kuravisma

Anlage zum Hauptblatt: Technische und organisatorische Maßnahmen

1 Zutrittskontrolle

Begleitung der Besucher durch Mitarbeiter Besucher dürfen sich nicht frei im Unternehmen bewegen. Sie werden ständig von Mitarbeitern begleitet.

Dokumentation der Anwesenden (Datum, Zeit, Dauer) in Sicherheitsbereichen Zeit, Datum und Dauer des Aufenthalts in den Bereichen der Datenverarbeitungsanlagen werden dokumentiert durch: Mitarbeiter: Personalbüro Dokument: Besucherbuch im Personalbüro

Dokumentation v. Zutrittsrechten Zutrittsrechte zu den Datenverarbeitungsanlagen werden dokumentiert durch: IT-Administratoren Dokument: kein Dokument, gesichert durch gesteuerte Schlüsselvergabe

Erfassung von Besuchern Der Besuch wird dokumentiert durch: Eintrag in ein Besucherbuch

Liste von berechtigten Personen (Serverraum) Es wird eine Liste mit zugangsberechtigten Personen geführt. Diese sind: IT-Administratoren weitere Mitarbeiter: Helmut Radtke, Marion Richter Dokument: kein Dokument, gesichert durch gesteuerte Schlüsselvergabe

Schädigende Umwelteinflüsse für die Datenverarbeitung Es existieren in den Räumen der Datenverarbeitung folgende Gefahren durch Umwelteinflüsse: Feuer: Feuerlöscher Stromausfall: USV's für die wichtigsten Server Überspannung: das EDV-Stromnetz ist überspannungsgesichert

Schutzmaßnahmen für Serverraum Der Server befindet sich in einem verschlossenem Raum und ist gesichert durch: Sicherheitstür: ja, mit Stahlkern Sicherheitsfenster: nein, 1. OG

Sicherheitsmaßnahmen gegen Umwelteinflüsse Die Sicherheitsmaßnahmen gegen diese Gefahren durch Umwelteinflüsse sind: Feuerfeste wasserdichte Aufbewahrung der Akten, Datenträger Unterbrechungsfreie Stromversorgung Leistungsschutzschalter Überspannungsschutz

kuravisma

Sicherung der Zugänge (Nebentüren, Fenster) Die weiteren Zugänge (Nebentüren, Fenster) sind gesichert durch: Sicherheitsfenster Sicherheitstüren Fenster/Türen werden beim Verlassen der Räume geschlossen

Verantwortlicher für die Bestimmung welche Räume, Bereiche, Objekte gesichert werden müssen Die zu sichernden Objekte und Bereiche des Unternehmens werden festgelegt durch: Geschäftsführung

Verantwortlicher für die Zutrittskontrolle Der Verantwortliche für die Zutrittskontrolle in unserem Unternehmen ist: Verantwortlicher d. Rechenzentrums Geschäftsführer

2 Zugangskontrolle

Abmeldung vom PC bei Verlassen des Arbeitsplatzes Mitarbeiter müssen sich beim Verlassen des Arbeitsplatzes abmelden Eine automatische Abmeldung ab 5 Minuten

Authentifizierung bei IT-Systemen Eine Authentifizierung des Benutzer erfolgt über: Passwort

Benutzerrechte Benutzer haben ausschließlich die Rechte, die sie zur Erledigung ihrer Aufgaben benötigen. Über diese Rechte wird ebenfalls geregelt welche Software-Module (z.B. Einkauf, Auftragsverarbeitung, Personal) und damit welche Daten sichtbar sind.

Entsperrung von administrativen Zugängen Im Falle einer Sperrung eines administrativen Zugangs erfolgt die Entsperrung folgendermaßen: Entsperrung wird dokumentiert über Service Desk

Erstellung v. Protokollen über Tätigkeiten auf Datenverarbeitungsanlagen Die Erstellung von Protokollen über Tätigkeiten auf Datenverarbeitungsanlagen erfolgt: automatisch

Kontrolle der Protokolle über Tätigkeiten auf Datenverarbeitungsanlagen Die Protokolle Tätigkeiten auf Datenverarbeitungsanlagen automatische werden folgendermaßen kontrolliert: manuelle Kontrolle nach Bedarf.

