Die folgende Tabelle zeigt die strukturellen Verschiebungen von Version 3.1.5 nach Version 4 des Sicherheithandbuchs.

Sicherheitshandbuch (Version 3.1.5)		***Sicherheitshandbuch (Version 4)***
Kapitel	*Überschrift*	*Kapitel*
1	**Einführung**	**1**
1.1	Das Informationssicherheitshandbuch	1.1
1.1.1	Ziele des Informationssicherheitshandbuchs	1.1.1
1.1.1.1	Ziele der Version 3	1.1.1.1
1.1.2	Anwendungsbereich (Scope)	1.1.2
1.1.3	Neuheiten der Version 3	1.1.3
1.1.4	Quellen, Verträglichkeiten, Abgrenzungen	1.1.4
1.1.5	Informations- versus IT-Sicherheit	1.1.5
1.2	Informationssicherheitsmanagement	1.2
1.2.1	Ziele des Informationssicherheitsmanagements	1.2.1
1.2.2	Aufgaben des Informationssicherheitsmanagements	1.2.2
2	**Informationssicherheitsmanagementsystem (ISMS)**	**2**
2.1	Der Informationssicherheitsmanagementprozess	2.1
2.1.1	Entwicklung einer organisationsweiten Informationssicherheitspolitik	2.1.1
2.1.2	Risikoanalyse	2.1.2
2.1.3	Erstellung eines Sicherheitskonzeptes	2.1.3
2.1.4	Umsetzung des Informationssicherheitsplans	2.1.4
2.1.5	Informationssicherheit im laufenden Betrieb	2.1.5
2.2	Erstellung von Sicherheitskonzepten	2.2
2.2.1	Auswahl von Maßnahmen	2.2.1
2.2.1.1	Klassifikation von Sicherheitsmaßnahmen	2.2.1.1
2.2.1.2	Ausgangsbasis für die Auswahl von Maßnahmen	2.2.1.2
2.2.1.3	Auswahl von Maßnahmen auf Basis einer detaillierten Risikoanalyse	2.2.1.3
2.2.1.4	Auswahl von Maßnahmen im Falle eines Grundschutzansatzes	2.2.1.4
2.2.1.5	Auswahl von Maßnahmen im Falle eines kombinierten Risikoanalyseansatzes	2.2.1.5
2.2.1.6	Bewertung von Maßnahmen	2.2.1.6
2.2.1.7	Rahmenbedingungen	2.2.1.7
2.2.2	Risikoakzeptanz	2.2.2
2.2.3	Sicherheitsrichtlinien	2.2.3
2.2.3.1	Aufgaben und Ziele	2.2.3.1
2.2.3.2	Inhalte	2.2.3.2
2.2.3.3	Fortschreibung der Sicherheitsrichtlinien	2.2.3.3
2.2.3.4	Verantwortlichkeiten	2.2.3.4
2.2.4	Informationssicherheitspläne für jedes System	2.2.4
2.2.5	Fortschreibung des Sicherheitskonzeptes	2.2.5
2.3	Umsetzung des Informationssicherheitsplans	2.3
2.3.1	Implementierung von Maßnahmen	2.3.1
2.3.2	Sensibilisierung (Security Awareness)	2.3.2
2.3.3	Schulung	2.3.3
2.3.4	Akkreditierung	2.3.4
2.4	Informationssicherheit im laufenden Betrieb	2.4
2.4.1	Aufrechterhaltung des erreichten Sicherheitsniveaus	2.4.1
2.4.2	Wartung und administrativer Support von Sicherheitseinrichtungen	2.4.2
2.4.3	Überprüfung von Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking)	2.4.3
2.4.4	Fortlaufende Überwachung der IT-Systeme (Monitoring)	2.4.4
3	**Managementverantwortung und Aufgaben beim ISMS**	**3**
3.1	Verantwortung der Managementebene	3.1
3.1.1	Generelle Managementaufgaben beim ISMS	3.1.1
3.2	Ressourcenmanagement	3.2
3.2.1	Bereitstellung von Ressourcen	3.2.1
3.2.2	Schulung und Awareness	3.2.2
3.3	Interne ISMS Audits	3.3

3.3.1	Planung und Vorbereitung interner Audits	3.3.1
3.3.2	Durchführung interner Audits	3.3.2
3.3.3	Ergebnis und Auswertung interner Audits	3.3.3
3.4	Management-Review des ISMS	3.4
3.4.1	Management-Review Methoden	3.4.1
3.4.1.1	Review der Strategie und des Sicherheitskonzepts	3.4.1.1
3.4.1.2	Review der Sicherheitsmaßnahmen	3.4.1.2
3.4.2	Management-Review-Ergebnis und -Auswertung	3.4.2
3.5	Verbesserungsprozess beim ISMS	3.5
3.5.1	Grundlagen für Verbesserungen	3.5.1
3.5.2	Entscheidungs- und Handlungsbedarf	3.5.2
4	**Risikoanalyse**	**4**
4.1	Risikoanalysestrategien	4.1
4.2	Detaillierte Risikoanalyse	4.2
4.2.1	Abgrenzung des Analysebereiches	4.2.1
4.2.2	Identifikation der bedrohten Objekte (Werte, assets)	4.2.2
4.2.3	Wertanalyse (Impact Analyse)	4.2.3
4.2.3.1	Festlegung der Bewertungsbasis für Sachwerte	4.2.3.1
