und der Änderung der Konfiguration“
- Korrekte Aktualisierung des Computer-Viren-Schutzprogramms
- Sichere Nutzung der sonstigen IT-Dienste
- Verhalten bei Auftreten eines Computer-Virus (Meldewege etc.)

Mitarbeiter müssen auf das Problem von Falschmeldungen über Viren hingewiesen und darüber informiert werden, was beim Empfang einer Meldung zu tun ist.

20.4 GLOSSAR

Laut Definition ist ein Computer-Virus eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Dies bedeutet, dass der Virus ein Wirtsprogramm benötigt. Diese Eigenschaft und seine Befähigung zur Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung „Virus".

Trojanische Pferde sind Programme, die neben scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computer-Anwender und ohne dessen Wissen ausführen. Im Gegensatz zu Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten.

Eine Variante eines Trojanischen Pferdes ist die sogenannte Backdoor. Mit einem derartigen Programm wird eine Hintertür geöffnet, die es einem Angreifer ermöglicht, von außen den Rechner fernzusteuern. Diese Programme werden unter anderem auch zu sogenannten Denial of Service (DoS) Angriffen verwendet.

Ein Computer-Wurm ist ein Programm, das funktionierende Programme oder Programmsequenzen von sich herstellt. Ein Wurm kann sich über ein Netz selbständig weiter verbreiten. Das Ziel dabei ist, in einem Netz so viele Computer wie möglich zu befallen. Würmer benötigen dabei zum Ausbreiten kein menschliches Zutun. Würmer verbreiten sich rasend schnell. Manche Würmer tragen zusätzlich noch ein Schadprogramm.

Nicht nur Computer-Viren und -Würmer erzeugen einen großen Schaden. Auch unerwünschte Massen-E-Mails verursachen einen wirtschaftlichen Schaden. Spam ist eine Bezeichnung für Massen-E-Mail, meist Werbesendungen, die im Internet verbreitet werden. Diese Werbung wird unaufgefordert an Millionen von E-Mail-Adressen versendet. Durch die Übertragung und Bearbeitung von Spam entstehen jährlich Kosten in Milliardenhöhe. Oft ist die Absenderadresse der Spam-Mail gefälscht, so dass der eigentliche Verursacher nur schwer ausfindig gemacht werden kann.

Eine besondere Variante von Massen-E-Mail sind elektronische Enten, sogenannte Hoaxes. Diese enthalten häufig „Virus-Meldungen", die vor einem „ganz neuen, gefährlichen" Virus warnen. Die Meldungen stimmen jedoch nicht, sie sollen nur ungeschulte Anwender verunsichern und zu schädlichen Aktionen wie dem Löschen von Dateien oder dem Verbreiten der Falschmeldung veranlassen.

Eine weitere Art von Schaden wird durch Dialer-Programme verursacht. Zum Teil versuchen betrügerische Anbieter, einen solchen Dialer unbemerkt zu installieren. Die Dialer gelangen durch Computer-Viren oder E-Mail-Anhänge auf den Rechner.

Einige der verschiedenen E-Mail-Würmer benutzen als Absenderadresse eine Adresse aus dem E-Mail-Adressbuch des Benutzers, dessen E-Mail-Programm sie gerade befallen haben. So erhalten die nächsten Opfer die E-Mail, die den Wurm enthält, mit einer bekannten Absenderadresse und sind so eher gefährdet, die E-Mail oder gar den infizierten Anhang zu öffnen.

21 VERHALTEN BEI SICHERHEITSVORFÄLLEN

Die folgenden Verhaltensregeln sind bei den verschiedenen Sicherheitsvorfällen einzuhalten:

Sobald ein Fehler oder ein anderes Problem auftritt, ist umgehend der Administrator zu benachrichtigen. Im Umgang mit Sicherheitsvorfällen sind Ehrlichkeit und Kooperationsbereitschaft besonders wichtig. Die Meldung von Sicherheitsvorfällen wird daher immer positiv gewertet!

Die Anweisungen der Verwaltungsdirektion und der Administratoren sind zu befolgen.

SICHERHEITSRICHTLINIE FÜR DIE INTERNET- UND E-MAIL-NUTZUNG

22 EINLEITUNG

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist in weiten Bereichen zur Selbstverständlichkeit geworden. Folge ist das Ausrüsten aller PCs im Gemeindeverband Altenwohnheim Telfs mit einem Internet-Zugang. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Mit Hilfe von Attachments (Anhängen) können Dateien effizient transportiert und E-Mail als Gruppen-Lösung genutzt werden.

Dadurch können jedoch weitere Bedrohungen für die Institution entstehen: Neben dem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener, vertraulicher und weiterer sensitiver Informationen während des Versands über das Internet ist auch die Sicherheit der intern abgespeicherten Informationen durch Angriffe von außen bedroht.

Diese Risiken müssen durch entsprechende – dem angestrebten Sicherheitsniveau angemessene – Maßnahmen auf ein tragbares Maß reduziert werden.

23 GELTUNGSBEREICH

Diese Richtlinie zur Nutzung von E-Mail- und Internet-Diensten gilt für alle Beschäftigten ohne Ausnahmen. Die Richtlinie umfasst Vorgaben zur Organisation, zur Administration und zur Nutzung von E-Mail- und Internetdiensten.

Die Regelungen haben verbindlichen Charakter, so dass Verstöße gegen die Inhalte der Richtlinie zu arbeitsrechtlichen Konsequenzen führen können.

Sie gilt für alle Betriebsteile, das heißt auch bei Tele(heim)arbeit oder bei mobiler Arbeit außerhalb der Geschäftsräume.

24 ORGANISATION

24.1 STELLEN

Die Internet- und E-Mail-Dienste sind durch fachkundiges Personal zu administrieren und zu warten. Auch für die Überprüfung der Sicherheit des Netzes sind die Administratoren zuständig.

Administratoren haben sich regelmäßig über sicherheitsrelevante Patches, Updates oder sonstige Informationen zu informieren und die notwendigen Maßnahmen zu ergreifen. Im Rahmen ihrer Tätigkeit arbeiten sie eng mit dem Datenschutzbeauftragten zusammen und unterstützen und informieren ihn.

24.2 SCHULUNGEN

Die IT-Benutzer sind vor der erstmaligen Nutzung von E-Mail- und Internet-Programmen zu schulen. Dabei sind Ihnen die aus der Nutzung der Internet- und E-Mailnutzung resultieren Gefahren und die entsprechenden Sicherheitsregelungen näher zu bringen.

24.3 ZUGRIFF

Der Zugriff auf Internet- und E-Mail-Dienste ist für jeden Mitarbeiter individuell geregelt.

25 KONFIGURATION

25.1 ALLGEMEINES

Die E-Mail- und Internet-Programme, die Mail- und Internet-Server sowie die Hardwarekomponenten sind durch die Administratoren möglichst so zu konfigurieren, dass ohne weiteres Zutun der IT-Benutzer optimale Sicherheit erreicht werden kann.

Änderungen an den Sicherheitseinstellungen durch die IT-Benutzer sind nicht gestattet.

25.2 SCHUTZ GEGEN COMPUTER-VIREN

Ein- und ausgehende E-Mails sind zentral am Gateway auf Computer-Viren hin zu prüfen.

Es ist für einen Schutz gegen Dialerprogramme zu sorgen.

Innerhalb der Default-Einstellungen ist sicher zu stellen, dass Datei-Endungen nicht unterdrückt werden. Andernfalls wird es dem Nutzer erschwert, Dateiarten zu unterscheiden und Gefährdungspotentiale einzuschätzen.

25.3 INTERNET-BROWSER UND E-MAIL-CLIENT

Es sind bei Browsern und E-Mail-Clients nur die Funktionen und Programme zu aktivieren, die zwingend benötigt werden. Die Zuteilung der verwendeten Programme und Dienste ist zu dokumentieren.

Cookies sind aus datenschutzrechtlichen Gründen zu unterdrücken oder regelmäßig zu löschen.

Wenn der Cache des Browsers genutzt wird, ist dieser regelmäßig (nach der Sitzung) zu löschen.

Die Funktion des Browsers, heruntergeladene Daten automatisch zu öffnen, ist zu deaktivieren. Aktive Inhalte dürfen bei der Anzeige in E-Mail-Clients nicht automatisch ausgeführt werden (Vorschaufunktion deaktivieren).

Von der Funktion automatischer Lesebestätigungen ist abzusehen, da dies unerwünschte E-Mail-Versender unterstützen kann (Spam).

Bei einer automatischen Weiterleitung von E-Mails ist die Vertraulichkeit zu wahren, indem sichergestellt wird, dass alle Empfänger die E-Mails auch lesen dürfen.

Die Funktion des Browsers ist zu deaktivieren, die das automatische Ausfüllen von Formularen auf Internetseiten durch abgespeicherte persönliche Informationen oder Passwörter ermöglicht.

Die Funktion des E-Mail-Clients, die Adresse eines E-Mail-Empfängers automatisch zu vervollständigen, sollte nicht verwendet werden (Nachrichten werden womöglich an falsche Empfänger versendet.).

26 NUTZUNG

26.1 PRIVATE UND DIENSTLICHE NUTZUNG

Beim dienstlichen Gebrauch ist darauf zu achten, dass geltende Gesetze (insbesondere das Urheberrecht bei Bildern) eingehalten werden.

Privater Gebrauch des Internets ist während der Dienstzeit gestattet, wird jedoch ausnahmslos protokolliert, dokumentiert und gegebenenfalls ausgewertet.

- Auch bei der E-Mail-Nutzung sind die üblichen Gepflogenheiten in der Kommunikation zu wahren. Alle nach außen gehenden E-Mails sind daher mit Absenderangabe (Voreingestellte Signatur am Ende jeder E-Mail) zu versehen.
- Beiträge in Internet-Newsgroups oder Diskussionsforen unterliegen den gleichen Regelungen wie sonstige öffentliche Meinungsbekundungen und Veröffentlichungen im Namen des Arbeitgebers und sind von der Verwaltungsdirektion vorab freizugeben.

26.2 ÜBERTRAGUNG SCHÜTZENSWERTER DATEN

Die Übertragung von vertraulichen Informationen an Externe mittels E-Mail ist ausschließlich in verschlüsselter Form zulässig. E-Mails dürfen nicht an externe Stellen übermittelt werden, wenn diese nicht in der Lage sind, verschlüsselte E-Mails zu lesen.

