

Datenschutz- Managementsystem

November 2011

Einleitung

Das Datenschutz-Managementsystem (DSMS) basiert auf den Standards ISO/IEC 27001:2005 (ISO 27001) und ISO/IEC 27002:2005 (ISO 27002), welche mit den datenschutzrechtlichen Anforderungen ergänzt werden. Die Risikoanalyse wird durch eine Konformitätsanalyse ersetzt und die Anforderungen an Datenschutz und Informationssicherheit auf den Grundlagen des IDG definiert.

Die datenschutzrechtlichen Anforderungen können in Anhang A 15.1.4 des Standards ISO 27002 integriert werden, da ein Informationssicherheits-Managementsystem (ISMS) auch die rechtlichen Vorgaben zum Datenschutz erfüllen muss. Ein bestehendes zertifiziertes ISMS ist jedoch nicht Voraussetzung einer Zertifizierung nach IDG, kann aber als Grundlage dienen, indem Abweichungen analysiert und zusätzliche Massnahmen umgesetzt werden.

Die folgenden Anforderungen basieren auf den Bestimmungen des Gesetzes über die Information und den Datenschutz (IDG). Je nach Bereich sind diese mit den Anforderungen aus den spezialrechtlichen Grundlagen zu ergänzen.

Die Planung, Umsetzung, Überprüfung, Instandhaltung und Verbesserung des DSMS nach ISO 27001 sind nicht Bestandteile dieses Dokuments. Diesbezüglich wird auf die Prozesse zu ISO 27001 verwiesen.

Im Folgenden werden die datenschutzrechtlichen Anforderungen, welche den Inhalt des DSMS nach ISO 27002 definieren, beschrieben.

Datenschutzrechtliche Anforderungen

- 1. Gesetzmässigkeit**
 - 1.1. Gesetzliche Grundlage

- 2. Verhältnismässigkeit**
 - 2.1. Verhältnismässige Bearbeitung

- 3. Zweckbindung**
 - 3.1. Zweckbindung, Zweckänderung

- 4. Erkennbarkeit**
 - 4.1. Erkennbarkeit, Informationspflicht

- 5. Informationssicherheit**
 - 5.1. Vertraulichkeit, Integrität und Verfügbarkeit
 - 5.2. Zurechenbarkeit und Nachvollziehbarkeit
 - 5.3. Weitere Sicherheitsmassnahmen gemäss Informatiksicherheitsverordnung
 - 5.4. Managementsystem zur Umsetzung von Ziff. 5.1., 5.2. und 5.3.

- 6. Vermeidung des Personenbezugs**
 - 6.1. Datenvermeidung, Datensparsamkeit

- 7. Informationszugang**
 - 7.1. Auskunftsrecht

- 8. Rechtsansprüche**
 - 8.1. Rechtsansprüche

- 9. Vorabkontrolle**
 - 9.1. Vorabkontrolle

- 10. Datenbearbeitung im Auftrag**
 - 10.1. Datenbearbeitung durch Dritte

- 11. Aufbewahrung, Archivierung**
 - 11.1. Aufbewahrung
 - 11.2. Archivierung

- 12. Anhänge**
 - 12.1. Anhang 1: Zu den minimalen Controls zugeordnete Massnahmen (Ziff. 5.1.)
 - 12.2. Anhang 2: Beispiel einer Clause und der zugeordneten Massnahmen im Detail

1. **Gesetzmässigkeit**

Personendaten dürfen durch das öffentliche Organ bearbeitet werden, wenn dies zur Erfüllung der gesetzlich umschriebenen Aufgabe geeignet und erforderlich ist. Das Bearbeiten besonderer Personendaten muss in einer formell-gesetzlichen Grundlage geregelt sein.

1.1 **Gesetzliche Grundlage (§ 8 IDG)**

Massnahmen

Sicherstellen, dass das Bearbeiten von Personendaten durch öffentliche Organe aus einer gesetzlich umschriebenen Aufgabe abgeleitet werden kann und geeignet und erforderlich ist (§ 8 Abs. 1 IDG).

Sicherstellen, dass das Bearbeiten von besonderen Personendaten in einer hinreichend bestimmten Regelung in einem formellen Gesetz festgehalten ist (§ 8 Abs. 2 IDG).

