Mustervorlage für ein Sicherheitskonzept

KR Ing. Martin Prager
10. Oktober 2013, RTR Wien

Mustervorlage für ein Sicherheitskonzept

- **Zweck und Struktur**
  - Hintergrund und Entstehung
- **Mustervorlage Informationsicherheitsleitlinie**
  - Dokumentation der Sicherheitsziele und des Sicherheitsniveaus
- **Mustervorlage Sicherheitskonzept**
  - Konkrete Maßnahmen

Zweck und Struktur

- Gemäß unionsrechtlichen Vorschriften haben Betreiber öffentlicher Kommunikationsnetze und -dienste Maßnahmen zu ergreifen, um die Sicherheit und die Integrität der Netze und Dienste zu gewährleisten.
- Im Rahmen von Workshops der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) haben Vertreter von EU- bzw. EWR-Mitgliedstaaten und nationalen Regulierungsbehörden informell Mindestsicherheitsmaßnahmen vereinbart, die von allen Betreibern eingehalten werden sollen.

Zweck und Struktur

- Diese sind in dem von der ENISA veröffentlichten Dokument *Technical Guideline on Minimum Security Measures,* Version 1.0, veröffentlicht.

Leitlinie zur Informationssicherheit (Mustervorlage)

- Gemäß Vorgabe der ENISA sollte ein Betreiber eine geeignete High-Level-Leitlinie zur Informationssicherheit (IS) festlegen
- Der Begriff der IS-Leitlinie stammt aus ISO/IEC 27001 und 27002.
- Nach ISO/IEC 27002 besteht das Ziel der IS-Leitlinie darin, dem Management Anleitung und Unterstützung bezüglich Informationssicherheit entsprechend den Geschäftserfordernissen und relevanten Gesetzen und Regulierungen bereitzustellen.

Leitlinie zur Informationssicherheit (Mustervorlage)

- Die Mustervorlage der AG IT-Sicherheit lässt sich auch in kleineren Unternehmen einsetzen, muss jedoch geringfügig geändert und in einigen Abschnitten unternehmensspezifisch konkretisiert werden.
- Die IS-Leitlinie ist mit dem notwendigen Prozess zur Informationssicherheit eng verknüpft
- Die IS-Leitlinie ist eng verbunden mit der Etablierung eines Prozesses zur Gewährleistung der Informationssicherheit (Einrichtung eines IS-Managements).

Leitlinie zur Informationssicherheit (Mustervorlage)

- Mit der Mustervorlage werden Struktur und Inhalt (in Form von Erläuterungen) einer IS-Leitlinie in einheitlicher Weise empfohlen.

- Die Mustervorlage kann als Ausgangspunkt für die jeweilige Konkretisierung in einem Unternehmen dienen.

Rahmenbedingungen

- **Es gelten folgende Rahmenbedingungen:**
  - Erstellung durch IT-Sicherheitsbeauftragte (soweit schon vorhanden) oder durch IT-Management.
  - Die IS-Leitlinie bildet den Ausgangspunkt für die darauf aufbauende IT-Richtlinien-Struktur. Es ist daher auf eine allgemeine, kurze, prägnante, selten anzupassende Darstellung zu achten.

Rahmenbedingungen

- Bekanntgabe an alle Beschäftigten innerhalb des Geltungsbereichs und die IS-Aufgabenträger sowie nachfolgend an neue Beschäftigte und IS-Rollenträger (ggf. mit Bestätigung der Kenntnisnahme).

- Es ist darauf zu achten, dass externe Beschäftigte entsprechend verpflichtet werden.