4.2.3.2	Festlegung der Bewertungsbasis für immaterielle Werte	4.2.3.2
4.2.3.3	Ermittlung der Abhängigkeiten zwischen den Objekten	4.2.3.3
4.2.3.4	Bewertung der bedrohten Objekte	4.2.3.4
4.2.4	Bedrohungsanalyse	4.2.4
4.2.4.1	Identifikation möglicher Bedrohungen	4.2.4.1
4.2.4.2	Bewertung möglicher Bedrohungen	4.2.4.2
4.2.5	Schwachstellenanalyse	4.2.5
4.2.6	Identifikation bestehender Sicherheitsmaßnahmen	4.2.6
4.2.7	Risikobewertung	4.2.7
4.2.8	Auswertung und Aufbereitung der Ergebnisse	4.2.8
4.3	Grundschutzansatz	4.3
4.3.1	Die Idee des IT-Grundschutzes	4.3.1
4.3.2	Grundschutzanalyse und Auswahl von Maßnahmen	4.3.2
4.3.2.1	Modellierung	4.3.2.1
4.3.2.2	Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen	4.3.2.2
4.3.3	Vorgehen bei Abweichungen	4.3.3
4.3.4	Dokumentation der Ergebnisse	4.3.4
4.4	Kombinierter Ansatz	4.4
4.4.1	Festlegung von Schutzbedarfskategorien	4.4.1
4.4.2	Schutzbedarfsfeststellung	4.4.2
4.4.2.1	Erfassung aller vorhandenen oder geplanten IT-Systeme	4.4.2.1
4.4.2.2	Erfassung der IT-Anwendungen und Zuordnung zu den einzelnen IT-Systemen	4.4.2.2
4.4.2.3	Schutzbedarfsfeststellung für jedes IT-System	4.4.2.3
4.4.3	Durchführung von Grundschutzanalysen und detaillierten Risikoanalysen	4.4.3
4.5	Akzeptables Restrisiko	4.5
4.6	Akzeptanz von außergewöhnlichen Restrisiken	4.6
5	**Informationssicherheitspolitik**	**5**
5.1	Aufgaben und Ziele einer Informationssicherheitspolitik	5.1
5.2	Inhalte der Informationssicherheitspolitik	5.2
5.2.1	Informationssicherheitsziele und -strategien	5.2.1
5.2.2	Management Commitment	5.2.2
5.2.3	Organisation und Verantwortlichkeiten für Informationssicherheit	6.1.3
5.2.3.1	Die/Der IT-Sicherheitsbeauftragte	6.1.3.1
5.2.3.2	Das Informationssicherheitsmanagement-Team	6.1.3.2
5.2.3.3	Die Bereichs-IT-Sicherheitsbeauftragten	6.1.3.3
5.2.3.4	Applikations-/Projektverantwortliche	6.1.3.4
5.2.3.5	Die/Der Informationssicherheitsbeauftragte	6.1.3.5
5.2.3.6	Weitere Pflichten und Verantwortungen im Bereich Informationssicherheit	6.1.3.6
5.2.3.7	Informationssicherheit und Datenschutz	6.1.3.7
5.2.4	Risikoanalysestrategien, akzeptables Restrisiko und Akzeptanz von außergewöhnlichen Restrisiken	5.2.3
5.2.5	Klassifizierung von Informationen	8.2
5.2.5.1	Definition der Sicherheitsklassen	8.2.1
5.2.5.2	Festlegung der Verantwortlichkeiten und der Vorgehensweise für klassifizierte Informationen	8.2.2

5.2.5.3	Erarbeitung von Regelungen zum Umgang mit klassifizierten Informationen	8.2.3
5.2.6	Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity Planung	8.2.4
5.2.7	Überprüfung und Aufrechterhaltung der Sicherheit	5.1.1
5.2.8	Dokumente zur Informationssicherheit	5.2.4
5.3	Lifecycle der Informationssicherheitspolitik	5.3
5.3.1	Erstellung der Informationssicherheitspolitik	5.3.1
5.3.2	Offizielle Inkraftsetzung der Informationssicherheitspolitik	5.3.2
5.3.3	Regelmäßige Überarbeitung	5.3.3
6	**Organisation**	**6**
6.1	Interne Organisation	6.1
6.1.1	Managementverantwortung	6.1.1
6.1.1.1	Zusammenwirken verantwortliches Management - MitarbeiterInnen - Gremien	6.1.1.1
6.1.2	Koordination	6.1.2
6.1.3	Definierte Verantwortlichkeiten für Informationssicherheit	6.1.4
6.1.4	Benutzungsgenehmigung für Informationsverarbeitung	6.1.5
6.1.5	Vertraulichkeitsvereinbarungen	13.2.2
6.1.6	Kontaktpflege mit Behörden und Gremien	6.1.6
6.1.7	Unabhängige Audits der Sicherheitsmaßnahmen	18.1.1
6.1.8	Berichtswesen	18.1.2
6.2	Zusammenarbeit mit Externen	6.2
6.2.1	Outsourcing	6.2.1
6.2.2	Gefährdungen beim Outsourcing	6.2.2
6.2.3	Outsourcing-Planungs- und -Betriebsphasen	6.2.3
7	**Vermögenswerte und Klassifizierung von Informationen**	**8**
7.1	Vermögenswerte	8.1