Umsetzung

- Das für die Datenbearbeitung verantwortliche Organ ist bekannt.
- Das Bearbeiten von Personendaten kann aus einem Gesetz, einer Verordnung oder einem anderen durch die Behörden erlassenen Reglement abgeleitet werden.
- Das Bearbeiten von besonderen Personendaten kann auf ein formelles Gesetz abgestützt werden. Das verantwortliche Organ, der Zweck der Bearbeitung, die Datenkategorien sowie die Datenempfänger sind bezeichnet.
- Ein Bearbeiten zu nicht personenbezogenem Zweck kann erfolgen, wenn die Daten anonymisiert werden.
- Eine Datenbekanntgabe erfolgt nur unter den Voraussetzungen der §§ 16 und 17 IDG.
- Eine Datenbekanntgabe ins Ausland erfolgt nur unter Einhaltung der zu den §§ 16 und 17 IDG zusätzlichen Voraussetzungen von § 19 IDG.
- Eine Datenbekanntgabe für nicht personenbezogene Zwecke kann erfolgen, wenn keine rechtliche Bestimmung entgegensteht.
- Personendaten werden nur durch ein Abrufverfahren zugänglich gemacht werden, wenn dies ausdrücklich in einem Erlass vorgesehen ist.
- Besondere Personendaten werden nur durch ein Abrufverfahren zugänglich gemacht werden, wenn dies in einem formellen Gesetz vorgesehen ist.
- Instrumente für Datensperren sind im Rahmen der rechtlichen Voraussetzungen von § 22 IDG vorhanden und können umgesetzt werden.

2. Verhältnismässigkeit

Personendaten dürfen bearbeitet werden, wenn die Bearbeitung verhältnismässig, d.h. für den Zweck geeignet und erforderlich ist.

2.1 Verhältnismässige Bearbeitung (§ 8 IDG)

Massnahmen

Sicherstellen, dass nur diejenigen Daten bearbeitet werden, welche für die Aufgabenerfüllung geeignet und erforderlich sind.

Sicherstellen, dass die Prinzipien der Datenvermeidung und Datensparsamkeit eingehalten werden.

Umsetzung

- Die Datenbeschaffung ist auf den Zweck und auf die Aufgabenerfüllung abgestimmt.
- Es werden keine für den Zweck ungeeigneten und nicht erforderlichen Daten erhoben.
- Daten, bei welchen sich nachträglich herausstellt, dass sie nicht erforderlich sind, werden gelöscht. Die Archivierungsvorschriften bleiben vorbehalten.
- Datenbearbeitungssysteme werden auf den Einsatz von Privacy Enhancing Technology (PET) überprüft.
- Personendaten werden, wo möglich, anonymisiert.
- Falls eine Anonymisierung nicht möglich ist, wird eine Teilanonymisierung geprüft.
- Ist eine Anonymisierung oder Teilanonymisierung nicht möglich, wird eine Pseudonymisierung geprüft.

3. Zweckbindung

Das öffentliche Organ stellt sicher, dass Personendaten nur zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden, eine rechtliche Bestimmung eine anderweitige Zweckverwendung vorsieht oder im Einzelfall eine Einwilligung der betroffenen Person vorliegt.

Das öffentliche Organ gewährleistet, dass Personendaten zu einem nicht personenbezogenen Zweck nur bearbeitet werden, wenn diese anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind.

3.1. Zweckbindung, Zweckänderung (§ 9 IDG)

Massnahmen

Sicherstellen, dass die Bearbeitung der Daten nur zum dem Zweck erfolgt, zu dem die Daten erhoben wurden. Sicherstellen, dass beim Bearbeiten von besonderen Personendaten der Zweck in einem formellen Gesetz statuiert ist (§ 8 Abs. 2 IDG). Falls eine Zweckänderung erfolgt, sicherstellen, dass dies aufgrund einer rechtlichen Bestimmung der Einwilligung der betroffenen Person im Einzelfall beruht.

Umsetzung

- Überprüfen, ob die Daten zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden.
- Jede nachträgliche Zweckänderung muss nachvollziehbar sein.
- Das öffentliche Organ kontrolliert die Zweckverwendung mittels Stichproben.
- Eine Änderung des ursprünglichen Zwecks stützt sich auf eine rechtliche Grundlage oder die Einwilligung der Betroffenen.
- Überprüfen, ob bei Statistiken keine Rückschlüsse auf Personen mehr möglich sind.

4. Erkennbarkeit

Die Beschaffung von Personendaten und der Zweck ihrer Bearbeitung durch das öffentliche Organ müssen für die betroffenen Personen erkennbar sein.

Bei der Beschaffung von besonderen Personendaten ist der Inhaber der Datensammlung verpflichtet, die betroffene Person über den Zweck der Bearbeitung zu informieren.

4.1 Erkennbarkeit und Informationspflicht (§ 12 IDG)

Massnahmen

Sicherstellen, dass das öffentliche Organ Personendaten so beschafft, dass die Beschaffung und der Zweck der Bearbeitung für betroffene Personen erkennbar ist.

Bei der Beschaffung von besonderen Personendaten muss der Inhaber der Datensammlung betroffene Personen über den Zweck der Bearbeitung informieren.