Sicherheitsziele

- **Der Geltungsbereich der IS-Leitlinie umfasst alle Bereiche des Unternehmens, die in die Verwaltung und den Betrieb öffentlicher Kommunikationsnetze oder -dienste iSd TKG 2003 involviert sind**

Sicherheitsziele

- Festlegung der Informationssicherheitsleitlinie,
- Festlegung eines Rahmens für das Risikomanagement,
- Festlegung eines Rollenmodells für Sicherheitsaufgaben,
- Festlegung von Sicherheitsanforderungen für Leistungen Dritter,
- Durchführung von Hintergrundüberprüfungen,
- Vermittlung von Sicherheitskenntnissen und -training,
- Festlegung eines Prozesses zur Verwaltung personeller Wechsel,
- Festlegung eines Prozesses für disziplinäre Maßnahmen,
- Wahrung der physischen Sicherheit für Anlagen und Infrastruktur der Netze und Dienste sowie Schutz vor Elementarereignissen,
- Wahrung der Sicherheit von Betriebsstoffen und unterstützenden Anlagen,
- Kontrolle des Zugriffs auf Netzen und Informationssysteme,
- Wahrung der Informationssicherheit von Netzen und Informationssystemen zum Schutz vor Malware, Viren und üblichen Bedrohungen,
- Festlegung von Betriebsabläufen und Verantwortlichkeiten,

Sicherheitsziele

- **Festlegung eines Prozesses für das Veränderungsmanagement,**
- **Festlegung von Konfigurationskontrollen und Abläufen zur Verwaltung von IT-Einrichtungen,**
- **Festlegung standardisierter Abläufe für den Umgang mit Sicherheitsverletzungen und Integritätsverlusten,**
- **Herstellung der Fähigkeit zur Entdeckung von Sicherheitsverletzungen und Integritätsverlusten,**
- **Festlegung, Wartung und Einhaltung eines Kommunikationsplans für Sicherheitsverletzungen und Integritätsverluste,**
- **Festlegung einer Strategie zur Gewährleistung der Verfügbarkeit von Netzen und Diensten sowie Festlegung eines Notfallplans,**
- **Herstellung der Fähigkeit zum Disaster Recovery für die Wiederherstellung von Netzen und Diensten,**
- **Festlegung von Leitlinien für Systemüberwachung und Protokollierung,**

Sicherheitsziele

- **Festlegung von Leitlinien zum Testen und Üben von Notfallplänen,**
- **Festlegung von Leitlinien zum Testen von Netzen und Informationssystemen,**
- **Festlegung einer Leitlinie zur Durchführung von Sicherheitsbewertungen und Sicherheitstests,**
- **Festlegung einer Leitlinie zur Überwachung und Überprüfung der Befolgung von Vorschriften.**

Kernelemente der IS-Strategie

- **Hier werden Leitaussagen/strategische Vorgaben zu wesentlichen Maßnahmen zur Gewährleistung der IS aufgeführt. Dazu zählen z. B.**

  - Grundsätzliche technisch-organisatorische Sicherheitsmaßnahmen, wie
    - *Zutritts-, Zugangs- und Zugriffsschutz,*
    - *Umgang mit Vorfällen, die die Informationssicherheit beeinträchtigen,*
    - *Sichere Nutzung Internet, E-Mail, Virenschutz,*
    - *Notfallvorsorge*

Kernelemente der IS-Strategie

- Vorgabe zur Festlegung von Verantwortlichkeiten und Vertretungen;
- Vorgabe zur IT-/IS-Dokumentation;
- Hinweis auf Schulungs-/Sensibilisierungsmaßnahmen;
- Auftrag an Beschäftigte zur Beachtung und Umsetzung von IT-/IS-Regelungen;
- Aussagen zur Nutzungseinschränkung von IT bei unzureichender Sicherheit.

Verantwortlichkeiten und IS Organisation

- **Festlegung der Organisationsstruktur zur IS und Angabe von Ansprechpersonen, ggf. Bildung eines IT-Sicherheitsmanagementteams. Beschreibung von Aufgaben und Verantwortlichkeiten, z. B. der/des IT-Sicherheitsbeauftragten und deren/dessen Einbindung in IT-Maßnahmen. Hinweis auf atenschutzbeauftragten (vgl. § 17a DSG 2000) und Zusammenarbeit. Verantwortung der Leitungsebene z. B. bzgl.**
  - Bereitstellung ausreichender Ressourcen für IT-Sicherheit,
  - Unterstützung der bedarfsgerechten Fort- und Weiterbildung,
  - ständiger Verbesserung des Sicherheitsniveaus.