Maßnahmen zum Schutz der Datenverwaltung Zum Schutz der Datenverwaltung werden folgende Maßnahmen getroffen: Für IT-Systeme: Passwortvergabe Protokollierung der Login-Daten Für die Aktenablage: verschlossene Aktenschränke verschlossener Aktenraum

kuravisma

Personelle Passwortvergabe Die Sicherheit der personellen Passwortvergabe wird gewährleistet durch: Jeder Mitarbeiter verfügt über eigenes Passwort Verbot der Weitergabe

Der Schutz der administrativen Passwörter wird gewährleistet durch: Hinweisblatt für Berechtigte über den Umgang mit administrativen Passwörtern Zugang nur für ausgewählte Personen Liste der Mitarbeiter Dokument:

Sichere Aufbewahrung von Administrationspasswörtern Die sichere Aufbewahrung von Administrationspasswörtern wird folgendermaßen gewährleistet: Aufbewahrungsort ist nur ausgewählten Mitarbeitern bekannt Aufbewahrung in Papierform, Sicherung durch: verschlossener Schrank Tresor Verschlüsseltes Dokument, Zugriff haben nur die MA IT

Sicherheit der Passwörter Die Sicherheit der Passwörter wird gewährleistet durch: Vorgabe einer Mindestlänge Vorgabe der Komplexität (z.B. Gebrauch v. Sonderzeichen, Zahlen)

Sicherung der IT-Systeme gegen Unbefugte Die IT-Systeme des Unternehmens sind durch folgende Maßnahmen gesichert: Standleitung Teilnehmererkennung

Speicherung der Passwörter Nutzer
Passwörter werden verschlüsselt gespeichert

Speicherung der Systempasswörter
Systempasswörter werden verschlüsselt gespeichert

Sperrung bei falscher Passworteingabe Eine Sperrung des Benutzers bei falscher Passworteingabe ist für den Domain-Zugriff nicht aktiviert.

Verantwortlicher für die Zugangskontrolle Der Verantwortliche für die Zugangskontrolle in unserem Unternehmen ist: Geschäftsführer IT-Administratoren

Vergabe von Gruppenpasswörtern Gruppenpasswörter werden vergeben Bereich: Praktikanten Hinweis: Gruppenpasswörter sollten nach Möglichkeit vermieden werden.

kuravisma

3 Zugriffskontrolle

Aufbewahrungsort bzw. -art der Datenträger
Datenträger werden folgendermaßen aufbewahrt:
verschlossenes Archiv verschlossene Schränke
Tresor

Aufteilung der Zugriffsberechtigung Die Zugriffsberechtigung ist aufgeteilt in/durch:
Anwendungsprogramme (bzw. einzelne Module der Software) Dateien Datensätze Datenfelder Betriebssystem Server IT-System

Protokollierung der Zugriffsberechtigungen
Die Zugriffsberechtigungen werden protokolliert:
Dokument: aktuell nicht verfügbar

Verantwortlicher für die Zugriffskontrolle Der Verantwortliche für die Zugriffskontrolle in unserem Unternehmen ist: Geschäftsführer
IT-Administratoren

Zugriff der Nutzer auf Software
Mitarbeitern ist lediglich der Zugriff auf
getestete freigegebene Software
möglich

Zugriffskontrolle für Mitarbeiter Der Zugriff durch Mitarbeiter wird folgendermaßen kontrolliert: Benutzer haben ausschließlich die Rechte, die sie zur Erledigung ihrer Aufgaben benötigen. Über diese Rechte wird ebenfalls geregelt welche Software-Module (z.B. Einkauf, Auftragsverarbeitung, Personal) und damit welche Daten sichtbar sind.

4
Weitergabekontrolle/Übermittlungskontrolle

Maßnahmen zur Organisation der Datenübertragung Zur Organisation der Datenübertragung wurden folgende Maßnahmen getroffen: Dokumentation und Regelung der Übermittlungswege/-Stellen Speicher-, Ablageort: Daten werden auch sicheren Server gespeichert, Zugriff haben zur Mitarbeiter mit spezieller Berechtigung

Mitbringen von privaten Datenträgern Das Mitbringen von privaten Datenträgern ist folgendermaßen geregelt: generelles Verbot

kuravisma

Nutzung von Online-Banking- RS Marion Das Online-Banking wird mit folgendem Programm ausgeführt: Direct Banking

Regelungen beim Ausscheiden v. Mitarbeitern Beim Ausscheiden eines Mitarbeiters aus dem Betrieb wird das Benutzerkonto umgehend gesperrt

Bei der Versetzung von Mitarbeitern werden nicht mehr benötigte Rechte werden umgehend gelöscht.