7.1.1	Inventar der Vermögenswerte (Assets) mittels Strukturanalyse	8.1.1
7.1.1.1	Erfassung von Geschäftsprozessen, Anwendungen und Informationen	81.1.1
7.1.1.2	Erfassung von Datenträgern und Dokumenten	81.1.2
7.1.1.3	Erhebung der IT-Systeme	81.1.3
7.1.1.4	Netzplan	81.1.4
7.1.1.5	Erfassung der Gebäude und Räume	81.1.5
7.1.1.6	Aktualisierung der Strukturanalyse	81.1.6
7.1.2	Eigentum von Vermögenswerten	8.1.2
7.1.2.1	Verantwortliche für Vermögenswerte (Assets)	8.1.2.1
7.1.2.2	Aufgaben der Eigentümer und Verantwortlichen	8.1.2.2
7.1.3	Zulässige Nutzung von Vermögenswerten	8.1.3
7.1.3.1	Herausgabe einer PC-Richtlinie	8.1.3.1
7.1.3.2	Einführung eines PC-Checkheftes	8.1.3.2
7.1.3.3	Geeignete Aufbewahrung tragbarer IT-Systeme	8.1.3.3
7.1.3.4	Mitnahme von Datenträgern und IT-Komponenten	8.1.3.4
7.1.3.5	Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Videokameras	8.1.3.5
7.1.3.6	Absicherung von Wechselmedien	8.1.3.6
7.2	Klassifizierung von Informationen	8.2
8	**Personelle Sicherheit**	**7**
8.1	Regelungen für MitarbeiterInnen	7.1
8.1.1	Verpflichtung der MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen	7.1.1
8.1.2	Aufnahme der sicherheitsrelevanten Aufgaben und Verantwortlichkeiten in die Stellenbeschreibung	7.1.2
8.1.3	*Vertretungsregelungen*	7.1.3
8.1.4	Geregelte Verfahrensweise beim Ausscheiden von MitarbeiterInnen	7.1.4
8.1.5	Geregelte Verfahrensweise bei Versetzung von MitarbeiterInnen	7.1.5
8.1.6	Gewährleistung eines positiven Betriebsklimas	7.1.6
8.1.7	Clear-Desk-Policy	7.1.7
8.1.8	*Benennung vertrauenswürdiger AdministratorInnen und VertreterInnen*	7.1.8
8.1.9	Verpflichtung der PC-BenutzerInnen zum Abmelden	7.1.9
8.1.10	Kontrolle der Einhaltung der organisatorischen Vorgaben	7.1.10

8.1.11	Geregelte Verfahrensweise bei vermuteten Sicherheitsverletzungen	7.1.11
8.2	Regelungen für den Einsatz von Fremdpersonal	7.2
8.2.1	Regelungen für den kurzfristigen Einsatz von Fremdpersonal	7.2.1
8.2.2	Verpflichtung externer MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen	7.2.2
8.2.3	Beaufsichtigung oder Begleitung von Fremdpersonen	7.2.3
8.2.4	Information externer MitarbeiterInnen über die IT-Sicherheitspolitik	7.2.4
8.3	Sicherheitssensibilisierung und -schulung	7.3
8.3.1	Geregelte Einarbeitung/Einweisung neuer MitarbeiterInnen	7.3.1
8.3.2	Schulung vor Programmnutzung	7.3.2
8.3.3	Schulung und Sensibilisierung zu IT-Sicherheitsmaßnahmen	7.3.3
8.3.4	Betreuung und Beratung von IT-BenutzerInnen	7.3.4
8.3.5	Aktionen bei Auftreten von Sicherheitsproblemen (Incident Handling-Pläne)	7.3.5
8.3.6	Schulung des Wartungs- und Administrationspersonals	7.3.6
8.3.7	Einweisung in die Regelungen der Handhabung von Kommunikationsmedien	7.3.7
8.3.8	Einweisung in die Bedienung von Schutzschränken	7.3.8
9	**Physische und umgebungsbezogene Sicherheit**	**11**
9.1	Bauliche und infrastrukturelle Maßnahmen	11.1
9.1.1	Geeignete Standortauswahl	11.1.1
9.1.2	Anordnung schützenswerter Gebäudeteile	11.1.2
9.1.3	Einbruchsschutz	11.1.3
9.1.4	Zutrittskontrolle	11.1.4
9.1.5	Verwaltung von Zutrittskontrollmedien	11.1.5
9.1.6	Portierdienst	11.1.6
9.1.7	Einrichtung einer Postübernahmestelle	11.1.7
9.1.8	Perimeterschutz	11.1.8
9.2	Brandschutz	11.2
9.2.1	Einhaltung von Brandschutzvorschriften und Auflagen	11.2.1
9.2.2	Raumbelegung unter Berücksichtigung von Brandlasten	11.2.2
9.2.3	Organisation Brandschutz	11.2.3
9.2.4	Brandabschottung von Trassen	11.2.4
9.2.5	Verwendung von Brandschutztüren und Sicherheitstüren	11.2.5
9.2.6	Brandmeldeanlagen	11.2.6
9.2.7	Brandmelder	11.2.7
9.2.8	Handfeuerlöscher (Mittel der Ersten und Erweiterten Löschhilfe)	11.2.8