Umsetzung

- Das öffentliche Organ stützt seine Datenbeschaffungen auf eine Rechtsgrundlage ab.
- Werden besondere Personendaten beschafft, muss der Zweck der einzelnen Bearbeitung aus der Rechtsgrundlage ersichtlich sein.
- Das öffentliche Organ macht ein Verzeichnis der Informationsbestände, die Personendaten beinhalten (§ 14 Abs. 4 IDG).

5. Informationssicherheit

Das öffentliche Organ schützt seine Informationen durch angemessene organisatorische und technische Massnahmen so, dass diese nicht unrechtmässig zur Kenntnis gelangen, richtig, vollständig und bei Bedarf vorhanden sind, einer Person zugerechnet werden können und Veränderungen erkennbar und nachvollziehbar sind.

5.1 Vertraulichkeit, Integrität und Verfügbarkeit (§ 7 IDG)

Massnahmen

Die folgende Liste enthält die gemäss „Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS“ und ISO 27002 minimalen Controls.

Clause ISO 27002	Titel	Sicherheitsziel
A.7.1 – 2	Management von organisationseigenen Werten	Vertraulichkeit (Klassifikation)
A.10.4.1 - 2	Schutz vor Schadsoftware und mobilem Programmcode	Integrität
A.10.5.1	Backup	Verfügbarkeit
A.10.6.1 - 2	Management der Netzsicherheit	Vertraulichkeit
A.10.7.1 - 4	Handhabung von Speicher- und Aufzeichnungsmedien	Vertraulichkeit
A.10.8.1 - 5	Austausch von Informationen	Vertraulichkeit
A.10.10.1 - 6	Überwachung	Vertraulichkeit
A.11.1 - 7	Zugangskontrolle	Vertraulichkeit
A.12.1 - 6	Beschaffung, Entwicklung und Wartung von Informationssystemen	Integrität
A.14.1.1 - 5	Sicherstellung des Geschäftsbetriebes (Business Continuity Management)	Verfügbarkeit
A.15.1.3	Schutz von organisationseigenen Aufzeichnungen	Verfügbarkeit

Die Zuordnung der vom BSI (Bundesamt für Sicherheit in der Informationstechnik, Deutschland) vorgeschlagenen Massnahmen zu den Controls ist in Ziff. 12.1., Anhang 1 „Zu den minimalen Controls zugeordnete Massnahmen“ ersichtlich (gemäss BSI-Dokument „Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz“). Die Anforderungen an die Umsetzung sind in Ziff. 5.4., „Managementsysteme zur Umsetzung der Ziff. 5.1. - 5.3.“ beschrieben.

5.2. Zurechenbarkeit und Nachvollziehbarkeit (§ 7 IDG)

Massnahmen

Für die Schutzziele Zurechenbarkeit und Nachvollziehbarkeit gemäss § 7 IDG sind folgende weitere Controls gemäss ISO 27002 einzurichten:

Clause ISO 27002	Titel
6.1.4, c	Authorization process for information processing facilities
8.1.1	Roles and responsibilities
8.1.3	Terms and conditions of employment
8.3.2	Return of assets
8.3.3	Removal of access rights
9.1.2	Physical entry controls
10.1.3	Segregation of duties
10.1.4	Separation of development, test and operational facilities
10.9.2	Online Transactions

Die Anforderungen an die Umsetzung sind in Ziff. 5.4., „Managementsysteme zur Umsetzung der Ziff. 5.1. - 5.3.“ beschrieben.

5.3. Weitere Sicherheitsmassnahmen gemäss Informatiksicherheitsverordnung

Massnahmen

Für die Stufe 3 gemäss der kantonalen Informatiksicherheitsverordnung (ISV) müssen immer alle zutreffenden Massnahmen und Bausteine aus dem BSI-Grundschatzkatalog geplant und umgesetzt werden. Für die Stufen 1 und 2 sind mindestens die Massnahmenkataloge der kantonalen Prüfstellen (Minimummassnahmen N1 und N2) zu beachten.

5.4 Managementsystem zur Umsetzung der Ziff. 5.1. – 5.3.

Die Umsetzung der Massnahmen im Bereich Informatiksicherheit erfolgt am besten über ein bestehendes Managementsystem, beispielsweise einem Qualitätsmanagementsystem oder einem Information Security Management System (Managementsystem für Informationssicherheit, ISMS). Zur dauerhaften Steuerung, Kontrolle und Verbesserung der Informatiksicherheit, respektive der Sicherheitsziele nach § 7 IDG, stellt das ISMS die notwendigen Verfahren und Regeln bereit. Das ISMS legt fest, wie die organisatorischen und technischen Massnahmen (des Informationssicherheits- respektive Datenschutzkonzepts) die rechtlichen Rahmenbedingungen einhalten sowie die gesetzmässige Informationsbearbeitung laufend sicherstellen.