Schutz der Daten vor Unbefugten bei der Übertragung Daten werden bei der Übertragung vor Unbefugten geschützt durch: Verschlüsselung

Sicherheitsmaßnahmen bei der Durchführung der Fernwartung Bei der Fernwartung gelten folgende Sicherheitsmaßnahmen: Fernwartung ist nur über einen unternehmenseigenen Login-Server erlaubt Zugriff ist zeitlich begrenzt Zugriff wird beobachtet Zugriff wird durch Log-Dateien detailliert protokolliert

Sicherheitsmaßnahmen bei der Nutzung des Internets Die Sicherheit der Nutzung des Internets wird durch folgend Maßnahmen gewährleistet: Einsatz Antivirenscanner (Hersteller automatisches update) Einsatz Firewall (Hersteller automatisches Update) Verwendung von https (SSL, TLS) FTP Verwendung Intrusion Detection System (IDS) Intrusion Prevention System (IPS) VPN

Sicherheitsmaßnahmen bei der Nutzung von Online-Banking Die Sicherheit des Online-Bankings wird durch folgende Maßnahmen gewährleistet: Push- Tan, SMS-Tan (je nach Bank)

Sicherheitsmaßnahmen bei der Versendung. E-Mails Bei der Versendung von E-Mails werden folgende Sicherheitsmaßnahmen getroffen. E-Mails werden: immer verschlüsselt bei sensiblen Daten (S/MiME, PGB) verschlüsselt

Sicherheitsmaßnahmen bei externen Dienstleistern, Dienstleistung (z.B. Reparatur) erfolgt außerhalb des Betriebs Werden Dienstleistungen außerhalb des Betriebes erbracht, werden folgende Sicherheitsmaßnahmen getroffen: Daten werden verschlüsselt

Verantwortlicher für die Genehmigung der Fernwartung Die Genehmigung zur Durchführung einer Fernwartung wird erteilt durch: Geschäftsführer Abteilungsleiter IT-Administratoren

kuravisma

Vernichtung von Datenträgern Datenträger werden vernichtet durch: magnetische Datenträger: durch ein gesichertes Verfahren mehrfaches Überschreiben Physisches Vernichtung zertifizierter externer Entsorger oder Shredder inhouse Papierakten: Aktenvernichter zertifizierter Entsorger Vernichtung wird dokumentiert

Verschlüsselung von Daten beim Transport
Beim Transport werden folgende Daten verschlüsselt: sensible Daten

Verwahrung von unbenutzten Datenträgern
Unbenutzte Datenträger werden folgendermaßen verwahrt: Verschlossener Schrank Tresor Verschlossener Raum

5 Eingabekontrolle/Plausibilitätskontrolle/Transaktionskontrolle

Installation von neuer Software Folgende Sicherheitsmaßnahmen gelten bei der Installation von neuer Software: Anti-Viren Scan Integritätsprüfung

Intervalle der Überprüfung durch Antiviren-Software
Eine Überprüfung durch Antiviren-Software findet statt: laufend

Netzwerkdokumentation Die Erstellung einer Netzwerkdokumentation erfolgt: Regelmäßig Speicher-, Ablageort: Google Docs/DC1 Hinweis: Die Mindestanforderung an eine Netzwerkdokumentation sollte einem bereinigten Netzplan entsprechen. Handelt es sich um Auftragsdatenverarbeitung, sollte darüber hinaus vom Auftragnehmer eine Anwendungslandkarte mit den Informationsflüssen der beauftragten IT-Umgebung bereitgestellt werden.

Schutz vor Schadsoftware Das System wird folgendermaßen vor Schadsoftware geschützt:
Antiviren-Software: Fortinet Antivirenscan, MS Defender
Firewall: Fortinet 6

Speicherung von Daten und Programmen Daten und Programme werden folgendermaßen gespeichert: in unterschiedlichen Verzeichnissen

kuravisma

Überprüfung fremder Datenträger Für die Benutzung fremder Datenträger gelten folgende Sicherheitsmaßnahmen: Benutzung fremder Datenträger ist ausgeschlossen

Update der Anwendungsprogramme
Updates der Anwendungsprogramme erfolgen: automatisch

Update des Betriebssystems Die Installation von sicherheitsrelevanten Updates des Betriebssystems erfolgt: Umgehend automatisch

