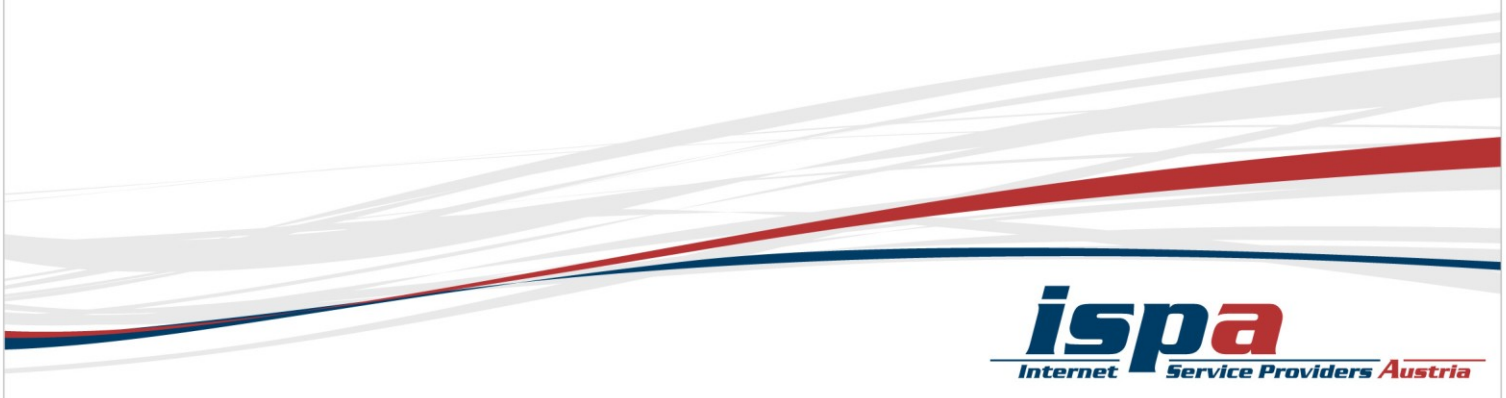
# Sicherheitskonzept (Mustervorlage) für Betreiber öffentlicher Kommunikationsnetze und -dienste

Ergebnis der ISPA-Arbeitsgruppe
unter Beteiligung der RTR-GmbH
19.11.2013



| | |
|---|---|
| Dokumentenstatus | freigegeben |
| Version | 1.1 |
| Letzte Änderung vom | 19.11.2013 |
| Dateiname | 201311_Mustervorlage_Sicherheitkonzept.docx |

# 1 Inhaltsverzeichnis

# 2Zweck und Struktur dieses Dokuments

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

Das Dokument wird derzeit überarbeitet. Eine neuere Fassung mit dem Titel *Technical Guideline on Security Measures,* Version 1.9, wurde am 26.03.2013 zur Begutachtung durch Betreiber freigegeben. Es ist in sieben Bereiche mit insgesamt 25 Sicherheitszielen gegliedert. Zu jedem Sicherheitsziel werden Maßnahmen für drei Vollkommenheitsgrade vorgeschlagen: „basic", „industry standard" und „state of the art". Die Einstufung in Vollkommenheitsgrade bleibt dem Betreiber überlassen und kann für verschiedene Sicherheitsziele unterschiedlich erfolgen.

Das vorliegende Dokument orientiert sich an den im ENISA-Dokument empfohlenen Sicherheitszielen und -maßnahmen. Es enthält Mustervorlagen für eine Informationssicherheitsleitlinie und für ein Sicherheitskonzept, die von Betreibern öffentlicher Kommunikationsnetze und -dienste verwendet werden können. Da sich das Dokument primär an kleinere Betreiber richtet, berücksichtigt es nur den Vollkommenheitsgrad „basic". Will ein Betreiber einzelnen Sicherheitszielen besser gerecht werden, so steht es ihm frei, die Mustervorlagen nur als Basis heranzuziehen und um entsprechende Maßnahmen zu ergänzen.

Kapitel 2 enthält die Mustervorlage einer Informationssicherheitsleitlinie. Diese soll die zu verfolgenden Sicherheitsziele und das angestrebte Sicherheitsniveau für alle Mitarbeiter dokumentieren. Sie soll daher nicht zu umfangreich sein.

Kapitel 3 enthält die Mustervorlage eines Sicherheitskonzepts. In diesem Dokument werden konkrete Maßnahmen festgelegt, die zur Erreichung der Sicherheitsziele ergriffen werden.