6. Vermeidung des Personenbezugs

Das öffentliche Organ gestaltet Datenbearbeitungssysteme und -programme so, dass möglichst wenige Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind. Es löscht, anonymisiert oder pseudonymisiert solche Personendaten, sobald und soweit dies möglich ist.

6.1 Datenvermeidung, Datensparsamkeit (§ 11 IDG)

Massnahmen

Datenbearbeitungssysteme und -programme müssen so entwickelt werden, dass möglichst wenige Personendaten anfallen (Datensparsamkeit).

Sicherstellen, dass Datenbearbeitungssysteme mit Blick auf die Randdaten so entwickelt werden, dass, sobald und soweit möglich, Personendaten gelöscht, anonymisiert oder pseudonymisiert werden (Datenvermeidung).

Umsetzung

- Datenbearbeitungssysteme werden auf den Einsatz von Privacy Enhancing Technology (PET) überprüft.
- Personendaten werden, wo möglich, anonymisiert.
- Falls eine Anonymisierung nicht möglich ist, wird eine Teilanonymisierung geprüft.
- Ist eine Anonymisierung oder Teilanonymisierung nicht möglich, wird eine Pseudonymisierung geprüft.

7. Informationszugang

Das öffentliche Organ gewährleistet Zugang zu bei ihm vorhandenen Informationen und zu eigenen Personendaten.

7.1. Informationszugang (§ 20 IDG)

Massnahmen

Sicherstellen, dass sowohl Ersuchen zu Informationen im Sinne des Öffentlichkeitsprinzips als auch Auskunftersuchen betreffend die eigenen Daten durch das öffentliche Organ innert Frist behandelt und beantwortet werden.

Umsetzung

- Das öffentliche Organ macht ein Verzeichnis der Informationsbestände, die Personendaten beinhalten (§ 14 Abs. 4 IDG).
- Das für den Informationsbestand verantwortliche Organ hat die Prozesse zur Behandlung von Auskunftersuchen definiert und dokumentiert.
- Technische Systeme sind so gestaltet, dass Recherchen und eine vollständige Auskunft möglich sind.
- Auskünfte werden nur in den gesetzlich vorgesehenen Fällen verweigert, eingeschränkt oder aufgeschoben.
- Auskunftsverweigerungen oder -beschränkungen werden in einer Verfügung festgehalten.

8. Rechtsansprüche

Betroffene Personen können beim öffentlichen Organ Berichtigungs-, Vernichtungs-, Unterlassungs-, Beseitigungs- und Feststellungsansprüche geltend machen.

8.1. Rechtsansprüche (§ 21 IDG)

Massnahmen

Sicherstellen, dass Berichtigungs-, Vernichtungs-, Unterlassungs-, Beseitigungs- oder Feststellungsbegehren von betroffenen Personen im Falle von unrechtmässigen Datenbearbeitungen überprüft, bearbeitet und beantwortet werden.

Umsetzung

- Die Instrumente und Verfahren für die Ausübung des Berichtigungs-, Vernichtungs-, Unterlassungs-, Beseitigungs- und Feststellungsrechts wurden implementiert.
- Unrichtige Daten werden durch das öffentliche Organ berichtigt oder vernichtet.
- Widerrechtliche Datenbearbeitungen werden festgestellt, in der Folge unterlassen und die Folgen beseitigt.
- Die Widerrechtlichkeit wird festgestellt und dokumentiert.

9. Vorabkontrolle

Das öffentliche Organ unterbreitet eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen vorab der oder dem Beauftragten für den Datenschutz zur Prüfung.

9.1. Vorabkontrolle (§ 10 IDG)

Massnahmen

Datenbearbeitungen mit besonderen Risiken für die Rechte und Freiheiten müssen dem Datenschutzbeauftragten vorab zur Prüfung vorgelegt werden.

Umsetzung

- Datenbearbeitungen, welche ein im Sinne von § 24 IDV festgehaltenes Risiko beinhalten, wie z.B. ein Abrufverfahren, werden in der Planungsphase dem Datenschutzbeauftragten zur Vorabkontrolle vorgelegt.

10. Datenbearbeitung im Auftrag

Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht.

Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.

10.1. Datenbearbeitung durch Dritte (§ 6 IDG)

Massnahmen

Sicherstellen, dass das Übertragen einer Bearbeitung von Informationen an Dritte in einem Gesetz festgehalten oder in einem schriftlichen Vertrag dokumentiert ist. Sicherstellen, dass keine rechtlichen Bestimmungen entgegenstehen und dass die Daten nur so bearbeitet werden, wie dies das öffentliche Organ auch darf.