Update des Schadsoftwareschutzes
Update des Schadsoftwareschutzes erfolgen: automatisch

6 Auftragskontrolle/Vertrags-Konformitätskontrolle

Maßnahmen zur Gewährleistung, dass Datenverarbeitung weisungsgemäß stattfindet Durch folgende Maßnahmen wird gewährleistet, dass die Verarbeitung der Daten weisungsgemäß ausgeführt wird: schriftlicher Vertrag Auftraggeber erhält Datenausgaben zur Kontrolle Kontrolle vor Ort durch Auftraggeber möglich

7 Verfügbarkeitskontrolle

Anzahl der Generationen der Sicherheitskopien
Sicherheitskopien werden nach dem Generationenprinzip erstellt. Anzahl der Generationen: Großvater-Vater-Sohn-Prinzip

Archivierung wichtiger E-Mails Wichtige E-Mails werden folgendermaßen archiviert: automatisch

Archivordnung Eine Archivordnnung liegt vor
Hinweis: In einer Archivordnung wird z.B. geregelt welche Dokumente archiviert werden Wer der Verantwortliche ist Wann welche Daten archiviert werden Aufbewahrungsfristen Löschfristen Anforderungen an Einsicht, Ausgabe der Daten

Archivverwalter Der Archivverwalter unseres Unternehmens ist:
Frau Marion Richter

Aufbewahrung Backupmedien Die Backupmedien werden aufbewahrt:
Tresor Serverraum

Backup-Methode Bei einem Backup wird Folgendes gesichert: Totalsicherung
Datenbestände veränderte Daten

Dokumentation Backupverfahren Das Backupverfahren wird dokumentiert
regelmäßig

Gesetzlichen Aufbewahrungspflichten Die gesetzlichen Aufbewahrungspflichten werden eingehalten. Die Einhaltung wird kontrolliert.

Klimatisierung des Serverraums
Der Serverraum ist klimatisiert

Kontrolle Backupverfahren Das Backupverfahren wird kontrolliert
regelmäßig, durch Geschäftsführer
IT-Administratoren

Schutzmaßnahmen des Archivs Das Archiv ist durch folgende Maßnahmen geschützt: eigener Raum, verschlossen Zugang nur für Berechtigte
Archivverwalter vor Ort

Zeitintervall Backup Ein Backup wird erstellt gemäß Backupplan
https://docs.google.com/spreadsheets/d/1MYY78hlbQ41S3gDex_RwPVgOo0JaS0EkrWIeA4FcfWE/edit#gid=0

8 Prüfung der Betriebsorganisation und Rechenschaftspflicht

Organisatorische Maßnahmen zur Einhaltung des Datenschutzes bzgl. der Daten Durch folgende organisatorische Maßnahmen wird die Einhaltung des Datenschutzes bzgl. der Daten gewährleistet: Dokumentation aller Programme Regelung der Aufbewahrung/Archivierung aller Protokolle Verfahren für die Erteilung von Zugangsberechtigungen

kuravisma

Organisatorische Maßnahmen zur Einhaltung des Datenschutzes bzgl. der Rechte der Betroffenen Durch folgende organisatorische Maßnahmen wird die Einhaltung des Datenschutzes bzgl. der Rechte der Betroffenen gewährleistet: Geltendmachung der Rechte (Auskunft, Löschung usw.) werden umgehend bearbeitet und dokumentiert Einhaltung des Schutzniveaus der Art. 44 ,46, 49 DS-GVO bei Übertragung in Drittländer

Organisatorische Maßnahmen zur Einhaltung des Datenschutzes bzgl. Mitarbeiter Durch folgende organisatorische Maßnahmen wird die Einhaltung des Datenschutzes durch Mitarbeiter gewährleistet: Verarbeitungsverzeichnis vollständig und aktuell Mitarbeiterschulungen zum Datenschutz Vertraulichkeitsverpflichtungen für Mitarbeiter externer Datenschutzbeauftragter Fachkundenachweis des Datenschutzbeauftragten Vertraulichkeitsverpflichtungen freier Mitarbeiter Vertrag mit Auftragsverarbeiter

Diese Angaben beziehen sich auf den Serverraum in unserem Unternehmen. Die Web-Applikation wird extern gehostet, die dies professionell macht und gesonderte Sicherheitsstandards verwirklicht hat.