26.3 HERUNTERLADEN VON DATEIEN

Dateien und Programme sind nur durch Berechtigte von vertrauenswürdigen Quellen herunterzuladen.

26.4 E-MAIL-ADRESSEN

Mitarbeiter erhalten unter Umständen eine mitarbeiterspezifische E-Mail-Adresse. Diese sind ausschließlich der betrieblichen Nutzung vorbehalten, eine Privatnutzung ist ausgeschlossen. Personalisierte E-Mail-Adressen werden nach Ausscheiden des Dienstnehmers aus dem Gemeindeverband drei Monate bestehen bleiben; elektronische Postnachrichten werden dem logisch folgenden Mitarbeiter bzw. der Abteilung weitergeleitet.

Zusätzlich werden funktionsbezogene E-Mail-Adressen eingerichtet, die für dienstliche Angelegenheiten verwendet werden müssen. Auf der Internetseite sollten nach Möglichkeit nur funktionsbezogene E-Mail-Adressen genannt werden.

Es muss durch Vertretungsregeln gesichert werden, dass E-Mails im Abwesenheitsfall beantwortet werden. Diese Pflicht gilt insbesondere für funktionsbezogene E-Mail-Adressen.

Die Adressierung von E-Mails muss eindeutig erfolgen. Vorhandene Adressbücher und Verteilerlisten sind zu nutzen und müssen gepflegt werden. Verteilerlisten dürfen nicht externen zugänglich gemacht werden.

Sofern E-Mails an mehrere Empfänger versandt werden, sind nach Möglichkeit Verteilerlisten oder die „BCC-Option“ zu nutzen, so dass der Empfänger nicht die komplette Empfängerliste einsehen kann.

SICHERHEITSRICHTLINIE FÜR DIE IT-NUTZUNG

27 EINLEITUNG

In der Sicherheitsleitlinie wird die Bedeutung der Informationssicherheit für den Gemeindeverband Altenwohnheim Telfs dargelegt und die grundsätzliche Informationssicherheitsstrategie beschrieben. Die "Sicherheitsrichtlinie zur IT-Nutzung" leitet aus den Vorgaben der Sicherheitsleitlinie konkrete organisatorische und technische Anforderungen, die unabhängig von konkreten Produkten für alle Projekte und Prozesse gelten, ab. Diese Anforderungen sind die Grundlage für die Standard-Sicherheitsmaßnahmen und legen das angestrebte Sicherheitsniveau fest.

28 GELTUNGSBEREICH

Diese Richtlinie gilt verbindlich für alle Mitarbeiter ohne Ausnahme für die Nutzung dienstlicher IT. Verstöße gegen die Inhalte der Richtlinie können zu arbeitsrechtlichen Konsequenzen führen.

Auch beim Abschluss von Verträgen mit externen Dienstleistern ist darauf zu achten, dass die Vorgaben dieser Richtlinie beachtet werden.

Für die Pflege und Weiterentwicklung der Richtlinie ist der Administrator zuständig.

29 UMGANG MIT INFORMATIONEN

Für Geschäftsprozesse, Informationen, Anwendungen und IT-Systeme werden Verantwortliche („Eigentümer") festgelegt.

Alle Informationen müssen anhand ihres Schutzbedarfs klassifiziert werden.

Ziel ist es, Informationen entsprechend ihres Schutzbedarfs zu verarbeiten. Nur wenn IT-Benutzer und Verantwortliche wissen, welche Informationen besonders schutzbedürftig sind, können sie diese auch angemessen schützen. Aus dem Schutzbedarf der Informationen leitet sich letztendlich der Schutzbedarf der IT-Systeme ab, auf denen die Informationen verarbeitet werden.

Die Verantwortlichen legen fest, wer unter welchen Bedingungen auf Informationen zugreifen bzw. Anwendungen und IT-Systeme nutzen darf.

30 RECHTSVORSCHRIFTEN

Beim Einsatz der IT sind einschlägige Gesetze (DSGVO, Urheberrechtsgesetze etc.), Vorschriften und (interne) Regelungen einzuhalten.

Dies gilt insbesondere für die

- Datenschutzrichtlinie
- Datenschutzerklärung
- Richtlinie zur Verwendung von Cookies und ähnlichen Technologien
- Richtlinie hinsichtlich der Verwendung personenbezogener Daten
- Richtlinie hinsichtlich der Verwendung personenbezogener Daten - Dienstnehmer
- Richtlinie hinsichtlich der Verwendung personenbezogener Daten - Bewohner

31 ORGANISATION

31.1 STELLEN

Die organisationsweiten IT-Dienste sind durch die bestellten Administratoren zu administrieren und zu warten.

Der Datenschutzbeauftragte ist zur Erreichung der Informationssicherheitsziele in alle IT-Projekte frühzeitig einzubeziehen.

Die Administratoren unterstützen und beraten die IT-Benutzer.

Neue Mitarbeiter und Mitarbeiter, die in eine vertrauensvollere Position wechseln, sind auf ihre Vertrauenswürdigkeit und Qualifikation zu überprüfen.

31.2 SCHULUNG UND SENSIBILISIERUNG

IT-Benutzer und Administratoren sind vor der erstmaligen Nutzung der jeweiligen IT-Dienste zu schulen. Schulungsinhalte sind:

- Handhabung der jeweilig verwendeten IT-Dienste
- Inhalte der Sicherheitsleitlinie und der Sicherheitsrichtlinien zu verschiedenen Themen (Notfallvorsorge, Datensicherung etc.) sowie die umzusetzenden Sicherheitsmaßnahmen
- Sensibilisierungsmaßnahmen („Warum ist Informationssicherheit so wichtig für mich und meinen Dienstgeber?“)
- rechtliche Rahmenbedingungen

31.3 VERTRETUNGSREGELN

Für den Fall der Abwesenheit (Dienstreise, Urlaub, Krankheit) sind Vertreter benannt.

32 VERWALTUNG UND NUTZUNG VON IT-DIENSTEN

32.1 BESCHAFFUNG

Für die Beschaffung von Soft- und Hardware ist als Grundlage ein Anforderungsprofil erstellt worden, das neben fachlichen und technischen Ausstattungsmerkmalen sowie ergonomischen Aspekten auch Anforderungen an die Informationssicherheit beschreibt. Nach Möglichkeit wurden Arbeitsplätze standardisiert ausgestattet, um Verwaltung und Administration zu erleichtern.

Es wurde beachtet, dass die Integration in die vorhandene oder geplante, informationstechnische Infrastruktur gewährleistet ist. Für den jeweiligen Bereich geltenden Normen (ISO, ÖNORM, DIN).

Im Rahmen der Kommunikation und Archivierung wurden bevorzugt Programme beschafft, die eine Verschlüsselung ermöglichen.

32.2 EINSATZ

Vor dem Einsatz ist neue Soft- und Hardware zu testen. Dabei sollten nach Möglichkeit Testsystem und Produktivbetrieb getrennt werden.

Nicht freigegebene Hard- und Software ist nicht einzusetzen.

Softwareänderungen machen eine erneute Freigabe erforderlich.

Die IT-Dienste sind nur für die festgelegten Aufgaben zu nutzen. Die Nutzung für private Zwecke ist nicht zulässig. Der Anschluss privater Hardware an dienstliche IT-Systeme und die Nutzung privater Software zu dienstlichen Zwecken ist nur mit Genehmigung durch die Verwaltungsdirektion zulässig.

Die Nutzung aller nicht ausdrücklich erlaubten Dienste ist technisch zu unterdrücken. Dienste und Berechtigungen, die nicht oder nicht mehr benötigt werden, sind durch den Administrator zu deaktivieren.

Soft- und Hardware sind durch die Administratoren möglichst so zu konfigurieren, dass ohne weiteres Zutun der IT-Benutzer optimale Sicherheit erreicht werden kann. Default-Einstellungen sind zu überprüfen und Default-Passwörter zu ändern. Es sind angemessene Sicherheitsprodukte einzusetzen.

32.3 WARTUNG

Die mit Pflege und Wartung verbundenen Maßnahmen sind nach Art, Inhalt und Zeitpunkt zu protokollieren.

Der Zugriff auf Daten durch Wartungstechniker ist soweit wie möglich zu vermeiden. Die eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen. Bei Arbeiten an organisationsweiten IT-Diensten mit sensiblen Informationen ist das Vier-Augen-Prinzip anzuwenden.

Arbeiten am System sind gegenüber den betroffenen Mitarbeitern rechtzeitig anzukündigen.

Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten IT-Systeme zu überprüfen.

32.4 REVISION

Alle Maßnahmen an IT-Diensten sind revisionssicher zu dokumentieren. Administratortätigkeiten sind zu protokollieren.

Es ist eine regelmäßige Kontrolle der Funktionalität der IT-Dienste, der Informationssicherheit und der Einhaltung der Richtlinien durchzuführen.

Sicherheitsrelevante Ereignisse und Zugriffe auf kritische Bereiche sind automatisch zu protokollieren und durch Administratoren regelmäßig zu überprüfen.

Bei der Protokollierung sind Datenschutzaspekte zu beachten. Ermöglicht die Auswertung der Daten eine Verhaltens- und Leistungskontrolle, ist sie mitbestimmungspflichtig. Eine Information an den Datenschutzbeauftragten hat zu erfolgen.

32.5 WEITERGABEREGELUNGEN

Bei der Weitergabe von Informationen ist ihr Schutzbedarf zu beachten und eine geeignete Versandart zu wählen. Vertrauliche Informationen oder Datenträger (USB, CD, DVD, SSD etc.) mit vertraulichen Informationen dürfen erst dann versendet werden, wenn die Vertraulichkeit beim Versand gewährleistet ist. Der Empfänger der Informationen ist zur vertraulichen Behandlung zu verpflichten.

Wird eine Hardware außer Haus gegeben, sind, sofern dies möglich ist, alle vertraulichen Informationen, die sich in Datenspeichern befinden, vorher si-

cher zu löschen. Ist dies nicht möglich, so ist der Vertragspartner auf Geheimhaltung zu verpflichten. Die Übergabe bzw. der Transport ist sicher zu gestalten.

