

# Inhalt

<b>Einleitung</b> .....	<b>9</b>
<b>ORGANISATION UND PERSONAL</b>	
<b>1. Personal</b> .....	<b>12</b>
Geregeltes Einarbeiten neuer Mitarbeiter.....	12
Geregeltes Ausscheiden von Mitarbeitern .....	13
Vertretungsregelungen.....	13
Regelungen für externe Mitarbeiter und Fremdpersonal .....	13
Dokumentation von Aufgaben und Zuständigkeiten.....	14
Überprüfen von Zuverlässigkeit und Vertrauenswürdigkeit.....	14
Mitarbeiter regelmäßig schulen & sensibilisieren.....	14
Störungen des Betriebsklimas vermeiden .....	14
Ansprechperson für Fragen zu Datenschutz und IT-Sicherheit .....	15
<b>2. Sensibilisieren und schulen</b> .....	<b>15</b>
Vorbildfunktion der Unternehmensleitung und Führungskräfte .....	15
Ansprechperson für Fragen zu Datenschutz und IT-Sicherheit .....	16
Sensibilisierungsmaßnahmen und Schulungen .....	16
Spezielle Schulung von exponierten Personen.....	16
<b>3. Berechtigungsmanagement</b> .....	<b>17</b>
Geregeltes Einrichten, Ändern & Entziehen von Berechtigungen.....	17
Dokumentation der zugelassenen Benutzer und Rechteprofile .....	17
Zutritts- und Zugangsberechtigungen sowie Zugriffsrechte .....	18
Regelungen für sichere Passwörter und deren Handhabung .....	18
Identifikation und Authentisierung .....	18
<b>VORGEHENSWEISEN</b>	
<b>4. Datensicherung</b> .....	<b>20</b>
Regelmäßige Datensicherungen.....	20
Beachten von rechtlichen Einflussfaktoren .....	21
Funktionstests und Überprüfung der Wiederherstellbarkeit .....	21
Regelungen für die Online-Datensicherung.....	21
Sicherungskopie der eingesetzten Anwendungen .....	21
Geeignetes Aufbewahren der Backup-Datenträger .....	21
Verschlüsseln von gesicherten Daten .....	22
<b>5. Löschen und vernichten</b> .....	<b>22</b>
Verfahren zum Löschen oder Vernichten von Datenträgern.....	22
Löschen von Daten auf eingebauten Datenträgern .....	23
Vernichten von Datenträgern durch externe Dienstleister .....	23

## BETRIEB IM ALLTAG

<b>6. Schutz vor Schadprogrammen .....</b>	<b>26</b>
Nutzen systemspezifischer Schutzmechanismen .....	26
Betrieb von geeigneten Viren-Schutzprogrammen.....	26
Aktualisieren der eingesetzten Viren-Schutzprogramme.....	26
Sensibilisieren und Verpflichten der Benutzer .....	26
Sicherer Umgang mit nicht vertrauenswürdigen Dateien.....	27
Sicherer Einsatz von Datenträgern von Dritten .....	27
<b>7. Outsourcing von Aufgaben an Dritte.....</b>	<b>27</b>
Auswahl geeigneter Outsourcing-Dienstleister.....	28
Vertragsgestaltung mit Outsourcing-Dienstleistern .....	28
Notfallvorsorge beim Outsourcing .....	28
Geordnetes Beenden eines Outsourcing-Verhältnisses.....	28
<b>8. Einsatz von Cloud-Lösungen.....</b>	<b>29</b>
Sicherheitskonzept für die Cloud-Nutzung.....	29
Sorgfältige Auswahl von Cloud-Dienstleistern.....	29
Vertragsgestaltung mit Cloud-Dienstleistern.....	30
Notfallkonzept für Cloud-Dienstleistungen .....	30
Geordnetes Beenden von Cloud-Nutzungsverhältnissen.....	30
Durchführen eigener Datensicherungen.....	30

## NOTFALLMANAGEMENT

<b>9. Notfallmanagement .....</b>	<b>32</b>
Notfallhandbuch .....	32
Mitarbeiter in das Notfallmanagement integrieren .....	32
Regelmäßiges Überprüfen und Verbessern .....	32
Notfallvorsorge für ausgelagerte Aufgaben.....	32