9.2.9	Löschanlagen	11.2.9
9.2.10	Brandschutzbegehungen	11.2.10
9.2.11	Rauchverbot	11.2.11
9.2.12	Rauchschutzvorkehrungen	11.2.12
9.3	Stromversorgung, Maßnahmen gegen elektrische und elektromagnetische Risiken	11.3
9.3.1	Angepasste Aufteilung der Stromkreise	11.3.1
9.3.2	Not-Aus-Schalter	11.3.2
9.3.3	Zentrale Notstromversorgung	11.3.3
9.3.4	Lokale unterbrechungsfreie Stromversorgung	11.3.4
9.3.5	Blitzschutzeinrichtungen (Äußerer Blitzschutz)	11.3.5
9.3.6	Überspannungsschutz (Innerer Blitzschutz)	11.3.6
9.3.7	Schutz gegen elektromagnetische Einstrahlung	11.3.7
9.3.8	Schutz gegen kompromittierende Abstrahlung	11.3.8
9.3.9	Schutz gegen elektrostatische Aufladung	11.3.9
9.4	Leitungsführung	11.4
9.4.1	Lagepläne der Versorgungsleitungen	11.4.1
9.4.2	Materielle Sicherung von Leitungen und Verteilern	11.4.2
9.4.3	Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen	11.4.3
9.4.4	Auswahl geeigneter Kabeltypen	11.4.4
9.4.5	Schadensmindernde Kabelführung	11.4.5
9.4.6	Vermeidung von wasserführenden Leitungen	11.4.6
9.5	Geeignete Aufstellung und Aufbewahrung	11.5
9.5.1	Geeignete Aufstellung eines Arbeitsplatz-IT-Systems	11.5.1
9.5.2	Geeignete Aufstellung eines Servers	11.5.2
9.5.3	Geeignete Aufstellung von Netzwerkkomponenten	11.5.3
9.5.4	Nutzung und Aufbewahrung mobiler IT-Geräte	11.5.4
9.5.5	Sichere Aufbewahrung der Datenträger vor und nach Versand	11.5.5

9.5.6	Serverräume	11.5.6
9.5.7	Beschaffung und Einsatz geeigneter Schutzschränke	11.5.7
9.6	Weitere Schutzmaßnahmen	11.6
9.6.1	Einhaltung einschlägiger Normen und Vorschriften	11.6.1
9.6.2	Regelungen für Zutritt zu Verteilern	11.6.2
9.6.3	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile	11.6.3
9.6.4	Geschlossene Fenster und Türen	11.6.4
9.6.5	Alarmanlage	11.6.5
9.6.6	Fernanzeige von Störungen	11.6.6
9.6.7	Klimatisierung	11.6.7
9.6.8	Selbsttätige Entwässerung	11.6.8
9.6.9	Videounterstützte Überwachung	11.6.9
9.6.10	Aktualität von Plänen	11.6.10
9.6.11	Vorgaben für ein Rechenzentrum	11.6.11
10	**Sicherheitsmanagement in Kommunikation und Betrieb**	**12**
10.1	IT-Sicherheitsmanagement	12.1
10.1.1	Etablierung eines IT-Sicherheitsmanagementprozesses	12.1.1
10.1.2	Erarbeitung einer organisationsweiten Informationssicherheitspolitik	12.1.2
10.1.3	Erarbeitung von IT-Systemsicherheitspolitiken	12.1.3
10.1.4	Festlegung von Verantwortlichkeiten	12.1.4
10.1.5	Funktionstrennung	12.1.5
10.1.6	Einrichtung von Standardarbeitsplätzen	12.1.6
10.1.7	Akkreditierung von IT-Systemen	12.1.7
10.1.8	Change Management	12.1.8
10.1.8.1	Reaktion auf Änderungen am IT-System	12.8.1
10.1.8.2	Softwareänderungskontrolle	12.8.2
10.2	Dokumentation	12.2
10.2.1	Dokumentation von Software	12.2.1
10.2.2	Sourcecodehinterlegung	12.2.2
10.2.3	Dokumentation der Systemkonfiguration	12.2.3
10.2.4	Dokumentation der Datensicherung	12.2.4
10.2.5	Dokumentation und Kennzeichnung der Verkabelung	12.2.5
10.2.6	Neutrale Dokumentation in den Verteilern	12.2.6
10.3	Dienstleistungen durch Dritte (Outsourcing)	15.1
10.3.1	Festlegung einer Outsourcing-Strategie	15.1.1
10.3.2	Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben	15.1.2
10.3.3	Wahl eines geeigneten Outsourcing-Dienstleisters	15.1.3
10.3.4	Vertragsgestaltung mit dem Outsourcing-Dienstleister	15.1.4
10.3.5	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben	15.1.5
10.3.6	Notfallvorsorge beim Outsourcing	15.1.6
10.4	Schutz vor Schadprogrammen und Schadfunktionen	12.3
10.4.1	Erstellung eines Virenschutzkonzepts	12.3.1
10.4.2	Generelle Maßnahmen zur Vorbeugung gegen Virenbefall	12.3.2
10.4.3	Empfohlene Virenschutzmaßnahmen auf Firewall-Ebene	12.3.3