32.6 ENTSORGUNG

Belege und Druckausgaben, die vertrauliche Informationen beinhalten, müssen getrennt vom übrigen Abfall entsorgt werden.

Elektronische Datenträger mit vertraulichen Informationen, die nicht weiter benötigt werden, sind vor der Entsorgung sicher zu löschen.

Sofern keine sichere Entsorgung durchgeführt werden kann, ist mit der Entsorgung ein externes Unternehmen zu beauftragen. Ein Protokoll der positiven Vernichtung übergebener Datenträger ist eigens aufzubewahren.

33 SICHERHEITSMAßNAHMEN

33.1 ALLGEMEINES

Durch wirksame Maßnahmen ist zu gewährleisten, dass die Sicherungsziele realisiert werden und ihre Einhaltung kontrolliert werden können.

Alle IT-Systeme und Anwendungen sind sorgfältig zu konfigurieren und zu sichern. Wesentliche Punkte sind nachvollziehbar zu dokumentieren.

Die Gebäude und Räume sind gegen fahrlässig, vorsätzlich oder durch höhere Gewalt herbeigeführte Störungen zu schützen (zB Brandschutz).

Für Tele(heim)arbeit und mobile Arbeit sind Regelungen zu erstellen.

33.2 ZUTRITTS- UND ZUGANGSREGELUNGEN

Der Zutritt zu den Räumlichkeiten bzw. der Zugang zu den IT-Diensten ist gegen Unbefugte zu schützen und zu kontrollieren. Hierbei sind verschiedene Rollen festzulegen.

Für jeden Mitarbeiter sind Berechtigungen für den Zutritt zu Räumlichkeiten, den Zugang zu IT-Diensten und den Zugriff auf Informationen festzulegen. Alle Rechte sind restriktiv zu vergeben und zu dokumentieren. Hierbei sind die zwingenden dienstlichen Erfordernisse zugrunde zu legen.

Die Authentisierung der Zugangsberechtigung ist durch Passwörter sicherzustellen. Es sind Passwortregeln zu erstellen. Diese werden allen Betroffenen durch *Sicherheitshinweise für Benutzer* mitgeteilt.

Der Zugang der Administratoren ist speziell zu sichern. Die Passwörter der Administratoren sind sicher zu verwahren. Den Stellvertretern ist eine eigene Administratoren-Kennung zuzuteilen.

Besucher, Handwerker und andere fremde Personen dürfen sich nicht frei und unkontrolliert im Gebäude bewegen.

Bereiche, in denen hoch vertrauliche Informationen verarbeitet werden, sind besonders zu sichern. Nur berechtigte, namentlich benannte Personen haben Zutritt zu diesen Bereichen.

IT-Systeme im Eingangs- und Empfangsbereich sind so zu sichern, dass Unbefugte keinen unbeobachteten Zugriff nehmen und Informationen nicht eingesehen werden können.

33.3 VERSCHLÜSSELUNG

Vertrauliche und andere sicherheitsrelevante Daten sind verschlüsselt zu speichern. Sofern im Klartext gespeichert wird, ist beim Netzzugriff die Übertragung zu verschlüsseln.

Zur Verschlüsselung ist IT-Benutzern auf Antrag ein Programm zur Verfügung zu stellen. Berechtigten IT-Benutzern sind ein öffentlicher und ein geheimer Schlüssel zur Verfügung zu stellen.

33.4 SCHADSOFTWARE

Es ist ein Viren-Schutzprogramm zu installieren. Es sind regelmäßig Updates durchzuführen und die Viren-Signaturen zu aktualisieren.

Der Gemeindeverband Altenwohnheim Telfs verpflichtet sich, ob seiner Größe und Verarbeitung personenbezogener Daten besonderer Kategorien, ein Virenschutzkonzept zu erstellen.

33.5 DATENSICHERUNG/ARCHIVIERUNG

Es sind regelmäßig Datensicherungen durchzuführen. Die IT-Benutzer sind dabei zu unterstützen.

Informationen sind einheitlich und dokumentiert aufzubewahren, so dass sie problemlos wieder aufgefunden werden können (Datenschutzkonzept).

Sicherungskopien sind in gesicherten Behältnissen in einem anderen Brandabschnitt aufzubewahren. Die Datenträger sind eindeutig zu kennzeichnen.

Die Archivierung ist ein Teil des Dokumentenmanagement-Prozesses und dient der dauerhaften und unveränderbaren Speicherung von elektronischen

Dokumenten und anderen Daten. Innerhalb eines Archivierungssystems aufbewahrte Daten sind konsistent so zu indizieren, dass sie eindeutig und schnell gefunden werden können. Die Speicherressourcen sind zu überwachen. Durch regelmäßig Funktions- und Recovery-Tests ist einem Datenverlust auf den Datenträgern entgegen zu wirken (Stress-Test).

33.6 NOTFALLVORSORGE

Alle Probleme, die IT-Dienste betreffen, müssen der Verwaltungsdirektion und den Administratoren gemeldet werden.

Verhaltensregeln und Handlungsanweisungen für relevante Schadensereignisse sind in Form eines Notfallvorsorgekonzeptes allen Mitarbeitern zugänglich.

34 REGELUNGEN FÜR SPEZIFISCHE IT-DIENSTE

34.1 KOMMUNIKATIONSSPEZIFISCHE REGELUNGEN

Informationen, die elektronisch übermittelt werden (Fax, Telefonanlage, Internet etc.), sind zu schützen. Hierbei sind die technikspezifischen Sicherheitsprobleme zu berücksichtigen.

34.2 FERNZUGRIFF AUF DAS INTERNE NETZ

Generell ist der „Zugriff vor Ort“ dem „Fernzugriff“ vorzuziehen.

Eine externe Anbindung an das interne Netz ist speziell zu regeln. Sofern möglich, ist der Fernzugriff auf ein isoliertes Netz zu beschränken. Der Fernzugriff ist sicher zu konfigurieren.

Für besonders sensible Bereiche ist entweder ein Fernzugriff auszuschließen oder auf Notfälle zu beschränken. Der Notfall und die Verfahrensweise während des Notfalls ist genau zu definieren.

DATENSCHUTZERKLÄRUNG (WWW.AWH-TELFS.AT)

35 EINLEITUNG

WICHTIG: DURCH NUTZUNG UNSERER WEBSITE UND/ODER EINGABE PERSONENBEZOGENER DATEN GIBT DER NUTZER SEINE AUSDRÜCKLICHE EINWILLIGUNG, DASS WIR ALLE UNS ZUR VERFÜGUNG GESTELLTEN PERSONENBEZOGENEN DATEN AUF DIE WEISE UND ZU DEN ZWECKEN VERARBEITEN KÖNNEN WIE IN DER FOLGENDEN DATENSCHUTZERKLÄRUNG BESCHRIEBEN UND IN ÜBEREINSTIMMUNG MIT DEN EINSCHLÄGIGEN DATENSCHUTZGESETZEN UND -VORSCHRIFTEN.

35.1 BEACHTUNG DER PERSÖNLICHKEITSRECHTE DES NUTZERS

Wir verpflichten uns, die Persönlichkeitsrechte des Nutzers zu schützen und zu respektieren. Diese Datenschutzerklärung steckt den Rahmen ab, in dem wir personenbezogene Daten, die wir vom Nutzer erheben oder die dieser uns zur Verfügung stellt, auf unserer Website verarbeiten. Wir bewahren bestimmte grundlegende Informationen auf, wenn der Nutzer unsere Website besucht, und anerkennen die Wichtigkeit, diese Informationen sicher zu verwahren und den Nutzer wissen zu lassen, was wir damit tun werden. Der Nutzer kann sich dazu entscheiden, uns Informationen zur Verfügung zu stellen, die als personenbezogene Daten anzusehen sind. Der Begriff „personenbezogene Daten“, wie er in dieser Datenschutzerklärung verwendet wird, bezieht sich auf Informationen wie Name, E-Mail-Adresse, Postanschrift, Telefonnummer oder andere Daten, die dazu verwendet werden können, den Nutzer zu identifizieren. Es ist nicht erforderlich, personenbezogene Daten zur Verfügung zu stellen, um in den öffentlichen Bereichen dieser Website zu surfen.

35.2 INFORMATIONEN ÜBER DEN VERANTWORTLICHEN

Diese Website gehört dem Gemeindeverband Altenwohnheim Telfs, einer Körperschaft öffentlichen Rechts mit Sitz in 6410 Telfs, die die Aufgabe der Pflege und Betreuung von Menschen unterstützt. Wer sich freiwillig entscheidet, personenbezogene Daten zur Verfügung zu stellen, willigt dadurch in

diese Datenschutzerklärung ein sowie in die Speicherung seiner Daten auf Servern der Europäischen Union.

Verantwortlich für die Verarbeitung ist der Gemeindeverband Altenwohnheim Telfs als Körperschaft öffentlichen Rechts, vertreten durch den gewählten Verbandsobmann Bgm. Christian Härting, erreichbar unter folgenden Kontaktdaten: Wiesenweg 4+6, 6410 Telfs, info@awh-telfs.at, +43.(0)5262.62145.0.

35.3 DATENSICHERHEIT UND VERTRAULICHKEIT

Wir nehmen die Sicherheit und Vertraulichkeit der personenbezogenen Daten der Nutzer sehr ernst. Wir verwenden moderne Datenspeicherungs- und Sicherheitstechniken, um die personenbezogenen Daten des Nutzers vor unbefugtem Zugriff, unsachgemäßer Verwendung oder Offenlegung, nicht autorisierter Änderung, unrechtmäßiger Vernichtung oder versehentlichem Verlust zu schützen. Alle Auftragsverarbeiter von personenbezogenen Daten und alle Dritten, die wir mit der Verarbeitung der personenbezogenen Informationen des Nutzers beauftragen, sind verpflichtet, die Vertraulichkeit der Informationen des Nutzers zu wahren. Wir bewahren personenbezogene Daten des Nutzers nur so lange auf, wie dies vernünftigerweise erforderlich ist für die Zwecke, für die sie erfasst wurden, oder um anwendbaren gesetzlichen Berichtspflichten oder Aufbewahrungspflichten von Dokumenten zu entsprechen.