Sowohl die Informationssicherheitsleitlinie als auch das Sicherheitskonzept müssen an bestimmten Stellen an Gegebenheiten des konkreten Unternehmens angepasst werden. *Kursiv* gesetzte Abschnitte in den Kapiteln 2 und 3 bedeuten, dass an diesen Stellen unternehmensspezifische Informationen einzusetzen sind.
Kapitel 3 enthält auch Erläuterungen, die nicht zum eigentlichen Text des Sicherheitskonzepts gehören. Um Erläuterungen vom Sicherheitskonzept

abzugrenzen, werden jene Teile, die zum Sicherheitskonzept gehören, durch **Fettdruck** gekennzeichnet.

Für die Sitzung der ISPA-Arbeitsgruppe am 28.03.2013 umfasst Kapitel 3 nur jene Maßnahmen, die sich auf die im ENISA-Dokument genannten Bereiche D1 (Governance and risk management) und D2 (Human resources security) beziehen. Die Ergebnisse der Sitzung werden in das Dokument eingearbeitet. In weiteren Sitzungen am 25.04., 06.06. und 27.06.2013 wird Kapitel 3 um die Abschnitte D3 (Security of systems and facilities), D4 (Operations management), D5 (Incident management), D6 (Business continuity management), und D7 (Monitoring, auditing and testing) ergänzt.

Die ISPA bedankt sich bei allen TeilnehmerInnen sowie den Vertretern der RTR-GmbH. Bei Fragen wenden Sie sich bitte an die ISPA.

# 3 Leitlinie zur Informationssicherheit (Mustervorlage)

## 3.1 Vorbemerkung

Gemäß Vorgabe der ENISA sollte ein Betreiber eine geeignete High-Level-Leitlinie zur Informationssicherheit (IS) festlegen, die sich mit den wichtigsten Geschäftsprozessen der Organisation befasst, und diese IS-Leitlinie auf dem aktuellen Stand halten. 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.

Die AG IT-Sicherheit des Landes Berlin hat auf Basis der vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten IT-Grundschutzkataloge (insbesondere Baustein 1.0 und Maßnahme M 2.192) eine Mustervorlage für die IS-Leitlinie einer Behörde erstellt (http://www.berlin.de/imperia/md/content/seninn/itk/it-sicherheit/110310_is_leitlinie.pdf).
Ergänzt wird es durch ein weiteres Dokument, in dem die wesentlichen Punkte für den Prozess der Informationssicherheit stichpunktartig aufgelistet sind (http://www.berlin.de/imperia/md/content/seninn/itk/it-sicherheit/110310_prozess_informationssicherheit.pdf).

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. Dieser ergibt sich aus der Mustervorlage für ein Sicherheitskonzept (vgl. Kapitel 3). Das von der AG IT-Sicherheit erstellte Ergänzungsdokument ist somit in diesem Zusammenhang nicht relevant.

In einer IS-Leitlinie werden die Leitaussagen zur Informationssicherheitsstrategie in einem Unternehmen zusammengefasst, um die zu verfolgenden Sicherheitsziele und das angestrebte Sicherheitsniveau für alle Mitarbeiter zu dokumentieren. Mit der IS-Leitlinie bekennt sich die Unternehmensleitung sichtbar zu ihrer Verantwortung für Informationssicherheit. Die IS-Leitlinie ist eng verbunden mit der Etablierung eines Prozesses zur Gewährleistung der Informationssicherheit (Einrichtung eines IS-Managements).

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.

Das BSI stellt weitere ergänzende Unterlagen zum Thema bereit. Dazu zählt u. a. der BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 2.0, 2008.

Zusätzlich wird im Anhang A ein Beispiel einer Information Security Policy für erhöhte Sicherheitsanforderungen bereitgestellt. Die Grundlage wurde dankenswerterweise von der SV-Chipkarten Betriebs- und Errichtungsgesellschaft (SVC) zur Verfügung gestellt.

## 3.2 Rahmenbedingungen

Für die Erstellung einer IS-Leitlinie gelten folgende Anforderungen/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.
- Die Schlusszeichnung der IS-Leitlinie obliegt der Unternehmensleitung. Diese setzt die IS-Leitlinie im Rahmen ihrer Gesamtverantwortung für IT-Sicherheit explizit in Kraft.
- 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.