10.4.4	Empfohlene Virenschutzmaßnahmen auf Server-Ebene	12.3.4
10.4.5	Empfohlene Virenschutzmaßnahmen auf Client-Ebene und Einzelplatzrechnern	12.3.5
10.4.6	Vermeidung bzw. Erkennung von Viren durch die BenutzerInnen	12.3.6
10.4.7	Erstellung von Notfallplänen im Fall von Vireninfektionen	12.3.7
10.4.8	Auswahl und Einsatz von Virenschutzprogrammen	12.3.8
10.4.9	Verhaltensregeln bei Auftreten eines Virus	12.3.9
10.4.10	Warnsystem für Computerviren – Aktualisierung von Virenschutzprogrammen	12.3.10
10.4.11	Schutz vor aktiven Inhalten	12.3.11
10.4.12	Sicherer Aufruf ausführbarer Dateien	12.3.12
10.4.13	Vermeidung gefährlicher Dateiformate	12.3.13
10.5	Datensicherung	12.4
10.5.1	Regelmäßige Datensicherung	12.4.1
10.5.2	Entwicklung eines Datensicherungskonzeptes	12.4.2
10.5.3	Festlegung des Minimaldatensicherungskonzeptes	12.4.3
10.5.4	Datensicherung bei Einsatz kryptographischer Verfahren	12.4.4
10.5.5	Geeignete Aufbewahrung der Backup-Datenträger	12.4.5
10.5.6	Sicherungskopie der eingesetzten Software	12.4.6
10.5.7	Beschaffung eines geeigneten Datensicherungssystems	12.4.7
10.5.8	Datensicherung bei mobiler Nutzung eines IT-Systems	12.4.8
10.5.9	Verpflichtung der MitarbeiterInnen zur Datensicherung	12.4.9
10.6	Netzsicherheit	13.1
10.6.1	Sicherstellung einer konsistenten Systemverwaltung	13.1.1

10.6.2	Ist-Aufnahme der aktuellen Netzsituation	13.1.2
10.6.3	Analyse der aktuellen Netzsituation	13.1.3
10.6.4	Entwicklung eines Netzkonzeptes	13.1.4
10.6.5	Entwicklung eines Netzmanagementkonzeptes	13.1.5
10.6.6	Sicherer Betrieb eines Netzmanagementsystems	13.1.6
10.6.7	Sichere Konfiguration der aktiven Netzkomponenten	13.1.7
10.6.8	Festlegung einer Sicherheitsstrategie für ein Client-Server-Netz	13.1.8
10.6.9	Wireless LAN (WLAN)	13.1.9
10.6.10	Remote Access (VPN) - Konzeption	13.1.10
10.6.10.1	Durchführung einer VPN-Anforderungsanalyse	13.1.10.1
10.6.10.2	Entwicklung eines VPN-Konzeptes	13.1.10.2
10.6.10.3	Auswahl einer geeigneten VPN-Systemarchitektur	13.1.10.3
10.6.11	Remote Access (VPN) - Implementierung	13.1.11
10.6.11.1	Sichere Installation des VPN-Systems	13.1.11.1
10.6.11.2	Sichere Konfiguration des VPN-Systems	13.1.11.2
10.6.12	Sicherer Betrieb des VPN-Systems	13.1.12
10.6.13	Entwicklung eines Firewallkonzeptes	13.1.13
10.6.14	Installation einer Firewall	13.1.14
10.6.15	Sicherer Betrieb einer Firewall	13.1.15
10.6.16	Firewalls und aktive Inhalte	13.1.16
10.6.17	Firewalls und Verschlüsselung	13.1.17
10.6.18	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation	13.1.18
10.7	Betriebsmittel und Datenträger	8.3
10.7.1	Betriebsmittelverwaltung	8.3.1
10.7.2	Datenträgerverwaltung	8.3.2
10.7.3	Datenträgeraustausch	8.3.3
10.8	Informationsaustausch/E-Mail	13.2
10.8.1	Richtlinien beim Datenaustausch mit Dritten	13.2.1
10.8.2	Festlegung einer Sicherheitspolitik für E-Mail-Nutzung	13.2.3
10.8.3	Regelung für den Einsatz von E-Mail und anderen Kommunikationsdiensten	13.2.4
10.8.4	Sicherer Betrieb eines E-Mail-Servers	13.2.5
10.8.5	Einrichtung eines Postmasters	13.2.6
10.8.6	Geeignete Auswahl eines E-Mail-Clients/-Servers	13.2.7
10.8.7	Sichere Konfiguration der E-Mail-Clients	13.2.8
10.8.8	Verwendung von „Webmail" externer Anbietern	13.2.9
10.9	Internet, Web, E-Commerce, E-Government	14.7
10.9.1	Richtlinien bei Verbindung mit Netzen Dritter (Extranet)	14.7.1
10.9.2	Erstellung einer Internetsicherheitspolitik	14.7.2
10.9.3	Festlegung einer WWW-Sicherheitsstrategie	14.7.3
10.9.4	Sicherer Betrieb eines Webservers	14.7.4
10.9.5	Sicherheit von Webbrowsern	14.7.5
10.9.6	Schutz der WWW-Dateien	14.7.6
10.9.7	Einsatz von Stand-alone-Systemen zur Nutzung des Internets	14.7.7