Wir nutzen Computersysteme mit beschränktem Zugang, die sich in Räumlichkeiten befinden, in denen physische, elektronische und verfahrensmäßige Maßnahmen die Vertraulichkeit und Sicherheit der Informationen schützen, die uns übermittelt werden. Wir halten uns an strenge Sicherheitsstandards, um jeglichen unbefugten Zugang zu verhindern.

35.4 DRITTANBIETER

Gelegentlich enthält diese Website Links auf die Seiten eines Drittanbieters, den wir beauftragt haben, für uns Dienstleistungen zu erbringen (zum Beispiel beim Ausfüllen von Online-Formularen). Wann immer der Nutzer auf eine Seite eines Drittanbieters gelangt, ist dies an einem veränderten Aussehen sowie an einer Änderung der Adressleiste des Browsers zu erkennen. Zum Zeitpunkt der Auswahl von Drittanbietern und regelmäßig danach prüfen wir deren Datenschutzrichtlinien um sicherzustellen, dass sie die gleichen Standards haben wie wir. Bei Fragen zu Richtlinien eines Drittanbieters siehe die Angaben auf dessen Seiten.

35.5 MITTEILUNG VON ÄNDERUNGEN DIESER DATENSCHUTZERKLÄRUNG

Wir verbessern diese Website ständig und fügen neue Funktionalitäten hinzu und verbessern und ergänzen unser bestehendes Angebot. Aufgrund dieser fortlaufenden Änderungen sowie Gesetzesänderungen und technologischer Weiterentwicklungen werden sich unsere Vorgehensweisen mit Daten von Zeit zu Zeit ändern. Wenn es notwendig wird, unsere Datenschutzerklärung zu ändern, werden wir die Änderungen auf dieser Seite veröffentlichen, damit den Nutzern immer bewusst ist, welche Informationen wir erfassen und wie wir sie verwenden.

35.6 AKTIVES SCRIPTING ODER JAVASCRIPT

Scripting wird verwendet, um die Funktionalität unserer Website zu verbessern. Scripting-Technologien ermöglichen es der Website, dem Nutzer schneller zu antworten. Scripting wird von der Website nie dazu gebraucht, auf dem Computer des Nutzers Programme zu installieren, noch dazu, unerlaubte Informationen über den Nutzer zu sammeln.

Aktives Scripting oder JavaScript muss im Browser aktiviert sein, damit bestimmte Teile der Website korrekt funktionieren. Bei den meisten Browsern kann diese Funktion für bestimmte Websites aktiviert oder deaktiviert werden. Über die Hilfefunktion des Browsers ist zu erfahren, wie das Scripting für ausgewählte Websites aktiviert wird.

RICHTLINIE ZUR VERWENDUNG VON COOKIES ODER ÄHNLICHEN TECHNOLOGIEN

36 EINLEITUNG

Wie die meisten Websites speichert auch diese Website beim Besuch möglicherweise eine kleine Menge Daten auf dem Mobiltelefon, Tablet oder der Computerfestplatte des Nutzers unter Verwendung von „Cookies", „Web Beacons" und ähnlichen Technologien. Der Gebrauch des Begriffs „Cookies" in dieser Richtlinie ist weit gefasst und umfasst auch ähnliche Technologien wie „localStorage". Cookies helfen dabei, dass diese Website funktioniert, und liefern uns Informationen darüber, wie Nutzer mit unserer Website interagieren. Wir verwenden diese Informationen, um unsere Website zu verbessern. Wir versuchen nicht, einzelne Besucher zu identifizieren, sofern sie nicht von sich aus ihre Kontaktdaten durch ein Formular oder eine Bewerbung auf der Website übermitteln.

36.1 COOKIES

Es gibt verschiedene Arten von Cookies, die unterschiedliche Funktionen erfüllen, um grundsätzlich das Nutzungserlebnis auf der Website zu verbessern. Wir verwenden möglicherweise Cookies, um zu erfahren, ob der Nutzer schon zuvor die Website besucht hat, oder um Präferenzen des Nutzers beim Gebrauch der Website zu speichern. Wir nutzen Cookies nicht für Werbezwecke.

Die Arten von Cookies auf dieser Website können in folgende drei Kategorien eingeordnet werden:

1. Unbedingt notwendige Cookies. Diese sind unerlässlich, um dem Nutzer die Verwendung bestimmter Funktionen der Website zu ermöglichen, wie z. B. den Login oder das Absenden von Formularen auf der Website. Ohne diese Cookies können vom Nutzer gewünschte Dienste, nicht zur Verfügung gestellt werden. Davon umfasst sind auch Cookies, die es uns erlauben, Dienste zur Verfügung zu stellen, die der Nutzer während der Browsersitzung ausdrücklich erbeten hat. Diese Cookies sammeln über den Nutzer keine Informationen, die für

Werbezwecke genutzt werden könnten, oder die abspeichern, wo man sich im Internet aufgehalten hat.

2. Cookies für die Funktionsfähigkeit — Diese werden verwendet, damit die Website Auswahlentscheidungen zur Verfügung stellen kann, um das Nutzungserlebnis zu verbessern.
3. Analytische Cookies — Diese werden verwendet, um Informationen darüber zu sammeln, wie Besucher diese Website verwenden, beispielsweise die Anzahl von Besuchen auf dieser Website oder die durchschnittliche Verweildauer. Diese Informationen werden ausschließlich dazu verwendet, die Funktionalität dieser Website zu verbessern.

Einige Cookies werden von unserer Website selbst gesetzt („first-party cookies"). Andere werden von einer anderen Domain gesetzt („third-party cookies"). Wir verwenden ausschließlich „first-party cookies", mit Ausnahme der „third-party cookies" in Verbindung mit Google Analytics.

Diese Website benutzt Google Analytics, einen Webanalysedienst der Google Inc. („Google"). Google Analytics verwendet sog. „Cookies", Textdateien, die auf dem Computer gespeichert werden und die eine Analyse der Benutzung der Website ermöglichen. Die durch den Cookie erzeugten Informationen über Ihre Benutzung dieser Website umfassen (1) zwei Bytes der IP-Adresse des aufrufenden Systems des Nutzers, (2) die aufgerufene Webseite, (3) die Website, von der der Nutzer auf die aufgerufene Webseite gelangt ist (Referrer), (4) die Unterseiten, die von der aufgerufenen Webseite aus aufgerufen werden, (5) die Verweildauer auf der Webseite und (6) die Häufigkeit des Aufrufs der Webseite und werden an einen Server von Google in den USA übertragen und dort gespeichert.

Google wird diese Informationen benutzen, um Ihre Nutzung der Website auszuwerten, um Reports über die Websiteaktivitäten für die Websitebetreiber zusammenzustellen und um weitere mit der Websitenutzung und der Internetnutzung verbundene Dienstleistungen zu erbringen. Auch wird Google diese Informationen gegebenenfalls an Dritte übertragen, sofern dies gesetzlich vorgeschrieben oder soweit Dritte diese Daten im Auftrag von Google verarbeiten. Google wird in keinem Fall Ihre IP-Adresse mit anderen Daten von Google in Verbindung bringen. Die Google-Datenschutzerklärung findet sich unter https://www.google.com/intl/de/policies/privacy/.

36.2 WEB BEACONS

Die Seiten unserer Website können kleine elektronische Dateien enthalten, bekannt als „Web Beacons“, die uns eine Aufzeichnung von Aktivitäten ermöglichen, wie z. B. wann der Nutzer eine bestimmte Seite besucht. Web Beacons werden dazu verwendet, die Verwendung dieser Website nachzuvollziehen und ihre Leistungsfähigkeit zu überwachen.

36.3 VERWENDUNG VON IP-ADRESSEN

Eine IP-Adresse ist eine Zahlenfolge, die den Computer des Nutzers im Internet identifiziert. Wir verwenden die IP-Adresse und den Browsertyp des Nutzers, um Nutzungsverläufe analysieren zu können und Probleme dieser Website zu diagnostizieren und um die Dienste, die wir zur Verfügung stellen, zu verbessern. Ohne zusätzliche Informationen identifiziert die IP-Adresse jedoch nicht den Nutzer.

36.4 ENTSCHEIDUNGEN DES NUTZERS

Beim Aufrufen dieser Website wurden unsere Cookies an den Webbrowser des Nutzers gesendet und auf seinem Computer gespeichert. Durch die Verwendung unserer Website stimmt der Nutzer der Verwendung von Cookies und ähnlichen Technologien zu. Wenn der Nutzer sie entfernen möchte, ist dies über die Einstellungen in seinem Browser möglich; ohne Cookies kann der Nutzer allerdings möglicherweise nicht die volle Funktionalität unserer Website in Anspruch nehmen. Wie Cookies gelöscht werden, variiert von Browser zu Browser. Die Hilfefunktion des Browsers sollte eine ausführliche Anleitung dazu enthalten.

NOTFALLVORSORGEKONZEPT

37 EINLEITUNG

37.1 NOTFALL-DEFINITION

Der Ausfall eines IT-Systems in Folge eines Sicherheitsvorfalls kann einen großen Schaden nach sich ziehen. So kann der Ausfall eines zentralen IT-Systems zu einem Ausfall des gesamten IT-Betriebs führen. Auch der Ausfall von Komponenten der technischen Infrastruktur, beispielsweise Klimaanlage oder Stromversorgung, kann zu Störungen des IT-Betriebs führen.

Technisches Versagen muss nicht zwingend die Ursache für den Ausfall von IT-Systemen sein. Ausfälle werden oft durch menschliches Fehlverhalten (zB fahrlässige Zerstörung von Gerät oder Daten) oder vorsätzliche Handlungen (zB Diebstahl, Sabotage, Viren-Angriff) verursacht. Auch durch höhere Gewalt (wie Feuer, Blitzschlag oder Hochwasser) können hohe Schäden eintreten.

Ein Sicherheitsvorfall stellt jedoch nicht zwangsläufig einen Notfall dar.

Für einen Notfall gilt die folgende Definition:

Ein Notfall tritt ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit nicht möglich ist ***und*** *sich daraus ein untragbarer Schaden ergibt.*

37.2 ZIELSETZUNG EINES NOTFALLVORSORGEKONZEPTS

Um größere Schäden zu begrenzen beziehungsweise diesen vorzusorgen, ist eine zügige und effiziente Behandlung von Sicherheitsvorfällen, die zum Ausfall von IT-Systemen führen, notwendig.