Erfolgskontrolle

- **Das angestrebte Sicherheits- und Datenschutzniveau wird sichergestellt, indem**
  - Sicherheitsregelungen in angemessener Zeit an neue Situationen angepasst und mindestens jährlich auf Aktualität überprüft werden;
  - Die Einhaltung von Sicherheitsregelungen laufend überwacht wird
- **Im Zuge der kontinuierlichen Revision von Sicherheitsregelungen werden Abweichungen mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand zu halten**
- **Die vorliegende Leitlinie zur Informationssicherheit wird mindestens alle zwei Jahre auf ihre Aktualität und Wirksamkeit hin überprüft und ggf. überarbeitet, wobei Änderungen von Rahmenbedingungen, Aufgaben und der Sicherheitsstrategie berücksichtigt werden**

Sicherheitskonzept (Mustervorlage)

- Betriebsführung und Risikomanagement
- Sicherheit personeller Ressourcen
- Sicherheit von Systemen und Einrichtungen
- Betriebsmanagement
- Incident-Management
- Betriebliches Kontinuitätsmanagement
- Monitoring, Auditing und Tests

Betriebsführung und Risikomanagement (Mustervorlage)

- **IS-Leitlinie**
  - Das vorliegende Sicherheitskonzept konkretisiert die von der Unternehmensleitung erlassene IS-Leitlinie
  - Gemäß Vorgabe durch die IS-Leitlinie wird diese allen Beschäftigten innerhalb des Geltungsbereichs und den IS-Aufgabenträgern sowie nachfolgend neuen Beschäftigten und IS-Rollenträgern bekanntgemacht
  - Die Beschäftigten haben die Kenntnisnahme zu bestätigen

Betriebsführung und Risikomanagement (Mustervorlage)

- **IS-Leitlinie**
  - Externe Dienstleister haben die Einhaltung der IS-Leitlinie im Rahmen einer Verpflichtungserklärung zu bestätigen
  - Bestätigungen und Verpflichtungserklärungen sind so abzulegen, dass sie bei Bedarf, insbesondere im Rahmen einer Sicherheitsüberprüfung, verfügbar sind

Betriebsführung und Risikomanagement (Mustervorlage)

- **Rahmenbedingungen des Risikomanagements**
  - Eine Liste der höchsten Risiken für die Sicherheit und die Integrität der Kommunikationsnetze und -dienste ist zu erstellen
  - Die Liste ist bei größeren technischen oder organisatorischen Änderungen, mindestens aber jährlich, zu prüfen und ggf. zu überarbeiten

Betriebsführung und Risikomanagement (Mustervorlage)

- **Rahmenbedingungen des Risikomanagements**

  - Die Liste der wesentlichen Risiken einschließlich der unter SM 2a genannten zusätzlichen Angaben für jedes Risiko ist nach Erstellung sowie nach jeder Änderung allen Entscheidungsträgern des Unternehmens bekanntzugeben

Betriebsführung und Risikomanagement (Mustervorlage)

- **Sicherheitsrollen und –verantwortlichkeiten**

  - Die Geschäftsführung ist verantwortlich für die Bereitstellung ausreichender Ressourcen für die IT-Sicherheit, für die Unterstützung der bedarfsgerechten Fort- und Weiterbildung und für die ständige Verbesserung des Sicherheitsniveaus. Folgende Sicherheitsrollen werden festgelegt:

Betriebsführung und Risikomanagement (Mustervorlage)

- **Sicherheitsrollen und –verantwortlichkeiten**
  - Sicherheitsexperte: Mindestens ein Sicherheitsexperte muss benannt werden. Dieser muss regelmäßig und direkt der Unternehmensführung berichten können.
  - [Datenschutzexperte: Es kann ein Datenschutzexperte benannt werden, der sich insbesondere mit Datensicherheitsmaßnahmen befasst.]