Umsetzung

- Es ist eine vertragliche Vereinbarung oder eine gesetzliche Bestimmung vorhanden, welche die Datenbearbeitung vorsieht und die Anforderungen von § 25 IDV erfüllt.
- Es stehen keine gesetzlichen oder vertraglichen Geheimhaltungspflichten entgegen.
- Betrifft es besondere Personendaten, liegt eine Genehmigung durch die vorgesetzte Behörde vor.
- Die Verantwortung ist klar definiert.
- Der Geltungsbereich der ISV ist abgeklärt und falls anwendbar, der Inhalt umgesetzt.
- Die Anwendbarkeit der AGB Sicherheit wurde abgeklärt und falls bejaht, in die Verträge einbezogen.
- Finden die AGB Sicherheit keine Anwendung, wird ein gleichwertiger Schutz durch das Einbinden ebenbürtiger Vertragsklauseln gewährleistet.
- Erfolgt die Auslagerung ins Ausland, werden zusätzliche Massnahmen analog derjenigen in § 19 IDG und § 22 IDV umgesetzt.

11. Aufbewahrung und Archivierung

Das öffentliche Organ bewahrt Informationen so lange auf, als es diese für das Verwaltungshandeln benötigt. Danach noch höchstens zehn Jahre, es sei denn, Rechts- oder Verjährungsfristen verlangen eine darüber hinausgehende Aufbewahrung.

Nach Ablauf der Aufbewahrungsfrist sind die Informationen dem zuständigen Archiv anzubieten. Informationen, die nicht zu archivieren sind, sind zu vernichten.

11.1. Aufbewahrung (§ 5 IDG)

Massnahmen

Sicherstellen, dass das öffentliche Organ die Informationen nur so lange aufbewahrt, als es diese benötigt. Die Aufbewahrungsfristen müssen durch das öffentliche Organ definiert und dokumentiert werden.

Umsetzung

- Aufbewahrungsfristen wurden definiert.
- Über die Aufbewahrungsfrist hinausgehende Verjährungs- und Rechtsmittelfristen wurden beachtet.
- Lösungsmechanismen sind Teil der technischen Lösung.

11.2. Archivierung (§ 5 IDG)

Massnahmen

Sicherstellen, dass Informationen und Findmittel nach Ablauf der Aufbewahrungsfrist archiviert werden.

Umsetzung

- Das öffentliche Organ hat die Informationen unabhängig von Form und Träger nach Ablauf der Aufbewahrungsfrist dem zuständigen Archiv zur Archivierung angeboten oder nach den Vorgaben des Archivgesetzes archiviert.

12. Anhänge

12.1 Anhang 1

Zu den minimalen Controls zugeordnete Massnahmen (Ziff. 5.1)

Clauses	Zugeordnete Massnahmen
A 7.1.1	BSI-Standard 100-2, Kapitel 4.2 Strukturanalyse B 1.0 Sicherheitsmanagement B 1.1 Organisation M 2.139 Ist-Aufnahme der aktuellen Netzsituation M 2.195 Erstellung eines Sicherheitskonzepts M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
A 7.1.2	M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
A 7.1.3	M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz M 1.34 Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz M 2.118 Festlegung einer Sicherheitspolitik für E-Mail-Nutzung M 2.119 Regelung für den Einsatz von E-Mail M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten M 2.226 Regelungen für den Einsatz von Fremdpersonal M 2.235 Richtlinien für die Nutzung von Internet-PCs M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung M 5.88 Vereinbarung über Datenaustausch mit Dritten
A 7.2.1	BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung B 1.0 Sicherheitsmanagement M 2.195 Erstellung eines Sicherheitskonzepts M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
A 7.2.2	BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung B 1.0 Sicherheitsmanagement M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
A.10.4.1	B 1.6 Schutz vor Schadprogrammen B 1.8 Behandlung von Sicherheitsvorfällen M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.10 Überprüfung des Software-Bestandes M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 2.154 Erstellung eines Sicherheitskonzeptes gegen Schadprogramme M 6.23 Verhaltensregeln bei Auftreten von Schadprogrammen
A.10.4.2	M 5.69 Schutz vor aktiven Inhalten B 1.6 Schutz vor Schadprogrammen M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit M 4.23 Sicherer Aufruf ausführbarer Dateien M 4.100 Firewalls und aktive Inhalte M 4.199 Vermeidung gefährlicher Dateiformate