Ein Notfallvorsorgekonzept hat zum Ziel, die Geschäftstätigkeit während eines Ausfalls eines IT-Systems oder einer IT-Anwendung aufrechtzuerhalten und sicherzustellen (Business Continuity) sowie die Betriebsfähigkeit innerhalb einer tolerierbaren Zeitspanne wiederherzustellen (Business Recovery).

Dabei sind nicht nur die technischen Maßnahmen zum Wiederanlauf zu beachten. Besonders wichtig ist die Planung im Vorfeld, um Notfälle zu verhindern oder zumindest die Auswirkungen begrenzen zu können. Zur Vorberei-

tung gehören die Dokumentation von Verfahren und Maßnahmen sowie organisatorische Regelungen. Im Notfall muss es zum Beispiel Verantwortliche mit klaren Kompetenzen geben.

Zu einer guten Vorbereitung gehören ebenso Notfallschulungen und -übungen sowie eine stetige Pflege und Aktualisierung des Notfallvorsorgekonzeptes. Ein Notfallvorsorgekonzept beschreibt, welche Maßnahmen zur Vorbereitung auf Notfälle unternommen werden und was im Notfall zu tun ist.

38 VERANTWORTLICHE PERSONEN

Ein "Notfall" sollte formal durch einen „Notfall-Verantwortlichen“ ausgerufen werden, da schnelle Entscheidungen unabhängig von Hierarchieebenen getroffen und Mitarbeiter vielleicht außerhalb der normalen Arbeitszeit verständigt werden müssen. Auch könnten Maßnahmen, die vom normalen Arbeitsablauf abweichen und Sonderberechtigungen erfordern, notwendig werden.

In Notfällen müssen unter Umständen Beschränkungen und Sicherheitsvorkehrungen außer Kraft gesetzt werden, um ein Problem schneller lösen zu können.

In den Notfallplänen muss daher festgelegt werden, welche Aufgaben einzelne Personen im Notfall übernehmen und welche Rechte sie haben. Die beteiligten Personen und Organisationseinheiten sind dann im Notfall befugt, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen.

Anhang A enthält eine taxative Aufzählung der verschiedenen Rollen.

39 VERHALTEN IN NOTFÄLLEN

39.1 ALLGEMEINE REGELN FÜR ALLE MITARBEITER

Folgende Verhaltensregeln gelten allgemein für alle Mitarbeiter:

- Alle Mitarbeiter haben im Vorfeld die Erstellung des Notfallfallvorsorgekonzepts (zB Erstellung der Dokumentationen) nach Kräften zu unterstützen. Nur durch eine gute Vorbereitung ist es möglich, im Notfall Ruhe zu bewahren und nicht durch unüberlegte Handlungen den Schaden zu vergrößern.
- Unregelmäßigkeiten, die auf einen Sicherheitsvorfall hindeuten, sind gemäß der *Alarmierungspläne* unverzüglich zu melden.
- Die *Handlungsanweisungen für ausgewählte Schadensereignisse* sind einzuhalten.
- Es sind Anweisungen und etwaige spezielle Verhaltensregeln zu beachten.

- Alle Begleitumstände sind ungeschönt, offen und transparent zu erläutern, um damit Schäden zu mindern, schnell Lösungen zu finden und Erkenntnisse zur Verbesserung des IT-Sicherheitskonzepts zu gewinnen.
- Informationen über den Notfall dürfen nicht an unautorisierte externe Dritte weitergegeben werden.
- Nach einem Notfall ist der sichere Normalzustand wieder herzustellen und an der Aufarbeitung des Notfalls mitzuarbeiten.

39.2 SOFORTMAßNAHMEN

Derjenige, der einen Sicherheitsvorfall bemerkt, leitet umgehend erste Maßnahmen ein (zB Alarmierung, Rechner ausschalten, ...).

39.3 ALARMIERUNG

Die verantwortlichen Stellen, die aktiv handeln oder Verantwortung übernehmen müssen, sind zu alarmieren (zB Feuerwehr, Administrator). Sie übernehmen dann in der Regel die weitere Untersuchung und Bewertung des Vorfalls und leiten Maßnahmen ein.

Im Vorfeld wurden Alarmierungspläne erstellt, die die Meldewege für ausgewählte Schadensereignisse beschreiben.

Als Anhang werden Adress- und Telefonlisten geführt, relevante Telefonnummern externer Dienstleister und Behörden sind evident.

Damit allen Mitarbeitern die Ansprechpartner bekannt sind werden diese Listen in Schriftform verteilt.

39.4 UNTERSUCHUNG UND BEWERTUNG DES VORFALLS

Um einen akuten Sicherheitsvorfall untersuchen und bewerten zu können, sind in der Regel folgende Informationen notwendig:

- betroffene IT-Komponenten (IT-Systeme und IT-Anwendungen – siehe Verfahrensverzeichnis)
- betroffene Prozesse (zB Dokumentationspflichten nach GuKG, steuerrelevante Termine)
- Ansprechpartner (Technik und Abteilungen)
- Verfügbarkeitsanforderungen der IT-Komponenten
- Schutzbedarf der IT-Komponenten und der damit verarbeiteten Informationen
- möglicher Schaden: Schadensart, Schadenshöhe, Geschädigte (zB Kunden, Mitarbeiter und/oder Geschäftspartner)

- mögliche Folgeschäden
- Ursache des Vorfalls (technisches Versagen, Unachtsamkeit, gezielter Angriff)
- Maßnahmen zur Behebung des Vorfalls

40 ESKALATIONSSTRATEGIE

Unter Umständen müssen Stellen mit größerer Kompetenz und höherer Verantwortung benachrichtigt werden (Verbandsobmann, Verbandsversammlung). Anhand der Eskalationsstrategie ist zu entscheiden,

- ob eine sofortige Eskalation ohne weitere Untersuchungen und Bewertungen erforderlich ist,
- ob zunächst eine genauere Untersuchung des Vorfalls erfolgen soll,
- wer intern informiert werden muss,
- welche externen Stellen informiert werden müssen.

Die Meldung über einen Sicherheitsvorfall oder eine darauf hindeutende Unregelmäßigkeit muss zunächst dahingehend geprüft werden, welches Ausmaß und Bedeutung der Vorfall bzw. die Unregelmäßigkeit hat, um dann entsprechende Maßnahmen zu ergreifen. Innerhalb einer Eskalationsstrategie werden Personen, Zeitpunkte und Medien der Eskalation definiert.

40.1 ENTSCHEIDUNGSHILFE FÜR ESKALATION

Sicherheitsvorfälle verursacht durch „höhere Gewalt“ (Brand, Explosion, Hochwasser, Leitungswasserschäden, Vandalismus, Sabotage, Einbruch) haben eine sofortige Eskalation ohne weitere Untersuchungen und Bewertungen zur Folge.

Ob bei anderen Vorfällen eine Eskalation notwendig ist, wird anhand folgender Fragen geprüft:

- (Vermutete) Schadenshöhe übertrifft den Verantwortungsbereich
- Kosten und Ressourcen für die erforderlichen Maßnahmen übertreffen den Kompetenzbereich
- Komplexität des Sicherheitsvorfalls übersteigt Kompetenz- bzw. Zuständigkeitsbereich

40.2 ESKALATIONSWEGE

Es wurde definiert, wer an wen eine Meldung weitergibt. Dabei sind sowohl die regulären Eskalationswege als auch der Vertretungsfall berücksichtigt worden. Ein solcher Eskalationswegeplan ist vorfallsspezifisch – sinnvollerweise graphisch – zu erstellen.

Die notwendigen Adress- und Telefonlisten werden geführt.

40.3 ART UND WEISE DER ESKALATION

Es sind zum einen zeitliche Vorgaben gemacht worden, zum anderen die Art der Benachrichtigung festgeschrieben (telefonisch, Formular, E-Mail etc.). In zeitkritischen Fällen sollte die Eskalation persönlich oder per Telefon erfolgen.

41 MAßNAHMEN ZUR PROBLEMLÖSUNG

41.1 REIHENFOLGE DER FEHLERBEHEBUNG

Bei der Behebung von Schäden sind verschiedene Aspekte zu berücksichtigen, wenn unterschiedliche Vorfälle, mehrere IT-Komponenten oder verschiedene Geschäftsprozesse betroffen sind und eine Wiederanlaufreihenfolge festgelegt werden muss.

41.2 VORAUSSETZUNGEN FÜR KURZE WIEDERANLAUFZEITEN

Um im Schadensfall Probleme möglichst schnell lösen zu können, müssen rechtzeitig Vorbereitungen getroffen werden:

- Erstellung von eigenen Dokumentationen und sorgfältige Archivierung von externen Dokumenten
- Datensicherung
- Verträge mit externen Dienstleistern, Herstellern und Lieferanten
- Ersatzbeschaffungsplan für Hardware (siehe Anhang B 2.1)

NOTBETRIEB

Nicht immer kann jedes Problem in einer tolerierbaren Zeitspanne behoben werden (Beispiel: Reparatur eines IT-Systems dauert zu lange). In diesen Fällen ist es erforderlich, die wichtigsten Geschäftsprozesse provisorisch aufrecht zu erhalten. Verschiedene Möglichkeiten bieten sich je nach Vorfall an:

- Einschränkung des IT-Betriebs
- manuelle Ersatzverfahren
- interne oder externe Ausweichmöglichkeiten

Die notwendigen Dokumentationen sowie Kontaktadressen von Dienstleistern, Herstellern und Lieferanten sind im Vorfeld zusammenzustellen.

41.3 INFORMATIONSPOLITIK

Unter Umständen müssen betroffene interne und externe Stellen über den Vorfall informiert werden. Dies sind insbesondere diejenigen Stellen, die di-

rekt durch den Sicherheitsvorfall Schäden erleiden könnten, Gegenmaßnahmen ergreifen müssen oder solche, die Informationen über Sicherheitsvorfälle aufbereiten und bei der Vorbeugung oder Behebung helfen können. In Einzelfällen kann es auch notwendig sein, die Medien zu informieren.