## 3.3 Inhalte

### 3.3.1 Geltungsbereich

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.

### 3.3.2 Stellenwert der Informationssicherheit

Der Stellenwert der Informationssicherheit ergibt sich aus unionsrechtlichen Vorschriften, insbesondere aus Erwägungsgrund 44 der Richtlinie 2009/140/EG: „Die zuverlässige und sichere Kommunikation von Informationen über elektronische Kommunikationsnetze erlangt zunehmend zentrale Bedeutung für die Gesamtwirtschaft und die Gesellschaft im Allgemeinen. Die Systemkomplexität, technische Ausfälle, Bedienungsfehler, Unfälle und vorsätzliche Eingriffe können Auswirkungen auf die Funktion und die Verfügbarkeit der physischen Infrastruktur haben, die wichtige Dienste für die EU-Bürger, einschließlich elektronischer Behördendienste, bereitstellt. […] In Anbetracht der Tatsache, dass die erfolgreiche Anwendung angemessener Sicherheitsmaßnahmen keine einmalige Angelegenheit ist, sondern einen ständigen Prozess der Durchführung, Überprüfung und Aktualisierung darstellt, sollten die Betreiber elektronischer Kommunikationsnetze und -dienste verpflichtet sein, Maßnahmen zum Schutz ihrer Integrität und Sicherheit im Einklang mit der Risikobeurteilung zu treffen, wobei dem Stand der Technik solcher Maßnahmen Rechnung zu tragen ist."

### 3.3.3 Sicherheitsziele

Die Ziele zur Informationssicherheit ergeben sich aus der von der Europäischen Agentur für Netz- und Informationssicherheit veröffentlichten *Technical Guideline on Security Measures,* Version 1.9. Im Einzelnen sind dies

1. Festlegung der Informationssicherheitsleitlinie,
2. Festlegung eines Rahmens für das Risikomanagement,
3. Festlegung eines Rollenmodells für Sicherheitsaufgaben,
4. Festlegung von Sicherheitsanforderungen für Leistungen Dritter,
5. Durchführung von Hintergrundüberprüfungen,
6. Vermittlung von Sicherheitskenntnissen und -training,
7. Festlegung eines Prozesses zur Verwaltung personeller Wechsel,
8. Festlegung eines Prozesses für disziplinäre Maßnahmen,
9. Wahrung der physischen Sicherheit für Anlagen und Infrastruktur der Netze und Dienste sowie Schutz vor Elementarereignissen,
10. Wahrung der Sicherheit von Betriebsstoffen und unterstützenden Anlagen,
11. Kontrolle des Zugriffs auf Netzen und Informationssysteme,
12. Wahrung der Informationssicherheit von Netzen und Informationssystemen zum Schutz vor Malware, Viren und üblichen Bedrohungen,
13. Festlegung von Betriebsabläufen und Verantwortlichkeiten,
14. Festlegung eines Prozesses für das Veränderungsmanagement,
15. Festlegung von Konfigurationskontrollen und Abläufen zur Verwaltung von IT-Einrichtungen,
16. Festlegung standardisierter Abläufe für den Umgang mit Sicherheitsverletzungen und Integritätsverlusten,

17. Herstellung der Fähigkeit zur Entdeckung von Sicherheitsverletzungen und Integritätsverlusten,
18. Festlegung, Wartung und Einhaltung eines Kommunikationsplans für Sicherheitsverletzungen und Integritätsverluste,
19. Festlegung einer Strategie zur Gewährleistung der Verfügbarkeit von Netzen und Diensten sowie Festlegung eines Notfallplans,
20. Herstellung der Fähigkeit zum Disaster Recovery für die Wiederherstellung von Netzen und Diensten,
21. Festlegung von Leitlinien für Systemüberwachung und Protokollierung,
22. Festlegung von Leitlinien zum Testen und Üben von Notfallplänen,
23. Festlegung von Leitlinien zum Testen von Netzen und Informationssystemen,
24. Festlegung einer Leitlinie zur Durchführung von Sicherheitsbewertungen und Sicherheitstests,
25. Festlegung einer Leitlinie zur Überwachung und Überprüfung der Befolgung von Vorschriften.

Eine hohe Verfügbarkeit der Kommunikationsnetze und -dienste wird angestrebt, aber nicht allgemein garantiert (eventuell jedoch im Rahmen eines Service Level Agreements). Eine hohe Verfügbarkeit kritischer Systemkomponenten wird durch Redundanz und entsprechende Wartungsverträge gewährleistet.