Betriebsführung und Risikomanagement (Mustervorlage)

- **Sicherheitsrollen und –verantwortlichkeiten**
  - Koordinatoren: Es sind Telekommunikationstechniker oder andere Beschäftigte zu benennen, die über erforderlichen Berechtigungen bzw. geeignete Kenntnisse und Fähigkeiten verfügen, um Angelegenheiten im Zusammenhang mit der Installation, der Wartung und dem Betrieb von Telekommunikationseinrichtungen für das Telekommunikationsgeschäft zu koordinieren.

Betriebsführung und Risikomanagement (Mustervorlage)

- **Sicherheitsrollen und –verantwortlichkeiten**
  - Ob eine Rolle durch eine oder mehrere Personen besetzt wird, obliegt dem Unternehmen

Betriebsführung und Risikomanagement (Mustervorlage)

- **Sicherheitsrollen und –verantwortlichkeiten**

  - Der Anbieter sollte eine geeignete Struktur der Sicherheitsrollen und -verantwortlichkeiten festlegen und regelmäßig aktualisieren
  - Für folgende Aufgaben sind Verantwortlichkeiten festzulegen:
    - Umsetzung und Befolgung der Informationssicherheitsleitlinie;

Betriebsführung und Risikomanagement (Mustervorlage)

- **Sicherheitsrollen und –verantwortlichkeiten**
  - Schutz von Betriebsmitteln vor unbefugtem Zugriff, Enthüllung, Veränderung, Zerstörung oder Beeinträchtigung;
  - Ausführung besonderer Sicherheitsprozesse oder -tätigkeiten;
  - Sicherstellung, dass Verantwortlichkeiten bestimmten Personen zugewiesen werden;
  - Information der Organisation über Sicherheitsereignisse oder potenzielle Ereignisse oder andere Sicherheitsrisiken.

Betriebsführung und Risikomanagement (Mustervorlage)

- **Sicherheitsrollen und –verantwortlichkeiten**
  - Jede Rolle wird mindestens einer Person durch die Unternehmensführung oder einen entsprechend bevollmächtigten Entscheidungsträger zugewiesen und gemeinsam mit den zugehörigen Verantwortlichkeiten in der Stellenbeschreibung dokumentiert
  - Die betroffenen Personen sind über die ihnen zugewiesenen Rollen und Verantwortlichkeiten in Kenntnis zu setzen

Betriebsführung und Risikomanagement (Mustervorlage)

- **Sicherheitsrollen und –verantwortlichkeiten**
  - Es ist eine Liste der Beschäftigten mit Sicherheitsaufgaben, ihrer jeweiligen Sicherheitsrollen und Kontaktdaten zu erstellen und den Beschäftigten bekanntzugeben
  - Es muss gewährleistet sein, dass Träger der wesentlichen Sicherheitsrollen unter den angegebenen Kontaktdaten erreichbar sind
  - Die Liste ist bei personellem Wechsel zu aktualisieren und mindestens jährlich auf Aktualität zu prüfen

Betriebsführung und Risikomanagement (Mustervorlage)

- **Management von Netzen und Diensten Dritter**
  - Bei der Bereitstellung von Diensten, Systemen und Netzen Dritter sind Sicherheitsanforderungen zu berücksichtigen
  - Sicherheitsanforderungen sind in Verträge einzubeziehen

Sicherheit personeller Ressourcen (Mustervorlage)

- **Hintergrundüberprüfungen**
  - Schlüsselpersonal (Systemadministratoren, Sicherheitsbeauftragte, Wachpersonal usw.) ist vor Aufnahme der Tätigkeit einer geeigneten Hintergrundüberprüfung (z. B. Einholung einer Strafregisterbescheinigung) zu unterziehen, wenn dies für seine Pflichten und Verantwortlichkeiten erforderlich ist

Sicherheit personeller Ressourcen (Mustervorlage)

- **Sicherheitskenntnisse und –training**
  - Für Entscheidungsträger und IS-Rollenträger ist Zugang zu aktuellem Schulungsmaterial und bei Bedarf Training zu ermöglichen, das die jeweils relevanten Sicherheitsaufgaben umfasst