41.4 DOKUMENTATION

Eine Dokumentation des Notfalls ist notwendig, um für zukünftige Vorfälle zu lernen und Veränderungen an IT-Systemen und IT-Anwendungen nachvollziehen zu können. Dies ist besonders wichtig, wenn unter Zeitdruck oder mit Sonderrechten gearbeitet wurde.

Protokoll- und Log-Dateien können im Nachhinein eine wertvolle Hilfe sein und sollten daher gesichert werden.

Bei der Dokumentation sollte auch an eine mögliche Strafverfolgung gedacht werden.

42 NACHBEREITUNG VON NOTFÄLLEN

Eine Nachbereitung von Notfällen hat aus zwei Gründen zu erfolgen:

Verbesserungspotentiale erkennen

Dazu sind zum Beispiel folgende Fragen zu klären:

- Waren die Reaktionszeiten ausreichend?
- Hat die Alarmierung funktioniert oder gab es Probleme bei der Eskalation des Vorfalls?
- Wurde die Ursache des Vorfalls schnell gefunden und wurden die Auswirkungen richtig eingeschätzt?
- Waren alle Dokumentationen brauchbar und aktuell?
- Wenn es einen Täter gab: Was hat ihn motiviert?
- Was muss in Zukunft verbessert werden?

Wiederherstellung eines stabilen Normalzustandes

Nach einem Notfall ist dafür zu sorgen, dass möglichst schnell der sichere Normalzustand wieder erreicht wird. Zur Behebung des Notfall sind unter Umständen Anwendungen, IT-Systeme oder Konfigurationen verändert oder elektronische Abläufe durch manuelle ersetzt worden.

Es kann zum Beispiel auch erforderlich sein, Passwörter neu zu vergeben und zu verändern.

43 PRÄVENTION UND VORBEREITUNG

Die folgenden Maßnahmen sollten zur Notfallvorsorge ergriffen werden.

43.1 DATENSICHERUNGSPLAN

Datensicherungen sind zu erstellen, um Datenverlust vorzubeugen und Ersatz-Systeme schnell in Betrieb nehmen zu können.

Mit Hilfe eines Datensicherungsplans muss ein sachverständiger Dritter in der Lage sein, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten in angemessener Zeit beschaffen und installieren zu können. Ein Datensicherungsplan muss Auskunft geben können über:

- Datum der Datensicherung
- Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert)
- Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind
- Datenträger, auf dem die Daten gesichert wurden
- für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer)
- bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.)
- Ort der Aufbewahrung

43.2 OUTSOURCING, VERTRÄGE MIT HERSTELLER UND LIEFERANTEN

Notfallvorsorge muss Bestandteil von Verträgen mit externen Dienstleistern sein. Außerdem kann es erforderlich sein, bei Notfällen auf die Dienste von Spezialisten zurückzugreifen.

Die wichtigsten Vorgaben sind vertraglich zu vereinbaren, z. B:

- Zuständigkeiten, Ansprechpartner und Abläufe
- Datensicherung
- Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen
- regelmäßige Notfallübungen

Bei der Auswahl von Software sind Support- und Serviceleistungen als Auswahlkriterium zu berücksichtigen. Bei Bedarf sind vertragliche Regelungen (Hotline, Antwortzeiten, individuelle Updates und Patches) mit den Herstellern abzuschließen.

43.3 VERSICHERUNGSSCHUTZ

Verbleibende Restrisiken sind unter Beachtung von Kosten- Nutzen-Aspekten durch Versicherungen abgedeckt werden.

- Sachversicherungen
- Feuerversicherung
- Einbruch- und Diebstahlversicherung
- Transportversicherung
- Datenträgerversicherung
- Elektrogeräteversicherung

43.4 TECHNISCHE MAßNAHMEN

Um zu vermeiden, dass ein Sicherheitsvorfall zum Notfall wird, müssen Sicherheitsvorfälle durch technische Maßnahmen verhindert oder möglichst frühzeitig entdeckt werden.

EINSATZ VON TECHNISCHEN DETEKTIONSMAßNAHMEN

Es gibt eine Reihe von Sicherheitsvorfällen, die mit entsprechender technischer Unterstützung automatisiert und daher frühzeitig erkannt werden können. Zu diesem Zweck sollen Detektionsmaßnahmen installiert werden.

Beispiele für solche technischen Detektionsmaßnahmen sind:

- Gefahrenmeldeanlage
- Rauchmelder
- Fernanzeige von Störungen
- Computer-Viren-Schutzprogramme
- Intrusion Detection und Intrusion Response Systeme
- Kryptographische Checksummen und digitale Signaturen

Die technischen Detektionsmaßnahmen müssen durch zusätzliche organisatorische Maßnahmen ergänzt werden (zum Beispiel Meldewege, regelmäßige Aktualisierung und Überprüfung).

Bei der Auswahl von Detektionsmaßnahmen ist immer eine Kosten-Nutzen-Berechnung vorzulegen und die Wirksamkeit kritisch zu hinterfragen.

SICHERE INFRASTRUKTUR

Die Infrastruktur (Gebäude und Räume) ist durch geeignete Maßnahmen zu sichern. Dazu gehören beispielsweise die Bereiche Zugangsschutz, Diebstahlschutz, Schutz vor Naturereignissen, Stromversorgung, Klimatisierung.

Durch eine unterbrechungsfreie Stromversorgung ist sicherzustellen, dass für hochverfügbare IT-Systeme ein kurzzeitiger Stromausfall keinen Schaden verursacht.

43.5 AUSBILDUNG UND TRAINING DER MITARBEITER

NOTFALLSCHULUNGEN

Ein qualitativ hochwertiges Notfall- und Kontinuitätsmanagement greift nur dann optimal, wenn die Mitarbeiter zum einen für sicherheitsrelevante Vorfälle sensibilisiert sind und zum anderen bestmöglich für sicherheitsrelevante Vorfälle geschult werden.

Sämtliche Mitarbeiter (auch nicht unmittelbar mit dem IT-Betrieb befasste Personen wie Pflegepersonal und Funktionspersonal) werden in der Anwendung des Notfallvorsorgekonzeptes geschult.

NOTFALLÜBUNGEN

Es sind regelmäßig angekündigte und unangekündigte Übungen durchzuführen.

Übungen sind sorgfältig zu planen, um Schäden an IT-Systemen, Daten oder sonstigem zu verhindern.

Bei einer Notfallübung sind zum Beispiel folgende Tätigkeiten durchzuführen:

- Durchspielen der Notfallsituation im Team
- Durchführung einer Alarmierung
- Funktionstests von Stromaggregaten
- Durchführung von Feuerübungen
- Wiedereinspielen von Datensicherungen
- Wiederanlauf nach Ausfall eines ausgewählten IT-Systems

Es sollten nicht nur Schreibtischübung, sondern auch Feldübung mit Problemsimulationen sowie echte Übung (zum Beispiel Notstromprobe) durchgeführt werden.

Die wichtigsten Ergebnisse einer Notfallübung sind zu dokumentieren und bekannt zu geben. Die Erkenntnisse aus den Übungen sollten möglichst schnell zur Verbesserung des Notfallvorsorgekonzepts genutzt werden.

ANHANG A: VERANTWORTLICHE PERSONEN

1 NOTFALL-VERANTWORTLICHER/ADMINISTRATOR

Der Administrator nimmt Meldungen über Sicherheitsvorfälle entgegen und informiert bei Bedarf die Verwaltungsdirektion. Bei der Behebung und Aufarbeitung eines Notfalls unterstützt er die Verantwortlichen. Er überwacht auch, ob alle IT-Sicherheitsmaßnahmen nach Beendigung des Vorfalls wieder in Kraft gesetzt werden und überprüft mit den Erkenntnissen aus dem Vorfall das IT-Sicherheitskonzept auf Schwächen und Verbesserungsmöglichkeiten.

Der Notfall-Verantwortliche hat folgende Aufgaben:

- Bewertung von Sicherheitsvorfällen
- formale Ausrufung und Beendigung des Notfalls
- Koordination der Notfallmaßnahmen
- Dokumentation des Notfalls, Erstellung eines Abschlussberichts
- Unterrichtung der betroffenen Fachabteilungen
- Zusammenstellung und Einberufung eines Notfall-Teams
- Organisation und Vorbereitung von Notfall-Schulungen und -Übungen

Administratoren haben eine große Verantwortung. Sie überwachen ihre IT-Systeme und Anwendungen und sind die ersten Ansprechpartner von IT-Benutzern bei Problemen und Fragen. Sie werden daher oftmals die ersten sein, die erkennen, dass eine Unregelmäßigkeit sicherheitsrelevant ist. Sie müssen dann verantwortungsbewusst entscheiden, ob sie das Problem selbst beheben können oder ob sie den Vorfall eskalieren.

Alle Mitarbeiter haben die Notfallvorsorge zu unterstützen.

2 BRANDSCHUTZBEAUFTRAGTER

Zu den Aufgaben des Brandschutzbeauftragten zählen u. a. Brandschutzbegehungen, die Zusammenarbeit mit der Feuerwehr, die Kontrolle und Wartungsüberwachung der Brandmelde- und Löschvorrichtungen und die Durchführung von Übungen.

Der Brandschutzbeauftragte und der Administrator arbeiten eng zusammen und sorgen dafür, dass bei den Brandschutzmaßnahmen die besonderen Belange der Informationssicherheit berücksichtigt werden.

3 VERWALTUNGSDIREKTION

Die Leitung trifft abschließende Entscheidung zur Durchführung von Maßnahmen. Sie schaltet die Polizei und Strafverfolgungsbehörden ein, wenn der Verdacht auf kriminelle Handlungen besteht.

In Notfällen sollte die Öffentlichkeit ausschließlich durch den Verbandsobmann bzw. die Verwaltungsdirektion informiert werden.

4 DATENSCHUTZBEAUFTRAGTER

Diese Positionen sind heranzuziehen, sofern ein Notfall datenschutzrechtliche oder mitbestimmungspflichtige Aspekte hat.

5 SICHERHEITSVORFALL-TEAM

Je nach Bedarf wird das Sicherheitsvorfall-Team von der Verwaltungsdirektion zusammengestellt und einberufen.