Maßnahmen zum Schutz von Integrität und Vertraulichkeit der Daten entsprechen den gesetzlichen Erfordernissen (insbesondere § 14 DSG 2000 und § 95 TKG 2003).

Sicherheitsmaßnahmen werden so ausgewählt, dass der dafür erforderliche Aufwand in einem günstigen Verhältnis zur Minderung des Risikos steht.

### 3.3.4 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;*
- *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.*

### 3.3.5 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 Zusammenarbeit.*
*Verantwortung der Leitungsebene z. B. bzgl.*

- *Bereitstellung ausreichender Ressourcen für IT-Sicherheit,*
- *Unterstützung der bedarfsgerechten Fort- und Weiterbildung,*
- *ständiger Verbesserung des Sicherheitsniveaus.*

### 3.3.6 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.

# 4Sicherheitskonzept (Mustervorlage)

## 4.1 D1 Betriebsführung und Risikomanagement

### 4.1.1 SO 1 IS-Leitlinie

Der Anbieter sollte eine geeignete IS-Leitlinie festlegen und diese auf dem aktuellen Stand halten.

**SM 1a: Das vorliegende Sicherheitskonzept konkretisiert die von der Unternehmensleitung erlassene IS-Leitlinie.**

**SM 1b: 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. 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.**

### 4.1.2 SO 2 Rahmenbedingungen des Risikomanagements

Der Anbieter sollte geeignete Rahmenbedingungen des Risikomanagements festlegen und regelmäßig aktualisieren, um Risiken für die Kommunikationsnetze und -dienste zu identifizieren und zu behandeln.

Risiko ist eine Funktion der Wahrscheinlichkeit, dass eine gegebene Bedrohung (z. B. Wassereintritt) auf eine bestimmte Schwachstelle (z. B. Server) einwirkt, und dem resultierenden Schaden eines solchen Ereignisses auf die Organisation.

**SM 2a: 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.**

**SM 2b: 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.**

### 4.1.3 SO 3 Sicherheitsrollen und -verantwortlichkeiten

Der Anbieter sollte eine geeignete Struktur der Sicherheitsrollen und -verantwortlichkeiten festlegen und regelmäßig aktualisieren.

**SM 3a: 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:**

1. **Sicherheitsexperte: Mindestens ein Sicherheitsexperte muss benannt werden. Dieser muss regelmäßig und direkt der Unternehmensführung berichten können.**

2. **[Datenschutzexperte: Es kann ein Datenschutzexperte benannt werden, der sich insbesondere mit Datensicherheitsmaßnahmen befasst.]**

3. **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.**

**Ob eine Rolle durch eine oder mehrere Personen besetzt wird, obliegt dem Unternehmen.**

*Für folgende Aufgaben sind Verantwortlichkeiten festzulegen:*

*a) Umsetzung und Befolgung der Informationssicherheitsleitlinie;*
*b) Schutz von Betriebsmitteln vor unbefugtem Zugriff, Enthüllung, Veränderung, Zerstörung oder Beeinträchtigung;*
*c) Ausführung besonderer Sicherheitsprozesse oder -tätigkeiten;*
*d) Sicherstellung, dass Verantwortlichkeiten bestimmten Personen zugewiesen werden;*
*e) Information der Organisation über Sicherheitsereignisse oder potenzielle Ereignisse oder andere Sicherheitsrisiken.*

**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.**

**SM 3b: 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.**

### 4.1.4 SO 4 Management von Netzen und Diensten Dritter

Der Anbieter sollte eine Leitlinie mit Sicherheitsanforderungen für Bereitstellung und Management von Netzen und Diensten Dritter (z. B. IT-Dienste, Software, Callcenter, Zusammenschaltungen, Gemeinschaftseinrichtungen) festlegen und aktuell halten, sodass Consulting, Outsourcing bzw. andere Dienste Dritter die Sicherheit des Anbieters nicht beeinträchtigen.