## ANWENDUNGEN

<b>10. Office-Anwendungen .....</b>	<b>34</b>
Bezug von Office-Anwendungen aus sicheren Quellen.....	34
Einschränken von aktiven Inhalten .....	34
Achtsames Öffnen von Dokumenten aus externen Quellen .....	34
Sicherer laufender Betrieb von Office-Anwendungen.....	35
Sicheres Installieren und Konfigurieren.....	35
Verzicht auf Cloud-Speicherung .....	35
<b>11. Internet-Browser .....</b>	<b>35</b>
Verschlüsseln der Datenübertragung.....	36
Einsatz digitaler Zertifikate .....	36
Versionsprüfung und aktualisieren des Internet-Browsers.....	36

Sicheres Passwort-Management im Internet-Browser.....	37
Datenschutzeinstellungen nutzen .....	37
Plug-ins und Erweiterungen einschränken.....	37
Automatisches Überprüfen auf schädliche Inhalte .....	37
<b>12. Mobile Anwendungen (Apps) .....</b>	<b>38</b>
Regeln für das Verwenden von Apps.....	38
Sichere Bezugsquellen für Apps .....	38
Einschränken von App-Berechtigungen .....	38
Zeitnahes Einspielen von Updates.....	39
Datenabfluss verhindern .....	39
Sicheres Deinstallieren von Apps .....	39
<b>13. File-Server (Daten-Server).....</b>	<b>39</b>
Geeignetes Aufstellen von File-Servern.....	40
Einsatz von Viren-Schutzprogrammen.....	40
Regelmäßige Datensicherung.....	40
Verschlüsseln der gespeicherten Daten.....	40
<b>14. Microsoft Exchange und Outlook.....</b>	<b>41</b>
Geeignetes Berechtigungsmanagement.....	41
Regelmäßige Datensicherung von Microsoft Exchange .....	41
Sicherer Betrieb von Microsoft Exchange.....	41
Sicheres Konfigurieren von Microsoft Exchange-Servern.....	41
Sichere (zentrale) Basiseinstellungen von Outlook.....	42
Notfallplan für den Ausfall von Microsoft Exchange und Outlook .....	42

## IT-SYSTEME

<b>15. Allgemeiner Client (Arbeitsplatzrechner).....</b>	<b>44</b>
Eindeutiges Identifizieren jedes Benutzers .....	44
Rollentrennung (Benutzer, Administrator, usw.).....	44
Regelmäßige Datensicherung.....	44
Automatische und manuelle Bildschirmsperre.....	45
Einsatz von Viren-Schutzprogrammen.....	45
Protokollierung.....	45
Sicherheitsrichtlinie für Clients .....	45
Zeitnahes Installieren von Updates und Patches .....	45
Sicheres Installieren und Konfigurieren von Clients .....	45
Deaktivieren und Deinstallieren nicht benötigter Komponenten .....	46
Nutzen sicherer Verbindungen .....	46
Restriktive Rechtevergabe.....	46
Abmelden nach Aufgabenerfüllung.....	46
Sicherer Umgang mit Wechseldatenträgern.....	46

Benutzerrichtlinie zur sicheren IT-Nutzung .....	47
Geregelte Außerbetriebnahme eines Clients .....	47
Verschlüsseln von Clients .....	47
<b>16. Laptops.....</b>	<b>47</b>
Sicheres mobiles Arbeiten an Laptops.....	47
Zugriffsschutz am Laptop .....	48
Einsatz von Personal Firewalls .....	48
Einsatz von Viren-Schutzprogrammen.....	48
Regelmäßige Datensicherung.....	48
Sicherheitsrichtlinien für Laptops.....	48
Sicherer Anschluss von Laptops an Datennetze .....	49
Sicherer Fernzugriff von unterwegs.....	49
Zeitnahes Melden von Verlusten .....	49
Verschlüsseln von Laptops .....	49
Sicheres Aufbewahren von Laptops.....	49
Geeigneter Sichtschutz .....	50
Einsatz von Diebstahl-Sicherungen .....	50
<b>17. Smartphones und Tablets.....</b>	<b>50</b>
Sichere Grundkonfiguration mobiler Endgeräte.....	50
Verwenden eines angemessenen Zugriffsschutzes.....	51
Regelmäßige Updates von Betriebssystem und Apps .....	51
Eingeschränkter Zugriff auf Daten.....	51
Klare Verhaltensregeln bei Sicherheitsvorfällen .....	51
Installieren von Apps nur aus sicheren Quellen.....	52
Verschlüsseln des Datenspeicher.....	52
Verwendung nicht personalisierter Gerätenamen .....	52
Schutz vor Phishing und Schadprogrammen.....	52
Deaktivieren nicht benutzter Kommunikationsschnittstellen .....	52
Verwendung der SIM-Karten-PIN .....	52
Eingeschränktes Verwenden eines Sprachassistenten.....	52
Sicheres Aufbewahren von Smartphones und Tablets .....	53
Nutzen von getrennten Arbeitsumgebungen .....	53
<b>18. Mobile Datenträger .....</b>	<b>53</b>
Sensibilisieren der Mitarbeiter zum sicheren Umgang.....	53
Sofortiges Melden von Verlust mobiler Datenträger .....	54
Sicherungskopien von übermittelten Daten .....	54
Sicheres Löschen von mobilen Datenträgern .....	54
Verschlüsseln von Datenträgern.....	54