Das Sicherheitsvorfall-Team ist befugt, die übertragenen Aufgaben eigenverantwortlich durchzuführen.

Zu einem Sicherheitsvorfall-Team können je nach Ausmaß und Art des Notfalls folgende Personenkreise gehören:

- Direktionen
- Administrator
- Datenschutzbeauftragter
- Personalvertretung
- die Bereiche Beschaffung, Haustechnik, weiteres Personal
- Brandschutzbeauftragter

ANHANG B: NOTFALLVORSORGE UND RICHTLINIEN

1 ALAMIERUNGSPLAN

Der Alarmierungsplan beschreibt die Meldewege für ausgewählte Schadensereignisse, die die IT-Sicherheit und Verfügbarkeit gefährden.

1.1 SCHADENSSZENARIEN UND HANDLUNGSPLÄNE

Bei Sicherheitsvorfällen und in Notfällen ist es entscheidend, dass alle Mitarbeiter wissen, was zu tun ist. Aus diesem Grund sind für die wichtigsten Schadensereignisse Handlungsanweisungen und Verhaltensregeln aufgestellt worden.

BRAND, EXPLOSION

1. Brand melden	**Brandmelder betätigen oder Notruf 122**
2. In Sicherheit bringen	**Gefährdete Personen mitnehmen** **Türen schließen** **Rettungsweg folgen** **Aufzug nicht benutzen** **Anweisungen beachten**
3. Löschversuche unternehmen	**Feuerlöscher, Wandhydrant nutzen**

In der Folge Meldung an den Brandschutzbeauftragten:

- **PH WIESENWEG Martin Larcher Telefon 0676.83038.5024**
- **PH SCHLICHTLING Martin Larcher Telefon 0676.83038.5024**
- **PH SEEFELD Martin Larcher Telefon 0676.83038.5024**

Der Brandschutzbeauftragte informiert telefonisch die Verwaltungsdirektion.

Eskalation: Bei Ausfall der IT-Verfügbarkeit wird sofort ein Sicherheitsvorfall-Team gebildet (siehe Anhang A 5)

STROMAUSFALL

Technische Einrichtungen sind mittels einer USV (Unterbrechungsfreie Stromversorung) gegen Ausfall abgesichert.

Bei Stromausfall UNBEDINGTE TELEFONISCHE Meldung an die Haustechnik!

Sollte die **Behebung** der Störung nicht innerhalb von **ZWEI STUNDEN** möglich sein, erfolgt eine telefonische Meldung an die Verwaltung, diese informiert alle betroffenen Pflegestationen und Bereiche.

Eskalation: Bei Ausfall der IT-Verfügbarkeit (voraussichtlich) länger als **24 STUNDEN** wird sofort ein Sicherheitsvorfall-Team gebildet (siehe Anhang A 5).

LEITUNGSWASSERSCHÄDEN, HOCHWASSER

Insbesondere bei Wasserschäden und Wassereintritt von außen ist vorrangig der **diensthabende Haustechniker** zu kontaktieren. Sollte kein Haustechniker erreichbar sein, **Feuerwehr unter 122** kontaktieren

Schäden sind nach Möglichkeit zu minimieren (abpumpen von Wasser etc.).

Sollte die Behebung des IT-Ausfalles aufgrund Leitungswasserschaden nicht innerhalb von **ZWEI STUNDEN** möglich sein, erfolgt eine telefonische Meldung an die Verwaltung, diese informiert alle betroffenen Pflegestationen und Bereiche.

Eskalation: Bei Ausfall der IT-Verfügbarkeit (Schäden offensichtlich irreparabel) wird sofort ein Sicherheitsvorfall-Team gebildet (siehe Anhang A 5)

HARDWARE-AUSFALL AUFGRUND TECHNISCHER DEFEKTE

Hardware-Ausfälle können zum Beispiel durch Unwetter und Blitzschlag entstehen. Die **Haustechnik und der IT-Techniker/Administrator** sind umgehend telefonisch zu informieren.

Schäden sind nach Möglichkeit zu minimieren (abpumpen von Wasser etc.).

Sollte die Behebung des IT-Ausfalles nicht innerhalb von **ZWEI STUNDEN** möglich sein, erfolgt eine telefonische Meldung an die Verwaltung, diese informiert alle betroffenen Pflegestationen und Bereiche.

Eskalation: Bei Ausfall der IT-Verfügbarkeit (Schäden offensichtlich irreparabel) wird sofort ein Sicherheitsvorfall-Team gebildet (siehe Anhang A 5)

SOFTWARE-AUSFALL

Der Ausfall einzelner oder mehrerer Anwendungen ist dem IT-**Techniker/Administrator** bei Bekanntwerden schriftlich (bei außerordentlicher Dringlichkeit telefonisch) zu melden.

Sollte die Behebung des IT-Ausfalles nicht innerhalb von **ZWEI STUNDEN** möglich sein, erfolgt eine telefonische Meldung an die Verwaltung, diese informiert alle betroffenen Pflegestationen und Bereiche.

Eskalation: Bei Totalausfall einer Software ist telefonisch SOFORT (und in der Folge schriftlich zu Dokumentationszwecken) der Softwareanbieter zu kontaktieren.

AUSFALL DER DATENÜBERTRAGUNGSEINRICHTUNGEN

Ausfälle der LWL-Anbindung (Lichtwellenleitung) an die Marktgemeinde Telfs stellt einen Totalausfall aller benötigten Systeme dar. Die **Haustechnik und der IT-Techniker/Administrator** sind umgehend telefonisch zu informieren.

Datenübertragungseinrichtungen können durch Straßengrabungen, Blitzschlag, Brand in Verteilern etc. beschädigt werden.

Sollte die Behebung des IT-Ausfalles nicht innerhalb von **ZWEI STUNDEN** möglich sein, erfolgt eine telefonische Meldung an die Verwaltung, diese informiert alle betroffenen Pflegestationen und Bereiche.

Eskalation: Bei Ausfall der IT-Verfügbarkeit (voraussichtlich) länger als **24 STUNDEN** wird sofort ein Sicherheitsvorfall-Team gebildet (siehe Anhang A 5).

VIRENBEFALL

SOFORTMAßNAHME: Rechner ausstecken, Netzwerkkabel entfernen!

Sobald ein Fehler oder ein anderes Problem auftritt, ist sofort telefonisch der **IT-Techniker/Administrator** zu benachrichtigen. Im Umgang mit Sicherheitsvorfällen sind Ehrlichkeit und Kooperationsbereitschaft besonders wichtig. Die Meldung von Sicherheitsvorfällen wird daher immer positiv gewertet!

Eskalation: Bei Ausfällen bzw. Rücksicherungen ist SOFORT die Verwaltungsdirektion telefonisch zu informieren. Bei Ausfall der IT-Verfügbarkeit (voraussichtlich) länger als **24 STUNDEN** wird sofort ein Sicherheitsvorfall-Team gebildet (siehe Anhang A 5).

VANDALISMUS, SABOTAGE, EINBRUCH

Eine Meldung hat umgehend telefonisch an die **Verwaltungsdirektion** und den **IT-Techniker/Administrator** zu erfolgen. Vandalismusschäden, Sabotage und Einbruch sind bei der **Polizei (Telefon 133)** zur Anzeige zu bringen.

Eskalation: Bei Vandalismus, Sabotage oder Einbruch der IT (Insbesondere der Server-Integrität) wird sofort ein Sicherheitsvorfall-Team gebildet (siehe Anhang A 5)

1.2 KONTAKTDATEN

HAUSTECHNIK

- **Daniel Kirchmair** **Telefon 0676.83038.5023**
- **Josef Köll** **Telefon 0676.83038.5112**
- **Martin Larcher** **Telefon 0676.83038.5024**
- **Tobias Pfister** **Telefon 0676.83038.5012**

IT-TECHNIKER/ADMINISTRATOR

- **MARKTGEMEINDE TELFS, IT-ABTEILUNG**
  BERNHARD STELZL
  TELEFON 05262.6961.1305
  MOBIL 0676.83038.308

VERWALTUNGSDIREKTION

- **GEMEINDEVERBAND ALTENWOHNHEIM TELFS**
  DIR. MATTHIAS KAUFMANN
  TELEFON 05262.62145.500
  MOBIL 0676.9597948

STANDARDNOTRUFNUMMERN (AUSZUG)

- **Feuerwehr** **122**
- **Polizei** **133**
- **Rettung** **144**
- **Gas-Notruf** **128**
- **Apotheken Notruf** **1455**
- **Euronotruf** **112**
- **Ärztenotdienst** **141**
- **Krankentransport** **14844**

2 VERFÜGBARKEITSANFORDERUNGEN UND ERSATZVERFAHREN

Prozesse von hoher Relevanz für die Geschäftstätigkeit sind alle Bereiche, die die Pflege, Betreuung und Abrechnung betreffen und daher ein Verlust oder die Nicht-Verfügbarkeit einen hohen Schaden bedeutet.

2.1 ERSATZBESCHAFFUNGSPLAN

Wenn die Reparatur eines ausgefallenen IT-Systems nicht möglich ist oder zu lange dauert, kann eine Ersatzbeschaffung notwendig werden. Zur Vorbereitung ist ein Ersatzbeschaffungsplan mit folgenden Angaben zu erstellen:

- Bezeichnung der IT-Komponente
- Hersteller
- Lieferant
- Dauer der Re-Installation

Der Ersatzbeschaffungsplan entspricht den aktuell genutzten IT-Systemen und entspricht der bestehenden Dokumentation, welche Teil des Verfahrensverzeichnisses des Gemeindeverbandes Altenwohnheim Telfs ist.