Sicherheit personeller Ressourcen (Mustervorlage)

- **Personalwechsel**
  - Verlässt ein Mitarbeiter das Unternehmen, so sind seine Zugriffs- und Zutrittsrechte zu widerrufen und sein Mitarbeiterausweis und allfällige sonstige Ausrüstung (Schlüssel usw.) einzuziehen
  - Wechselt ein Mitarbeiter seine Stelle innerhalb des Unternehmens, so sind Zugriffs- und Zutrittsrechte, die der Mitarbeiter nicht mehr benötigt, zu widerrufen
  - Die Durchführung ist in Form einer Checkliste oder in gleichwertiger Weise zu dokumentieren

Sicherheit personeller Ressourcen (Mustervorlage)

- **Umgang mit Verletzungen**
  - Mitarbeiter, die Sicherheitsverletzungen begehen, werden dafür zur Verantwortung gezogen

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Physische Sicherheit von Einrichtungen**

  - Unautorisierter physischer Zugang zu Einrichtungen und Infrastruktur ist durch Maßnahmen zu verhindern, die für das bestehende Risiko angemessen sind, beispielsweise
    - Absperren von Türen und offen zugänglichen Schränken
    - Vergittern leicht zugänglicher Fenster und
    - ggf. Installation und Betrieb einer Alarmanlage

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Physische Sicherheit von Einrichtungen**
  - Kritische oder sensible Informationsverarbeitungseinrichtungen sind in entsprechend gesicherten Bereichen unterzubringen, die durch definierte Sicherheitsperimeter mit geeigneten Sicherheitshürden und Zutrittskontrollen geschützt werden, beispielsweise
    - Mauern,
    - Eingänge mit Zutrittskontrollen und
    - Empfangsschalter.

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Physische Sicherheit von Einrichtungen**
  - Informationsverarbeitungseinrichtungen, die vom Anbieter verwaltet werden, sind, soweit dies wirtschaftlich vertretbar ist (z. B. versperrter Serverschrank), physisch von jenen zu trennen, die von Dritten verwaltet werden, oder so abzusichern, dass ein Zutritt durch Unbefugte hintangehalten wird
  - Einrichtungen und Infrastruktur sind in angemessener Weise vor Feuer und Wassereintritt zu schützen

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Sicherheit von Betriebsstoffen**
  - Die Sicherheit von Betriebsstoffen, z. B. Elektrizität, Treibstoff und Kühlung, ist in geeigneter Weise, beispielsweise durch
    - unterbrechungsfreie Stromversorgung (USV),
    - Dieselaggregate und
    - Reservetreibstoff

  zu gewährleisten. Betriebsstoffe und Hilfseinrichtungen (z. B. USV) sind regelmäßig zu überprüfen, um ihre Funktions- und Leistungsfähigkeit zu gewährleisten

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Zugriffskontrolle für Netz und Informationssysteme**
  - Nutzer und Systeme sollen eindeutige Benutzerkennungen haben und entsprechend authentifiziert werden
  - Zugriffe sind so zu protokollieren, dass Benutzerkennungen von Nutzern und Systemen, denen der Zugriff gewährt oder verweigert wird, ersichtlich sind

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Zugriffskontrolle für Netz- und Informationssysteme**
  - Für den Zugriff auf Netz und Informations-systeme werden Kontrollen eingerichtet, die Nutzern und Systemen nur dann Zugriff gewähren, wenn dies erforderlich ist (z. B. auf Basis eines Rollenmodells, vgl. SO 3)
  - Die Kontrollen sind in geeigneter Weise, zumindest in Form einer Übersicht über Authentifizierungs- und Zugriffskontroll-methoden, zu dokumentieren.