## NETZE UND KOMMUNIKATION

<b>19. Drahtlose Netzwerke (WLAN)</b> .....	<b>56</b>
Planen und Installieren von WLANs .....	56
Sensibilisieren und schulen der WLAN-Benutzer.....	56
Sicheres Nutzen von WLAN in unsicheren Umgebungen .....	57
Sicheres Gäste-WLAN .....	57
<b>20. Firewall</b> .....	<b>57</b>
Planen und Installieren von Firewalls .....	57
Zeitnahes Einspielen von Updates und Patches.....	58
Regelmäßige Datensicherung.....	58
<b>21. VPN-Verbindungen</b> .....	<b>58</b>
Sicheres Installieren und Konfigurieren .....	58
Sperren nicht mehr benötigter VPN-Zugänge.....	59
Sicheres Anbinden eines externen Netzes.....	59
Integrieren von VPN-Komponenten in eine Firewall .....	59

## INFRASTRUKTUR

<b>22. Gebäude, allgemein</b> .....	<b>62</b>
Geeignete Lage sensibler Bereiche .....	62
Einhalten von Brandschutzvorschriften .....	63
Branderkennung in Gebäuden (Rauch- und Brandmelder).....	63
Handfeuerlöscher .....	63
Geschlossene Fenster und Türen.....	63
Sichere Türen und Fenster .....	63
Einbruchsschutz .....	64
Zutrittsregelung und -kontrolle .....	64
Einrichten eines Empfangsdienstes .....	64
Rauchverbot.....	64
Schlüsselverwaltung.....	64
Organisatorische Vorgaben für die Gebäudereinigung .....	65
<b>23. Datenträgerarchiv</b> .....	<b>65</b>
Handfeuerlöscher .....	65
Zutrittsregelung und -kontrolle .....	65
Geschlossene Fenster und abgeschlossene Türen.....	65
Verwenden von Schutzschranken .....	66
Sichere Türen und Fenster .....	66
Kein gemischtes Nutzen des Datenträgerarchivs .....	66
<b>24. Büroarbeitsplatz</b> .....	<b>66</b>
Geeignetes Auswählen und Nutzen eines Büroraumes .....	66
Geschlossene Fenster und abgeschlossene Türen.....	67

Zutrittsregelungen und -kontrolle .....	67
Aufgeräumter Arbeitsplatz (Clean Desk-Politik) .....	67
Geeignetes Aufbewahren von Dokumenten und Datenträger.....	68
Einsatz von Diebstahlsicherungen.....	68
<b>25. Häuslicher Arbeitsplatz.....</b>	<b>68</b>
Geeignetes Einrichten eines häuslichen Arbeitsplatzes.....	68
Sicheres Verwahren von geschäftlichen Dokumenten.....	69
Sicherer Transport von Arbeitsmaterial .....	69
Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz .....	69
Aufgeräumter Arbeitsplatz (Clean Desk-Politik) .....	69
Sicheres Entsorgen von vertraulichen Informationen .....	70
<b>26. Mobiler Arbeitsplatz .....</b>	<b>70</b>
Geeignetes Auswählen eines mobilen Arbeitsplatzes .....	71
Regelungen für mobile Arbeitsplätze .....	71
Zutritts- und Zugriffsschutz .....	71
Sicheres Arbeiten mit fremden IT-Systemen .....	71
Zeitnahe Verlustmeldung .....	72
Sicheres Entsorgen von vertraulichen Informationen .....	72
Verschlüsselung tragbarer IT-Systeme und Datenträger .....	72
<b>27. Besprechungs-, Veranstaltungs- und Schulungsräume .....</b>	<b>73</b>
Sicheres Nutzen und Hinterlassen.....	73
Beaufsichtigen von Besuchern .....	73
Geschlossene Fenster und Türen .....	73
Keine fliegende Verkabelung.....	74
Einrichten sicherer Netzzugänge.....	74