10.9.8	Sichere Nutzung von E-Commerce- bzw. E-Government-Applikationen	14.7.8
10.9.9	Portalverbundsystem in der öffentlichen Verwaltung	14.7.9
10.10	Protokollierung und Monitoring	12.5
10.10.1	Erstellung von Protokolldateien	12.5.1
10.10.2	Datenschutzrechtliche Aspekte bei der Erstellung von Protokolldateien	12.5.2
10.10.3	Kontrolle von Protokolldateien	12.5.3
10.10.4	Rechtliche Aspekte bei der Erstellung und Auswertung von Protokolldateien zur E-Mail- und Internetnutzung	12.5.4
10.10.5	Audit und Protokollierung der Aktivitäten im Netz	12.5.5
10.10.6	Intrusion Detection Systeme	12.5.6
10.10.7	Zeitsynchronisation	12.5.7

11	**Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung**	**9**
11.1	Zugriffskontrollpolitik	9.1
11.1.1	Grundsätzliche Festlegungen zur Rechteverwaltung	9.1.1
11.2	Benutzerverwaltung	9.2
11.2.1	Vergabe und Verwaltung von Zugriffsrechten	9.2.1
11.2.2	Einrichtung und Dokumentation der zugelassenen BenutzerInnen und Rechteprofile	9.2.2
11.2.3	Organisatorische Regelungen für Zugriffsmöglichkeiten in Vertretungs- bzw. Notfällen	9.2.3
11.3	Verantwortung der BenutzerInnen	9.3
11.3.1	Regelungen des Passwortgebrauches	9.3.1
11.3.2	Bildschirmsperre	9.3.2
11.4	Fernzugriff	9.4

11.4.1	Nutzung eines Authentisierungsservers beim Fernzugriff	9.4.1
11.4.2	Einsatz geeigneter Tunnelprotokolle für die VPN-Kommunikation	9.4.2
11.4.3	Einsatz von Modems und ISDN-Adaptern	9.4.3
11.4.4	Geeignete Modemkonfiguration	9.4.4
11.4.5	Aktivierung einer vorhandenen Callback-Option	9.4.5
11.5	Zugriff auf Betriebssysteme	9.5
11.5.1	Sichere Initialkonfiguration und Zertifikatsgrundeinstellung	9.5.1
11.5.2	Nutzung der BIOS-Sicherheitsmechanismen	9.5.2
11.6	Zugriff auf Anwendungen und Informationen	9.6
11.6.1	Wahl geeigneter Mittel zur Authentisierung	9.6.1
11.6.2	Regelungen des Gebrauchs von Chipkarten	9.6.2
11.6.3	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen	9.6.3
11.7	Mobile Computing und Telearbeit	6.3
11.7.1	Mobile IT-Geräte	6.3.1
11.7.1.1	Laptop, Notebook, Tablet-PC	6.3.1.1
11.7.1.2	PDA (Personal Digital Assistant)	6.3.1.2
11.7.1.3	Mobiltelefon, Smartphone	6.3.1.3
11.7.1.4	Wechselmedien und externe Datenspeicher (USB-Sticks, -Platten, CDs, DVDs)	6.3.1.4
11.7.2	Geeignete Einrichtung eines häuslichen Arbeitsplatzes	6.3.2
11.7.3	Regelungen für Telearbeit	6.3.3
11.7.4	Regelung des Dokumenten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution	6.3.4
11.7.5	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger	6.3.6
11.7.6	Betreuungs- und Wartungskonzept für Telearbeitsplätze	6.3.6
11.7.7	Geregelte Nutzung der Kommunikationsmöglichkeiten	6.3.7
11.7.8	Regelung der Zugriffsmöglichkeiten von TelearbeiterInnen	6.3.8
11.7.9	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution	6.3.9
11.7.10	Sicherheitstechnische Anforderungen an den Kommunikationsrechner	6.3.10
11.7.11	Informationsfluss, Meldewege und Fortbildung	6.3.11
11.7.12	Vertretungsregelung für Telearbeit	6.3.12
11.7.13	Entsorgung von Datenträgern und Dokumenten	6.3.13
12	**Sicherheit in Entwicklung, Betrieb und Wartung eines IT-Systems**	**14**
12.1	Sicherheit im gesamten Lebenszyklus eines IT-Systems	14.1
12.1.1	IT-Sicherheit in der Systemanforderungsanalyse	14.1.1
12.1.2	Durchführung einer Risikoanalyse und Festlegung der ITSicherheitsanforderungen	14.1.2
12.1.3	IT-Sicherheit in Design und Implementierung	14.1.3
12.1.4	Entwicklungsumgebung	14.1.4
12.1.5	Entwicklung eines Testplans für Standardsoftware	14.1.5
12.1.6	Testen von Software	14.1.6
12.1.7	Abnahme und Freigabe von Software	14.1.7
12.1.8	Installation und Konfiguration von Software	14.1.8