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Informationssicherheit des Netzes und der Informationssysteme**
  - Es ist sicherzustellen, dass an der Software des Netzes und der Informationssysteme keine unbefugten Veränderungen vorgenommen werden, beispielsweise durch Einschränkung von Zugriffsmöglichkeiten sowie Einsatz von Firewalls und Verschlüsselung
  - Die Herkunft von Software ist auf aus Sicht des Anbieters (d. h. des Beziehers der Software) vertrauenswürdige Quellen einzuschränken

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Informationssicherheit des Netzes und der Informationssysteme**
  - Soweit die Authentizität von Software mittels digitaler Signaturen oder Prüfsummen feststellbar ist, sollten diese geprüft werden.

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Informationssicherheit des Netzes und der Informationssysteme**

  - Es ist sicherzustellen, dass sicherheitskritische Daten (z. B. Passwörter, private bzw. geheime kryptographische Schlüssel usw.) Unbefugten nicht zugänglich gemacht oder kompromittiert werden können (z. B. mittels Verschlüsselung).

Sicherheit von Systemen und Einrichtungen (Mustervorlage)

- **Informationssicherheit des Netzes und der Informationssysteme**

  - Internes Netz und Informationssysteme sind nach dem Stand der Technik aktuell zu halten (z. B. relevante System-Updates).

Betriebsmanagement (Mustervorlage)

- **Betriebsabläufe und Verantwortlichkeiten**

  - Für Betrieb und Verwaltung von Netz und Informationssystemen sind Betriebsabläufe aufzusetzen und Verantwortlichkeiten festzulegen. Beispielsweise sind Konsolen bei Verlassen zu sperren. Speichermedien wie USB-Sticks und Festplatten sind nicht unbeaufsichtigt zurückzulassen
  - Betriebsabläufe und Verantwortlichkeiten sind zu dokumentieren

Betriebsmanagement (Mustervorlage)

- **Änderungsmanagement**
  - Für das Änderungsmanagement sind Betriebsabläufe zu definieren und zu dokumentieren
  - Bei Änderungen wichtiger Komponenten des Netzes oder der Informationssysteme, insbesondere bei Installation, Verlagerung oder Entfernung von Einrichtungen eines Kommunikationsnetzes oder -dienstes, ist entsprechend den vordefinierten Betriebsabläufen vorzugehen
  - Wichtige Änderungen sind so zu dokumentieren, dass die angewandte Vorgangsweise nachvollziehbar ist

Betriebsmanagement (Mustervorlage)

- **Änderungsmanagement**
  - Für das Änderungsmanagement sind Betriebsabläufe zu definieren und zu dokumentieren
  - Bei Änderungen wichtiger Komponenten des Netzes oder der Informationssysteme, insbesondere bei Installation, Verlagerung oder Entfernung von Einrichtungen eines Kommunikationsnetzes oder -dienstes, ist entsprechend den vordefinierten Betriebsabläufen vorzugehen
  - Wichtige Änderungen sind so zu dokumentieren, dass die angewandte Vorgangsweise nachvollziehbar ist

Betriebsmanagement (Mustervorlage)

- **Management der IKT-Einrichtungen**
  - Zur Verwaltung von IKT-Einrichtungen und Systemkonfigurationen ist eine Liste wichtiger IKT-Einrichtungen und Systemkonfigurationen zu führen
  - Für jede IKT-Einrichtung ist ein „Besitzer" zu benennen, der für geeignete Kontrollen und für den Schutz der IKT-Einrichtung verantwortlich ist

Betriebsmanagement (Mustervorlage)

- **Management der IKT-Einrichtungen**
  - Information, die für den Betrieb des Kommunikationsnetzes oder -dienstes erforderlich ist, soll nach Sensibilität und Kritikalität klassifiziert und entsprechend der Klassifizierung durch geeignete Maßnahmen geschützt werden

Incident-Management (Mustervorlage)

- **Standards und Abläufe**
  - Sicherheitsverletzungen und Integritätsverluste (SVIV) sind sorgsam zu behandeln und ohne unnötigen Verzug an das zuständige Management (z. B. an den IT-Sicherheitsbeauftragten oder an die Geschäftsführung) zu melden
  - Mitarbeiter, Vertragspartner (Teilnehmer) und ggf. auch Dritte sind darüber zu informieren, wie mit SVIV umzugehen ist, wie diese zu melden sind (z. B. Webformular, Bugtracker) und welche Informationen die Meldung umfassen soll (z. B. Zeitpunkt, Art der Sicherheitsverletzung, Auswirkungen usw.)