**SM 4a: Bei der Bereitstellung von Diensten, Systemen und Netzen Dritter sind Sicherheitsanforderungen zu berücksichtigen. Sicherheitsanforderungen sind in Verträge einzubeziehen.**

Es erscheint wenig zielführend, SM 4a an dieser Stelle zu konkretisieren, weil die Sicherheitsanforderungen von der Art der Leistung abhängen, die ein Dritter erbringt. Bei manchen Leistungen stehen eher Sicherheitsanforderungen für den Schutz von Betriebs- und Geschäftsgeheimnissen im Vordergrund, bei anderen Leistungen beziehen sich Sicherheitsanforderungen vielleicht auf die Verfügbarkeit zugekaufter Dienste. Daher wird diese Bestimmung im Sicherheitskonzept eher allgemein gehalten. Hinsichtlich der Anwendbarkeit der IS-Leitlinie auf Dritte sei noch einmal auf SM 1b hingewiesen.

## 4.2 D2 Sicherheit personeller Ressourcen

### 4.2.1 SO 5 Hintergrundüberprüfungen

Der Anbieter sollte geeignete Hintergrundüberprüfungen für Personal (Angestellte, Vertragspartner und Drittnutzer) durchführen, wenn dies für ihre Pflichten und Verantwortlichkeiten erforderlich ist.

**SM 5a: 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.**

### 4.2.2 SO 6 Sicherheitskenntnisse und -training

Der Anbieter sollte sicherstellen, dass sein Personal über ausreichende Sicherheitskenntnisse verfügt und bezüglich Sicherheit regelmäßig trainiert wird.

**SM 6a: Für Entscheidungsträger und IS-Rollenträger ist Zugang zu aktuellem Schulungsmaterial und bei Bedarf Training zu ermöglichen, das die jeweils relevanten Sicherheitsaufgaben umfasst.**

### 4.2.3 SO 7 Personalwechsel

Der Anbieter sollte einen geeigneten Prozess zur Verwaltung von Personalwechsel (Angestellte, Vertragspartner und Drittnutzer) bzw. Änderungen von Rollen und Verantwortlichkeiten festlegen und auf dem aktuellen Stand halten. Neues Personal sollte über die in Kraft befindlichen Leitlinien und Verfahrensweisen informiert und darin eingeschult werden. Konten, Rechte und Besitz von Ausrüstung oder Daten sollen bei personellem Wechsel überprüft werden.

**SM 7a: 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.**

### 4.2.4 SO 8 Umgang mit Verletzungen

Der Anbieter sollte für Angestellte, die eine Sicherheitsverletzung begangen haben, einen disziplinären Prozess festlegen oder einen umfassenderen Prozess haben, der Sicherheitsverletzungen umfasst.

**SM 8a: Mitarbeiter, die Sicherheitsverletzungen begehen, werden dafür zur Verantwortung gezogen.**

## 4.3 Sicherheit von Systemen und Einrichtungen

### 4.3.1 SO 9 Physische Sicherheit von Einrichtungen

Der Anbieter sollte für angemessene physische Sicherheit von Einrichtungen und Infrastruktur für Netze und Dienste Sorge tragen.

**SM 9a: 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.**

**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.**

**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.**

### 4.3.2 SO 10 Sicherheit von Betriebsstoffen

Der Anbieter sollte für angemessene Sicherheit von Betriebsstoffen und Hilfseinrichtungen (z. B. Elektrizität, Treibstoff und Kühlung) Sorge tragen.

**SM 10a: 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.**

### 4.3.3 SO 11 Zugriffskontrolle für Netz und Informationssysteme

Der Anbieter sollte geeignete (logische) Zugriffskontrollen für den Zugriff auf Netz und Informationssysteme einrichten.

**SM 11a: 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.**

**SM 11b: Für den Zugriff auf Netz und Informationssysteme 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 Zugriffskontrollmethoden, zu dokumentieren.**

### 4.3.4 SO 12 Informationssicherheit des Netzes und der Informationssysteme

Der Anbieter sollte eine angemessene Informationssicherheit des Netzes und der Informationssysteme gewährleisten, um diese vor Schadprogrammen, Viren und anderen häufig vorkommenden Bedrohungen zu schützen.

**SM 12a: 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. Soweit die Authentizität von Software mittels digitaler Signaturen oder Prüfsummen feststellbar ist, sollten diese geprüft werden.**

**SM 12b: 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).**

**SM 12c: Internes Netz und Informationssysteme sind nach dem Stand der Technik aktuell zu halten (z. B. relevante System-Updates).**

## 4.4 Betriebsmanagement

### 4.4.1 SO 13 Betriebsabläufe und Verantwortlichkeiten

Der Anbieter sollte Betriebsabläufe und Verantwortlichkeiten festlegen.