A.10.5.1	B 1.4 Datensicherungskonzept M 6.20 Geeignete Aufbewahrung der Backup-Datenträger M 6.32 Regelmäßige Datensicherung M 6.41 Übungen zur Datenrekonstruktion
A.10.6.1	B 4.1 Heterogene Netze B 4.4 VPN M 2.38 Aufteilung der Administrationstätigkeiten M 2.169 Entwickeln einer Systemmanagementstrategie M 2.279 Erstellung einer Sicherheitsrichtlinie für Router und Switches M 4.79 Sichere Zugriffsmechanismen bei lokaler Administration M 4.80 Sichere Zugriffsmechanismen bei Fernadministration M 4.81 Audit und Protokollierung der Aktivitäten im Netz M 4.82 Sichere Konfiguration der aktiven Netzkomponenten M 5.7 Netzverwaltung M 5.9 Protokollierung am Server M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation M 5.71 Intrusion Detection und Intrusion Response Systeme
A.10.6.2	B 4.1 Heterogene Netze B 3.301 Sicherheitsgateway (Firewall) B 4.2 Netz- und Systemmanagement B 4.4 VPN B 4.5 LAN-Anbindung eines IT-Systems über ISDN M 4.133 Geeignete Auswahl von Authentifikations-Mechanismen M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
A.10.7.1	M 2.3 Datenträgerverwaltung B 5.14 Mobile Datenträger M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
A.10.7.2	B 1.15 Löschen und Vernichten von Daten M 2.431 Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen M 4.234 Geregelt Ausserbetriebnahme von IT-Systemen und Datenträgern
A.10.7.3	M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen B 5.2 Datenträgeraustausch B 5.3 E-Mail M 2.7 Vergabe von Zugangsberechtigungen M 2.42 Festlegung der möglichen Kommunikationspartner M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
A.10.7.4	M 2.25 Dokumentation der Systemkonfiguration M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
A.10.8.1	M 2.393 Regelung des Informationsaustausches B 3.402 Faxgerät B 3.403 Anrufbeantworter B 3.404 Mobiltelefon B 5.2 Datenträgeraustausch B 5.3 E-Mail B 5.14 Mobile Datenträger M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.398 Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten M 5.88 Vereinbarung über Datenaustausch mit Dritten

A.10.8.2	M 5.88 Vereinbarung über Datenaustausch mit Dritten M 2.45 Regelung des Datenträgeraustausches M 2.119 Regelung für den Einsatz von E-Mail M 2.393 Regelung des Informationsaustausches
A.10.8.3	M 5.23 Auswahl einer geeigneten Versandart M 2.3 Datenträgerverwaltung M 2.4 Regelungen für Wartungs- und Reparaturarbeiten M 2.44 Sichere Verpackung der Datenträger M 2.45 Regelung des Datenträgeraustausches M 2.112 Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
A.10.8.4	B 5.3 E-Mail M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 5.54 Schutz vor Mailüberlastung und Spam M 5.56 Sicherer Betrieb eines Mailservers M 5.108 Kryptographische Absicherung von E-Mail
A.10.8.5	M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz M 2.7 Vergabe von Zugangsberechtigungen M 2.8 Vergabe von Zugriffsrechten M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.338 Erstellung von zielgruppengerechten Sicherheitsrichtlinien
A.10.10.1	M 2.64 Kontrolle der Protokolldateien M 2.110 Datenschutzaspekte bei der Protokollierung M 4.81 Audit und Protokollierung der Aktivitäten im Netz M 5.9 Protokollierung am Server
A.10.10.2	M 2.64 Kontrolle der Protokolldateien M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems M 4.81 Audit und Protokollierung der Aktivitäten im Netz M 5.9 Protokollierung am Server
A.10.10.3	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.110 Datenschutzaspekte bei der Protokollierung M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen M 4.93 Regelmässige Integritätsprüfung M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien
A.10.10.4	M 2.64 Kontrolle der Protokolldateien M 2.110 Datenschutzaspekte bei der Protokollierung M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems M 4.5 Protokollierung der TK-Administrationsarbeiten
A.10.10.5	M 2.215 Fehlerbehandlung M 4.81 Audit und Protokollierung der Aktivitäten im Netz
A.10.10.6	M 4.227 Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation

A.11.1.1	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle B 5.15 Allgemeiner Verzeichnisdienst M 2.5 Aufgabenverteilung und Funktionstrennung M 2.7 Vergabe von Zugangsberechtigungen M 2.8 Vergabe von Zugriffsrechten M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen
A.11.2.1	M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile M 2.63 Einrichten der Zugriffsrechte M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern M 4.13 Sorgfältige Vergabe von IDs M 2.402 Zurücksetzen von Passwörtern
A.11.2.2	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.20 Kontrolle bestehender Verbindungen M 2.38 Aufteilung der Administrationstätigkeiten M 4.312 Überwachung von Verzeichnisdiensten
A.11.2.3	M 2.11 Regelung des Passwortgebrauchs M 2.22 Hinterlegen des Passwortes M 4.7 Änderung voreingestellter Passwörter M 4.133 Geeignete Auswahl von Authentifikations-Mechanismen M 5.34 Einsatz von Einmalpasswörtern
A.11.2.4	M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile M 2.199 Aufrechterhaltung der Informationssicherheit
A.11.3.1	M 2.11 Regelung des Passwortgebrauchs M 2.22 Hinterlegen des Passwortes M 3.5 Schulung zu Sicherheitsmaßnahmen M 3.26 Einweisung des Personals in den sicheren Umgang mit IT M 4.7 Änderung voreingestellter Passwörter
A.11.3.2	M 4.2 Bildschirmsperre M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger M 1.46 Einsatz von Diebstahl-Sicherungen M 2.37 "Der aufgeräumte Arbeitsplatz" M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
A.11.3.4	M 2.37 "Der aufgeräumte Arbeitsplatz" B 3.406 Drucker, Kopierer und Multifunktionsgeräte M 4.1 Passwortschutz für IT-Systeme M 4.2 Bildschirmsperre
A.11.4.1	M 2.172 Entwicklung eines Konzeptes für die Internet-Nutzung M 2.214 Konzeption des IT-Betriebs
A.11.4.2	B 4.4 VPN B 4.5 LAN-Anbindung eines IT-Systems über ISDN M 2.7 Vergabe von Zugangsberechtigungen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle
A.11.4.3	M 4.82 Sichere Konfiguration der aktiven Netzkomponenten M 4.133 Geeignete Auswahl von Authentifikations-Mechanismen

A.11.4.4	B 4.4 VPN M 4.80 Sichere Zugriffsmechanismen bei Fernadministration
A.11.4.5	M 5.77 Bildung von Teilnetzen M 5.61 Geeignete physikalische Segmentierung M 5.62 Geeignete logische Segmentierung
A.11.4.6	B 3.301 Sicherheitsgateway (Firewall) B 4.4 VPN M 4.238 Einsatz eines lokalen Paketfilters M 5.13 Geeigneter Einsatz von Elementen zur Netzkopplung
A.11.4.7	B 3.301 Sicherheitsgateway (Firewall) B 3.302 Router und Switches M 4.82 Sichere Konfiguration der aktiven Netzkomponenten M 5.61 Geeignete physikalische Segmentierung M 5.70 Adressumsetzung - NAT (Network Address Translation)
A.11.5.1	M 4.15 Gesichertes Login M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.321 Planung des Einsatzes von Client-Server-Netzen M 2.322 Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz M 4.133 Geeignete Auswahl von Authentifikations-Mechanismen
A.11.5.2	M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle
A.11.5.3	M 2.11 Regelung des Passwortgebrauchs M 4.133 Geeignete Auswahl von Authentifikations-Mechanismen
A.11.5.4	M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien
A.11.5.5	M 3.18 Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung M 4.2 Bildschirmsperre M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme
A.11.5.6	M 4.16 Zugangsbeschränkungen für Accounts und / oder Terminals M 4.133 Geeignete Auswahl von Authentifikations-Mechanismen
A.11.6.1	M 2.8 Vergabe von Zugriffsrechten M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle
A.11.6.2	M 5.77 Bildung von Teilnetzen M 5.61 Geeignete physikalische Segmentierung M 5.62 Geeignete logische Segmentierung
A.11.7.1	B 2.10 Mobiler Arbeitsplatz B 3.203 Laptop B 3.404 Mobiltelefon B 3.405 PDA M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
A.11.7.2	B 5.8 Telearbeit