Incident-Management (Mustervorlage)

- **Standards und Abläufe**
  - Die Meldung soll nach Möglichkeit über verschiedene, technologisch unabhängige Kommunikationskanäle durchführbar sein.

Incident-Management (Mustervorlage)

- **Standards und Abläufe**
  - Als Dokumentation ist eine Liste aller Sicherheitsvorfälle einschließlich des jeweiligen Status zu führen
  - Meldungen nach SM 16a, in diesem Zusammenhang ergriffene Maßnahmen sollten in der Dokumentation zu erfasst werden
  - Dokumentationseinträge sind mit Zeitangaben zu versehen
  - Es soll auch nachvollziehbar sein, welcher Mitarbeiter bei der Behandlung eines Sicherheitsvorfalls bestimmte Schritte gesetzt hat

Incident-Management (Mustervorlage)

- **Fähigkeit zur Erkennung von Vorfällen**
  - Zur Erkennung von Sicherheitsverletzungen und Integritätsverlusten sind geeignete Prozesse oder Systeme einzurichten (beispielsweise durch eine automatisierte Systemüberwachung, die alle kritischen Komponenten des Netzes sowie der IT-Systeme umfasst und die bei einem Vorfall die zuständigen Personen benachrichtigt)
  - Die Erkennung eines Vorfalls und deren Zeitpunkt sind, ggf. in Form von Logdateien oder im Rahmen der Maßnahme SM 16b, zu protokollieren

Incident-Management (Mustervorlage)

- **Konzepte für Berichte über Vorfälle und deren Kommunikation**
  - Soweit dies für einen konkreten Vorfall gesetzlich vorgeschrieben, durch die zuständige Behörde angeordnet oder aus anderen Gründen angemessen ist, sind die RTR-GmbH, die Datenschutzkommission, CERTs, betroffene Personen und/oder die Öffentlichkeit über den Vorfall zu informieren

Incident-Management (Mustervorlage)

- **Konzepte für Berichte über Vorfälle und deren Kommunikation**
  - Jene Mitarbeiter, die für die Behandlung von Sicherheitsverletzungen und/oder Integritätsverlusten bzw. für Außenauftritt und/oder Kommunikation mit Behörden zuständig sind, müssen mit dieser Informationspflicht und diesbezüglichen unternehmensinternen Regelungen vertraut sein

Betriebliches Kontinuitätsmanagement

(Mustervorlage)

- **Kontinuitätsstrategie und Notfallpläne**
  - Eine Strategie ist zu entwickeln und umzusetzen, die auf hoher Ebene Ziele für Dienste und Geschäftsprozesse vorgibt und auch eine Strategie zur Gewährleistung der betrieblichen Kontinuität, einschließlich Zielvorgaben bezüglich der Wiederherstellungszeit für Dienste und Geschäftsprozesse umfasst

Betriebliches Kontinuitätsmanagement

(Mustervorlage)

- **Kontinuitätsstrategie und Notfallpläne**
  - Weiters sind kritische Dienste und Prozesse zu identifizieren und Notfallpläne für diese zu erstellen, die klare Handlungsanleitungen für Situationen enthalten, deren Eintreten nicht als unwahrscheinlich angesehen wird
  - Die Notfallpläne sind regelmäßig, zumindest jährlich, auf Aktualität zu überprüfen und ggf. anzupassen

Betriebliches Kontinuitätsmanagement

(Mustervorlage)