**SM 13a: 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.**

### 4.4.2 SO 14 Änderungsmanagement

Um die Wahrscheinlichkeit von Unterbrechungen und Fehlern auf Grund von Änderungen zu minimieren, sollte der Anbieter einen Prozess für das Änderungsmanagement aufsetzen.

**SM 14a: 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.**

### 4.4.3 SO 15 Management der IKT-Einrichtungen

Um die Verfügbarkeit und den Status von IKT-Einrichtungen zu verifizieren, sollte der Anbieter Konfigurationskontrollen und Betriebsabläufe für das Management festlegen.

**SM 15a: 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.**
**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.**

## 4.5 Incident-Management

### 4.5.1 SO 16 Standards und Abläufe

Der Anbieter sollte Standards und Abläufe für das Störungsmanagement etablieren und aktuell halten.

**SM 16a: 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.). Die Meldung soll nach Möglichkeit über verschiedene, technologisch unabhängige Kommunikationskanäle durchführbar sein.**

**SM 16b: 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.**

### 4.5.2 SO 17 Fähigkeit zur Erkennung von Vorfällen

Der Anbieter sollte imstande sein, Sicherheitsverletzungen und Integritätsverluste zu erkennen und darüber zeitnah die zuständigen Personen zu informieren.

**SM 17a: 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.**

### 4.5.3 SO 18 Konzepte für Berichte über Vorfälle und deren Kommunikation

Der Anbieter sollte geeignete Konzepte für Berichte über Sicherheitsverletzungen und Integritätsverluste sowie deren Kommunikation entwickeln, aktuell halten und umsetzen. Diese Konzepte sollten insbesondere auch Benachrichtigungen der Datenschutzkommission und ggf. betroffener Personen gemäß § 95a TKG 2003 und Mitteilungen an die RTR-GmbH gemäß § 16a TKG 2003 umfassen. Die Datenschutzkommission ist zu benachrichtigen, wenn durch den Vorfall der Schutz personenbezogener Daten verletzt wurde. Der RTR-GmbH sind nur Vorfälle mit beträchtlichen Auswirkungen mitzuteilen. Weitere Informationen dazu sind unter https://www.rtr.at/de/tk/Netzsicherheit verfügbar.

**SM 18a: 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. 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.**

## 4.6 Betriebliches Kontinuitätsmanagement

### 4.6.1 SO 19 Kontinuitätsstrategie und Notfallpläne

Der Anbieter sollte eine Strategie entwickeln und aktuell halten, um die kontinuierliche Verfügbarkeit seiner Kommunikationsnetze und -dienste zu gewährleisten, und er sollte Notfallpläne erstellen und aktuell halten.

**SM 19a: 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. 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.**

### 4.6.2 SO 20 Notfallwiederherstellung

Der Anbieter sollte die Fähigkeit zur Wiederherstellung seiner Kommunikationsnetze und -dienste nach einem Notfall entwickeln und beibehalten. Unter „Notfall" sind dabei technisches Versagen, aber auch Feuer, Wassereintritt, Erdbeben und andere Elementarereignisse, die die Infrastruktur betreffen könnten.

**SM 20a: 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.**

## 4.7 Monitoring, Auditing und Tests

### 4.7.1 SO 21 Monitoring- und Protokollierungsleitlinien

Der Anbieter sollte für Monitoring und Protokollierung Leitlinien erstellen und diese aktuell halten.

**SM 21a: 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.**

### 4.7.2 SO 22 Trainieren von Notfallplänen

Der Anbieter sollte zum Testen und Trainieren von Backup- und Notfallplänen, ggf. in Zusammenarbeit mit Dritten, z. B. Netzbetreibern, Leitlinien erstellen und aktuell halten.

**SM 22a: 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.**

### 4.7.3 SO 23 Testen von Netz- und Informationssystemen

Der Anbieter sollte zum Testen von Netz und Informationssystemen Leitlinien erstellen und aktuell halten, insbesondere beim Anschluss an neue Netz- und Informationssysteme.

**SM 23a: 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.**

### 4.7.4 SO 24 Überprüfen und Testen der Sicherheit

Der Anbieter sollte zur Durchführung von Sicherheitsbewertungen und Sicherheitstests aller Anlagen eine geeignete Leitlinie erstellen und aktuell halten.