3 PASSWORTRICHTLINIE

Folgende Regeln sind zu beachten:

1. Passwörter sind nirgends zu notieren und niemandem mitzuteilen.
2. Das Passwort darf nur dem Benutzer bekannt sein.
3. Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.
4. Passwörter dürfen nicht leicht zu erraten sein. Vor- und Familiennamen oder Geburtstage sind beispielsweise nicht zur Bildung von Passwörtern geeignet. Es dürfen niemals Trivialpasswörter verwendet werden (z. B. 4711; 12345 oder andere nebeneinanderliegende Tasten).
5. Die Passwörter sind spätestens alle 90 Tage zu wechseln.
6. Sofern Gruppenpasswörter zwingend erforderlich sind, gilt: Gruppenpasswörter sind umgehend zu ändern, wenn die Zusammensetzung der Gruppe sich verändert. Gleiches gilt, wenn Passwörter unautorisierten Personen bekannt geworden sind.
7. Einmal genutzte Passwörter sind nicht wieder zu verwenden.
8. Benutzer haben den Empfang von Initial-Passwörtern immer zu bestätigen und müssen diese sofort wechseln.
9. Alle IT-Systeme sind zum Schutz vor unbefugten Personen mit einem passwortunterstützten Bildschirmschoner ausgestattet, dieser ist auch immer zu benutzen.
10. Wenn der Verdacht besteht, dass die eigenen Zugangs- und Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist das Passwort umgehend zu ändern und der Administrator oder Datenschutzbeauftragte um Rat zu fragen.

4 VIRENSCHUTZRICHTLINIE

Die Benutzer tragen dafür Verantwortung, IT-Systeme so zu nutzen, dass eine Infektion mit Computer-Viren vermieden wird.

4.1 REGELUNGEN

- Alle verdächtigen Ereignisse sind unverzüglich dem Administrator zu melden.
- Verdächtige Dateien dürfen nicht selbständig geöffnet werden.
- Viren-Schutz-Programme dürfen nicht deaktiviert werden.
- Vorgegebene Sicherheitseinstellungen dürfen nicht deaktiviert oder umgangen werden.
- Software darf nur von berechtigten Administratoren oder in Absprache mit diesen installiert werden.
- Sofern die Nutzung privater Hardware (zum Beispiel Mobiltelefone) zusammen mit dienstlicher Hardware oder zur sonstigen dienstlichen Nutzung genehmigt wurde, sind die technischen und organisatorischen Maßnahmen im Rahmen des Computer-Virenschutzes zu beachten.
- IT-Systeme sollten sorgfältig hinsichtlich möglicher Gefahren beobachtet werden.
- Jeder Verdacht auf Computer-Viren muss sofort gemeldet werden.
- Eingehende und ausgehende Dateien sind im Falle eines Datenträgeraustauschs einer Viren-Prüfung zu unterziehen.
- Werden E-Mails nicht über das zentrale E-Mail-Gateway versendet, sind Dateianhänge ebenfalls vorher auf Viren zu prüfen.
- Jeder IT-Benutzer hat vor der ersten Nutzung von IT-Diensten an den angebotenen Schulungen teilzunehmen.

4.2 ANZEICHEN FÜR EINEN VIRENBEFALL

Folgende Anzeichen können auf einen Computer-Virenbefall hindeuten:

- häufige Programmabstürze
- Programmdateien werden länger
- unerklärliches Systemverhalten
- „unerklärliche“ System-Fehlermeldungen
- Nutzung unbekannter Dienste
- nicht auffindbare Dateien
- veränderte Dateiinhalte
- ständige Verringerung des freien Speicherplatzes, ohne dass etwas abgespeichert wurde

4.3 VERHALTENSREGELN FÜR DEN IT-BENUTZER

Bei Auftreten eines Computer-Virus ist zu verhindern, dass weitere IT-Systeme infiziert werden. Daher ist ein entdeckter Computer-Virus (bzw. der Verdacht) unverzüglich dem Administrator persönlich oder telefonisch zu melden.

Bis zur Klärung des Sachverhalts durch den Administrator darf das betroffene IT-System nicht mehr benutzt werden und sollte unverändert belassen werden, um keine Spuren zu verwischen.

Wer einen Viren-Vorfall verschleiert oder ignoriert, muss mit arbeitsrechtlichen Konsequenzen rechnen. Wer dagegen einen Viren-Vorfall meldet und alles unternimmt, um schlimmeren Schaden zu verhüten, wird nicht bestraft, auch wenn er durch fahrlässiges Verhalten den Viren-Befall verursacht hat.

ANHANG C: VERPFLICHTUNGSERKLÄRUNG

ZUM DATENGEHEIMNIS UND ZUR WAHRUNG VON GESCHÄFTS- UND BETRIEBSGEHEIMNISSEN

Diese Verpflichtungserklärung betrifft:

Familienname:

Vorname(n):

In Ausübung Ihrer beruflichen Tätigkeit erhalten Sie Kenntnis über personenbezogene Daten sowie Geschäfts- und Betriebsgeheimnisse. Alle diese Informationen sind absolut vertraulich zu behandeln und unterliegen den Bestimmungen des österreichischen und europäischen Datenschutzrechts sowie des Wettbewerbsrechts.

Mit Ihrer Unterschrift verpflichten Sie sich,

1. das Datenschutzrecht zu wahren, insbesondere § 6 DSG, einschließlich entsprechender betrieblicher Anordnungen;
2. Geschäfts- und Betriebsgeheimnisse zu wahren (§ 11 UWG);

und bei einem Verstoß gegen das Datengeheimnis oder eine Verletzung von Geschäfts- und Betriebsgeheimnissen, Schadenersatz zu leisten, und zwar ohne Rücksicht auf den tatsächlich eingetretenen Schaden durch Vereinbarung einer Konventionalstrafe pauschaliert, und zwar im Ausmaß von drei Bruttomonatsentgelten.

Die zitierten Bestimmungen sind im Anhang zu dieser Erklärung abgedruckt.

Ihnen ist bekannt, dass

- die personenbezogenen Daten natürlicher wie juristischer Personen einem besonderen Schutz unterliegen und die Verwendung solcher Daten nur unter besonderen Voraussetzungen zulässig ist.
- personenbezogene Daten und personenbezogene Daten besonderer Kategorien, die Ihnen auf Grund Ihrer beruflichen Beschäftigung anver-

traut oder zugänglich gemacht wurden, nur auf Grund einer ausdrücklichen Anordnung des jeweiligen Vorgesetzten übermittelt werden dürfen.

- es **untersagt** ist, Daten an unbefugte Empfänger innerhalb und außerhalb des Unternehmens zu übermitteln oder sonst zugänglich zu machen.
- es **untersagt** ist, sich unbefugt Daten zu beschaffen oder zu verarbeiten.
- es **untersagt** ist, personenbezogene Daten zu einem anderen als dem zum rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verarbeiten.
- anvertraute **Benutzerkennwörter**, **Passwörter** und sonstige **Zugangsberechtigungen** sorgfältig verwahrt und geheim zu halten sind (Zugangsberechtigungen können im Bedarfsfall von der EDV-Abteilung zurückgesetzt werden).
- die **Zugriffsberechtigungen** auf die zugewiesenen Laufwerke durch den EDV-Verantwortlichen verwaltet, dokumentiert und protokolliert werden.
- der private Gebrauch der EDV-Anlage (Hardware, Software, Internet, E-Mail) außerhalb der Dienstzeit **untersagt** ist.
- jeder private Gebrauch der EDV-Anlage während der Dienstzeit protokolliert und kontrolliert wird (Erfassung besuchter Websites, etc.).
- das Einspielen von Programmen (zum Beispiel für Internet-Telefonie, File-Sharing, usw.), Dateien, Dateifragmenten ausnahmslos **verboten** ist.
- der Download von Videonachrichten, Programmen, privaten Dateien oder der Vertrieb und Kauf von Artikeln in Tauschbörsen bzw. Verkaufsplattformen (Ebay, One2Sold, Shpock, etc.) **untersagt** ist.
- personalisierte **E-Mail-Adressen** dem Dienstnehmer zur treuhändigen Verwahrung überlassen werden, diese daher ausschließlich der betrieblichen Nutzung vorbehalten sind, eine Privatnutzung ausgeschlossen ist. Personalisierte E-Mail-Adressen werden nach Ausscheiden des Dienstnehmers aus dem Gemeindeverband drei Monate bestehen bleiben; elektronische Postnachrichten dem logisch folgenden Mitarbeiter bzw. der Abteilung weitergeleitet.
- die Nutzung dienstlicher E-Mail-Adressen protokolliert und gegebenenfalls kontrolliert wird. Eine Nutzung und Verwendung kann jederzeit seitens der Verwaltungsdirektion jederzeit widerrufen werden.
- allfällige weiterreichende andere Bestimmungen über die Geheimhaltungspflichten ebenfalls zu beachten sind.
- diese Verpflichtung auch nach Beendigung Ihrer Tätigkeit fortbesteht;

- **Verstöße** gegen die hier genannten Verschwiegenheitsverpflichtungen nicht nur arbeitsrechtliche Folgen, sondern auch (verwaltungs-)strafrechtliche Folgen haben und **schadenersatzpflichtig machen**.
- **Verstöße** gegen diese Verpflichtungserklärung der Verwaltungsdirektion **gemeldet werden**.

Es kann sein, dass sich die Vorgehensweise des Gemeindeverbandes bezüglich Datengeheimnis von Zeit zu Zeit ändern kann, zum Beispiel aufgrund Änderung, Wegfall oder Neueinführung von Prozessen oder aufgrund von Gesetzen oder Technik. Sollte es notwendig werden, beschriebenen Inhalt zu ändern, werden diese Änderung persönlich und/oder mittels interner Kundmachung veröffentlicht.

Hiermit erkläre ich, am _____ von meinem Dienstgeber über das Datengeheimnis nach § 6 DSG und die Verschwiegenheitsverpflichtungen nach § 11 UWG belehrt worden zu sein.

Ort, Datum	**Unterschrift des Verpflichteten**

Datengeheimnis nach § 6 DSG

(1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

Sicherheit der Verarbeitung nach Art. 32 Abs 4 DSGVO

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Verletzung von Geschäfts- oder Betriebsgeheimnissen und Missbrauch anvertrauter Vorlagen nach § 11 UWG

(1) Wer als Bediensteter eines Unternehmens Geschäfts- oder Betriebsgeheimnisse, die ihm vermöge des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des Wettbewerbes mitteilt, ist vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen. (BGBl. Nr. 120/1980, Art. I Z 6)

(2) Die gleiche Strafe trifft den, der Geschäfts- oder Betriebsgeheimnisse, deren Kenntnis er durch eine der im Abs. 1 bezeichneten Mitteilungen oder durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbes unbefugt verwertet oder an andere mitteilt.

(3) Die Verfolgung findet nur auf Verlangen des Verletzten statt.