- **Notfallwiederherstellung**
  - Es ist abzuschätzen, wie sich technisches Versagen oder Elementarereignisse auf die in SM 19a als kritisch identifizierten Dienste auswirken
  - Auf Basis dieser Abschätzung ist dafür Sorge zu tragen, dass die Verfügbarkeit kritischer Dienste nach technischem Versagen oder einem Elementarereignis rasch wiederhergestellt werden kann, beispielsweise durch eine geeignete Netztopologie, redundante Systeme an unterschiedlichen Standorten, ausgelagerte Backups kritischer Daten, Service Level Agreements mit Dienstleistern usw

Monitoring, Auditing und Tests

(Mustervorlage)

- **Monitoring- und Protokollierungsleitlinien**

  - In wichtigen Netz- und Informationssystemen sind Monitoring und Protokollierung so umzusetzen, dass wichtige Systemereignisse in Logdateien aufgezeichnet bzw. im Rahmen des Monitorings den zuständigen Personen mitgeteilt werden

Monitoring, Auditing und Tests

(Mustervorlage)

- **Trainieren von Notfallplänen**

  - Backup- und Notfallpläne sind zu trainieren und zu testen, um zu gewährleisten, dass Systeme und Prozesse funktionieren und dass das Personal auf große Ausfälle und Notfälle vorbereitet ist
  - Trainings von Backup- und Notfallplänen sind zu dokumentieren

Monitoring, Auditing und Tests

(Mustervorlage)

- **Testen von Netz- und Informationssystemen**

  - Netze und Informationssysteme sind zu testen, bevor sie verwendet oder an vorhandene Systeme angeschlossen werden
  - Tests sind auch nach größeren Änderungen durchzuführen
  - Die Tests sind zu dokumentieren

Monitoring, Auditing und Tests

(Mustervorlage)

- **Überprüfen und Testen der Sicherheit**

  - Es ist sicherzustellen, dass Sicherheitsüberprüfungen und Sicherheitstests bei Einführung neuer Systeme und bei signifikanten Änderungen ausgeführt werden
  - Sicherheitsüberprüfungen und Sicherheitstests sind zu protokollieren

Monitoring, Auditing und Tests

(Mustervorlage)

- **Compliance-Monitoring und Auditing**

  - Compliance-Monitoring und Audits sind in angemessenen Abständen durchzuführen
  - Die Ergebnisse sind in geeigneter Form zu dokumentieren

Vorwort zur Information Security Policy

- **Die vorliegende Information Security Policy stellt für die gesamte … (das Unternehmen) die geschlossene und strukturierte Dokumentation zur Etablierung und Umsetzung der Informationssicherheit dar. Die Information Security Policy wurde im Auftrag der Geschäftsführung erstellt und basiert auf der Norm ISO 27000ff.**

- **Die Grundlage wurde dankenswerterweise von der SV-Chipkarten Betriebs- und Errichtungsgesellschaft (SVC) zur Verfügung gestellt**

Information Security Policy (Mustervorlage)

- 1 Allgemeines Sicherheitsleitbild
- 2 Sicherheitsziele und Anforderungen
- 2.1 Identifizierung und Authentisierung
- 2.2 Zugriffskontrolle
- 2.3 Beweissicherung
- 2.4 Protokollauswertung
- 2.5 Wiederaufbereitung
- 2.6 Unverfälschtheit
- 2.7 Zuverlässigkeit der Dienstleistung
- 2.8 Übertragungssicherung

Information Security Policy (Mustervorlage)

- 2.9 Wissensteilung
- 2.10 Nachweis der Wirksamkeit / Revision
- 2.11 Kryptografisches Konzept
- 2.12 Rechtssicherheit
- 3 Verantwortlichkeiten
- 3.1 Geschäftsführung
- 3.2 Chief Information Security Officer (CISO)
- 3.3 Informationssicherheits-Management-Team
- 3.4 Mitarbeiterinnen und Mitarbeiter
- 3.5 Externe Partner

Information Security Policy (Mustervorlage)

- 4 Umsetzung
- 4.1 Informationssicherheits-Architektur
- 4.2 Geltungsbereich
- 4.3 Kontrolle
- 5 Gesetzliche und normative Rahmenbedingungen
- 6 Gültigkeitsbereich