A.12.1.1	M 2.80 Erstellung eines Anforderungskataloges für Standardsoftware B 1.10 Standardsoftware B 1.9 Hard- und Software-Management M 2.62 Software-Abnahme- und Freigabe-Verfahren M 2.66 Beachtung des Beitrags der Zertifizierung für die Beschaffung M 2.83 Testen von Standardsoftware
A.12.2.1	M 2.83 Testen von Standardsoftware M 2.363 Schutz gegen SQL-Injection
A.12.2.2	M 2.378 System-Entwicklung M 2.82 Entwicklung eines Testplans für Standardsoftware M 2.83 Testen von Standardsoftware
A.12.2.3	M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen B 1.7 Kryptokonzept
A.12.2.4	M 2.83 Testen von Standardsoftware
A.12.3.1	B 1.7 Kryptokonzept M 2.161 Entwicklung eines Kryptokonzepts
A.12.3.2	B 1.7 Kryptokonzept M 2.46 Geeignetes Schlüsselmanagement M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens
A.12.4.1	B 1.9 Hard- und Software-Management B 1.10 Standardsoftware M 2.62 Software-Abnahme- und Freigabe-Verfahren M 2.85 Freigabe von Standardsoftware M 2.86 Sicherstellen der Integrität von Standardsoftware M 2.87 Installation und Konfiguration von Standardsoftware M 2.88 Lizenzverwaltung und Versionskontrolle von Standardsoftware
A.12.4.2	M 2.83 Testen von Standardsoftware
A.12.4.3	M 2.378 System-Entwicklung M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.62 Software-Abnahme- und Freigabe-Verfahren M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien
A.12.5.1	B 1.14 Patch- und Änderungsmanagement M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.34 Dokumentation der Veränderungen an einem bestehenden System M 2.62 Software-Abnahme- und Freigabe-Verfahren
A.12.5.2	B 1.14 Patch- und Änderungsmanagement M 2.62 Software-Abnahme- und Freigabe-Verfahren
A.12.5.3	M 2.9 Nutzungsverbot nicht freigegebener Software
A.12.5.4	M 2.224 Vorbeugung gegen trojanische Pferde M 2.66 Beachtung des Beitrags der Zertifizierung für die Beschaffung M 2.87 Installation und Konfiguration von Standardsoftware M 2.214 Konzeption des IT-Betriebs M 3.10 Auswahl eines vertrauenswürdigen Administrators und Vertreters M 4.35 Verifizieren der zu übertragenden Daten vor Versand

A.12.5.5	<p>B 1.11 Outsourcing</p> <p>M 2.250 Festlegung einer Outsourcing-Strategie</p> <p>M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben</p> <p>M 2.252 Wahl eines geeigneten Outsourcing-Dienstleisters</p> <p>M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleisters</p> <p>M 2.254 Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben</p> <p>M 2.255 Sichere Migration bei Outsourcing-Vorhaben</p> <p>M 2.256 Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb</p>
A.12.6.1	<p>M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems</p> <p>M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates</p>
A.14.1.1	<p>B 1.3 Notfallmanagement</p> <p>BSI-Standard 100-2, Kapitel 3 Initiierung des Sicherheitsprozesses</p> <p>BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz</p> <p>BSI-Standard 100-4 Notfallmanagement</p> <p>B 1.8 Behandlung von Sicherheitsvorfällen</p>
A.14.1.2	<p>B 1.3 Notfallmanagement</p> <p>BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz</p> <p>BSI-Standard 100-4 Notfallmanagement</p> <p>B 1.8 Behandlung von Sicherheitsvorfällen</p>
A.14.1.3	<p>B 1.3 Notfallmanagement</p> <p>BSI-Standard 100-4 Notfallmanagement</p> <p>B 1.8 Behandlung von Sicherheitsvorfällen</p>
A.14.1.4	<p>B 1.3 Notfallmanagement</p> <p>BSI-Standard 100-4 Notfallmanagement</p> <p>B 1.8 Behandlung von Sicherheitsvorfällen</p>
A.14.1.5	<p>B 1.3 Notfallmanagement</p> <p>BSI-Standard 100-4 Notfallmanagement</p> <p>B 1.8 Behandlung von Sicherheitsvorfällen</p>
A.15.1.3	<p>M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen</p>

12.2. Anhang 2

Beispiel einer Clause und der zugeordneten Massnahmen im Detail (Ziff. 5.)

8.1.1	Roles and responsibilities
-------	----------------------------

Deutscher Text aus ISO/IEC 27001:

Aufgaben und Verantwortlichkeiten

Massnahme:

Sicherheitsaufgaben und -Verantwortlichkeiten von Angestellten, Auftragnehmern und Drittbenutzern müssen im Einklang mit den Informationssicherheitsgrundsätzen der Organisation definiert und dokumentiert werden.

Zugewiesene Bausteine und Massnahmen gemäss BSI-Tabelle:

A.8.1.1	<p>M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit M 3.1 Geregelte Einarbeitung/Einweisung neuer Mitarbeiter M 3.26 Einweisung des Personals in den sicheren Umgang mit IT</p> <p>M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz M 2.5 Aufgabenverteilung und Funktionstrennung M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit</p> <p>B 1.1 Organisation B 1.2 Personal</p>
---------	---

M2.198, M3.1 und M3.26 definieren und schulen die Aufgaben der Benützenten für IKT-Sicherheit.

M2.1, M2.5 und M.193 betreffen die Definition und Dokumentation der Verantwortlichkeiten für IKT-Sicherheit.

B1.1 und B1.2 sind die organisatorischen Hauptbausteine zur weiteren Umsetzung der Massnahme. Sie enthalten weitere Massnahmen zur Vervollständigung der Zielsetzung.