12.1.9	Sicherstellen der Integrität von Software	14.1.9
12.1.10	Lizenzverwaltung und Versionskontrolle von Standardsoftware	14.1.10
12.1.11	Deinstallation von Software	14.1.11
12.2	Evaluierung und Zertifizierung	14.2
12.2.1	Beachtung des Beitrags der Zertifizierung für die Beschaffung	14.2.1
12.3	Einsatz von Software	14.3
12.3.1	Nutzungsverbot nicht freigegebener Software	14.3.1
12.3.2	Nutzungsverbot privater Hard- und Softwarekomponenten	14.3.2
12.3.3	Überprüfung des Softwarebestandes	14.3.3
12.3.4	Update von Software	14.3.4
12.3.5	Update/Upgrade von Soft- und Hardware im Netzbereich	14.3.5
12.3.6	Softwarepflege- und -änderungskonzept	14.3.6
12.4	Korrekte Verarbeitung	14.4
12.4.1	Verifizieren der zu übertragenden Daten vor Weitergabe	14.4.1
12.5	Sicherheit von Systemdateien	14.5
12.5.1	Systemdateien	14.5.1
12.5.2	Sorgfältige Durchführung von Konfigurationsänderungen	14.5.2
12.6	Einsatz kryptographischer Maßnahmen	10.1
12.6.1	Entwicklung eines Kryptokonzepts	10.1.1
12.6.2	Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte	10.1.2

12.6.3	Auswahl eines geeigneten kryptographischen Verfahrens	10.1.3
12.6.4	Auswahl eines geeigneten kryptographischen Produktes	10.1.4
12.6.5	Regelung des Einsatzes von Kryptomodulen	10.1.5
12.6.6	Physikalische Sicherheit von Kryptomodulen	10.1.6
12.6.7	Schlüsselmanagement	10.1.7
12.6.8	Einsatz elektronischer Signaturen	10.1.8
12.6.9	Zertifizierungsdienste	10.1.9
12.7	Wartung	14.6
12.7.1	Regelungen für Wartungsarbeiten im Haus	14.6.1
12.7.2	Regelungen für externe Wartungsarbeiten	14.6.2
12.7.3	Fernwartung	14.6.3
12.7.4	Wartung und administrativer Support von Sicherheitseinrichtungen	14.6.4
13	**Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)**	**16**
13.1	Reaktion auf Sicherheitsvorfälle bzw. sicherheitsrelevante Ereignisse (Incident Handling)	16.1
13.1.1	Überlegungen zu Informationssicherheitsereignissen	16.1.1
13.1.2	Festlegung von Verantwortlichkeiten bei Informationssicherheitsereignissen	16.1.2
13.1.3	Erstellung eines Incident Handling-Plans und Richtlinien zur Behandlung von Sicherheitsvorfällen	16.1.3
13.1.4	Prioritäten bei der Behandlung von Sicherheitsvorfällen	16.1.4
13.1.5	Meldewege bei Sicherheitsvorfällen	16.1.5
13.1.6	Behebung von Sicherheitsvorfällen	16.1.6
13.1.7	Eskalation von Sicherheitsvorfällen	16.1.7
13.1.8	Nachbereitung von Sicherheitsvorfällen (Lessons Learned)	16.1.8
13.1.9	Computer Emergency Response Team (CERT)	16.1.9

14	**Disaster Recovery und Business Continuity**	**17**
14.1	Informationssicherheits-Aspekte des betrieblichen Kontinuitätsmanagements	17.1
14.1.1	Definition von Verfügbarkeitsklassen	17.1.1
14.1.2	Erstellung einer Übersicht über Verfügbarkeitsanforderungen	17.1.2
14.1.3	Benennung einer/eines Notfallverantwortlichen	17.1.3
14.1.4	Erstellung eines Disaster Recovery-Handbuches	17.1.4
14.1.5	Definition des eingeschränkten IT-Betriebs (Notlaufplan)	17.1.5
14.1.6	Regelung der Verantwortung im Notfall	17.1.6
14.1.7	Untersuchung interner und externer Ausweichmöglichkeiten	17.1.7
14.1.8	Alarmierungsplan	17.1.8
14.1.9	Erstellung eines Wiederanlaufplans	17.1.9
14.1.10	Ersatzbeschaffungsplan	17.1.10
14.1.11	Lieferantenvereinbarungen	17.1.11
14.1.12	Abschließen von Versicherungen	17.1.12
14.1.13	Redundante Leitungsführung	17.1.13
14.1.14	Redundante Auslegung der Netzkomponenten	17.1.14
14.2	Umsetzung und Test	17.2
14.2.1	Durchführung von Disaster Recovery-Übungen	17.2.1
14.2.2	Übungen zur Datenrekonstruktion	17.2.2
15	**Security Compliance**	**18**
15.1	Security Compliance Checking und Monitoring	18.1
15.1.1	Einhaltung von rechtlichen und betrieblichen Vorgaben	18.1.3
15.1.2	Überprüfung auf Einhaltung der Sicherheitspolitiken	18.1.4
15.1.3	Auswertung von Protokolldateien	18.1.5
15.1.4	Kontrolle bestehender Verbindungen	18.1.6
15.1.5	Durchführung von Sicherheitskontrollen in Client-Server-Netzen	18.1.7
15.1.6	Kontrollgänge	18.1.8
15.1.7	Fortlaufende Überwachung der IT-Systeme (Monitoring)	18.1.9

A.1	**Sicherheitsszenarien**	**A.1**
A.1.1	Industrielle Sicherheit	A.1.1
A.1.1.1	Beschreibung der generellen Anforderungen	A.1.1.1
A.1.1.2	Rechtlicher Hintergrund	A.1.1.2

A.1.1.3	Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung	A.1.1.3
A.1.2	Österreichische Sicherheits- und Verteidigungsdoktrin – Teilstrategie IKTSicherheit	A.1.2
A.1.3	Sicherheitsfunktionen für E-Government in Österreich	A.1.3
A.1.3.1	Konzept und Funktionen der Bürgerkarte	A.1.3.1
A.1.3.2	Personenkennzeichen und Stammzahlen	A.1.3.2
A.1.3.3	Vollmachten	A.1.3.3
A.1.3.4	Module für Online-Applikationen (MOA)	A.1.3.4
A.1.3.4.1	MOA-ID (Identifikation)	A.1.3.4.1
A.1.3.4.2	MOA-SP (Signaturprüfung)/MOA-SS (Signaturerstellung am Server)	A.1.3.4.2
A.1.3.4.3	MOA-ZS (Zustellung)	A.1.3.4.3
A.1.3.4.4	MOA-AS (Amtssignatur)	A.1.3.4.4
A.1.3.5	Portalverbund	A.1.3.5

A.2	**Sicherheitstechnologien**	**A.2**
A.2.1	Kryptographische Methoden	10.2
A.2.1.1	Elemente der Kryptographie	10.2.1
A.2.1.2	Kryptographische Grundziele	abgedeckt durch 10.1
A.2.1.3	Verschlüsselung	10.2.2
A.2.1.4	Integritätsschutz	10.2.3
A.2.1.5	Authentizitätsnachweise	10.2.4
A.2.1.6	Digitale Signaturen, elektronische Signaturen	10.2.5
A.2.1.7	Schlüsselmanagement	in 10.1.7 integriert
A.2.1.8	Schlüsselverteilungszentralen	abgedeckt durch 10.1.7
A.2.2	Tunneling	A.2.1
A.2.2.1	Tunnelprotokolle für die VPN-Kommunikation	A.2.1.1
A.2.3	Virtualisierung	A.2.2
A.2.3.1	Einführung in die Virtualisierung	A.2.2.1
A.2.3.2	Anwendungen der Virtualisierungstechnik	A.2.2.2
A.2.3.3	Gefährdungen in Zusammenhang mit Virtualisierung	A.2.2.3
A.2.3.4	Planung	A.2.2.4
A.2.3.5	Rollen und Verantwortlichkeiten bei der Virtualisierung	A.2.2.5
A.2.3.6	Anpassung der Infrastruktur im Zuge der Virtualisierung	A.2.2.6
A.2.3.7	Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern	A.2.2.7
A.2.3.8	Sichere Konfiguration virtueller IT-Systeme	A.2.2.8
A.2.3.9	Sicherer Betrieb virtueller Infrastrukturen	A.2.2.9
A.2.3.10	Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten	A.2.2.10

A.3	**Cloud Computing**	**A.3**
A.3.1	Begriffsdefinition	A.3.1
A.3.1.1	Charakteristiken von Cloud Computing	A.3.1.1
A.3.1.2	Servicemodelle des Cloud Computings	A.3.1.2
A.3.1.3	Ausprägungen von Cloud Computing	A.3.1.3
A.3.2	Rechtliche Aspekte/Auswirkungen/Chancen/Risiken	A.3.2
A.3.2.1	Grundsätzliches	A.3.2.1
A.3.2.2	Datenschutzrecht	A.3.2.2
A.3.2.3	Vertragsrecht, Haftung und Gewährleistung	A.3.2.3
A.3.2.4	Vergaberecht	A.3.2.4
A.3.2.5	Strafprozessrecht	A.3.2.5
A.3.2.6	Sonderprobleme	A.3.2.6
A.3.3	Strukturelle Aspekte/Auswirkungen/Chancen/Risiken	A.3.3
A.3.3.1	Grundsätzliches	A.3.3.1
A.3.4	Wirtschaftliche Aspekte/Auswirkungen/Chancen/Risiken	A.3.4
A.3.4.1	Grundsätzliches	A.3.4.1
A.3.5	Technische Aspekte/Auswirkungen/Chancen/Risiken und Sicherheit	A.3.5
A.3.5.1	Technische Aspekte	A.3.5.1
A.3.5.2	Zusammenfassung der technischen Aspekte	A.3.5.2
A.3.5.3	Sicherheit und Technik	A.3.5.3
A.3.6	Prozesse (Geschäftsprozesse) - Aspekte / Auswirkungen / Chancen / Risiken / Integration	A.3.6
A.3.6.1	Grundsätzliches	A.3.6.1
A.3.6.2	Strategische Aspekte der Prozessveränderung durch Cloud Computing	A.3.6.2
A.3.6.3	Cloud Compliance	A.3.6.3
A.3.6.4	Entscheidungskriterien zur Auswahl von Cloud-affinen Anwendungen und Services	A.3.6.4
A.3.6.5	Mögliche Cloud Services	A.3.6.5