**SM 24a: Es ist sicherzustellen, dass Sicherheitsüberprüfungen und Sicherheitstests bei Einführung neuer Systeme und bei signifikanten Änderungen ausgeführt werden. Sicherheitsüberprüfungen und Sicherheitstests sind zu protokollieren.**

### 4.7.5 SO 25 Compliance-Monitoring und Auditing

Der Anbieter sollte für Compliance-Monitoring und Auditing in Bezug auf dieses Dokument eine Leitlinie erstellen und aktuell halten. Compliance-Reporting und das Ansprechen von Unzulänglichkeiten beim Audit sollten in einem Prozess geregelt sein.

**SM 25a: Compliance-Monitoring und Audits sind in angemessenen Abständen durchzuführen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.**

# Anhang A
# Information Security Policy der <Firma>

Ergebnis der ISPA-Arbeitsgruppe
27.06.2013

ispa
Internet Service Providers Austria

# Inhaltsverzeichnis

# 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.

Diese Information Security Policy beschreibt die sicherheitsrelevanten Anforderungen, welche für alle physikalischen Systeme und Teilsysteme, für deren einzelne Komponenten, für jede Art von Software, Daten und Informationen, für Strukturen und Prozesse, für die erforderliche Infrastruktur sowie für alle internen und externen Mitarbeiterinnen und Mitarbeiter sowie Funktionsträger (Aufsichtsrat, Gesellschafter-Vertreter) gelten.

Mit der Information Security Policy wird keine Ausarbeitung geschaffen, welche lediglich den Charakter einer Momentaufnahme hat und mit der Änderung von technischen Randbedingungen oder Beurteilungen schnell an Wert verliert. Vielmehr ist diese ein fortschreibungsfähiges, lebendes Dokument.

Die Fortschreibung dieser Leitlinie in definierten Zyklen ist erforderlich, da jedes Sicherheitskonzept dynamische Komponenten besitzt, deren Änderungen Auswirkungen auf die identifizierten Risiken und damit auch auf die zu ergreifenden Sicherheitsmaßnahmen haben.

# 1 Allgemeines Sicherheitsleitbild

Die Geschäftsführung hat die Aufgabe, gemeinsam mit allen Mitarbeiterinnen und Mitarbeitern sowie externen Partnern die Vermögenswerte des Unternehmens und die ihr von Dritten anvertrauten schützenswerten Güter zu bewahren.

Zu den Vermögenswerten des Unternehmens zählen die materiellen Werte wie etwa das Inventar und die immateriellen Werte wie etwa das „Know How" der Mitarbeiterinnen und Mitarbeiter. Zu den schützenswerten Gütern, die dem Unternehmen von Dritten anvertraut sind, zählen die von uns im Rahmen unserer Dienstleistung ver- und erarbeiteten Informationen.

Die Gesamtheit aller Schutzmaßnahmen muss regelmäßig auf deren Aktualität und Wirksamkeit kontrolliert und in einem Sicherheitsbericht dargelegt werden.

Die in Folge beschriebene Information Security Policy stellt somit eine verbindliche Grundlage unseres Handelns dar.

# 2Sicherheitsziele und Anforderungen

Das vom Unternehmen eingeführte Informations-Sicherheits-Management-System (ISMS) orientiert sich an den Auflagen und Anforderungen der ISO 27000ff.

Weiterentwicklung und Betrieb der Internet Services und damit in Zusammenhang stehender Tätigkeiten erfordern die Definition angemessener Sicherheitsziele. Diese ergeben sich aus den Qualitäts- und Sicherheitsanforderungen des Unternehmens, des Mutterunternehmens und der Vertragspartner sowie den verschiedenen gesetzlichen Anforderungen (insbesondere dem TKG 2003 und den auf seiner Grundlage ergangenen Verordnungen).

Die Sicherheitsziele stellen die oberste Ebene der Sicherheitsanforderungen an alle Systeme und Prozesse des Unternehmens dar. Sie beinhalten sechs Grundwerte (oberste Regeln bzw. Schutzziele), die nachfolgend aufgeführt sind. Diese Grundwerte müssen

- von den Verantwortlichen des Unternehmens gelebt und ständig auf ihre Umsetzung überprüft werden,
- von allen Partnern des Unternehmens berücksichtigt werden.

Hierauf basierend leiten sich die systemspezifischen Schutzziele ab:

- Integrität
  Das Verhindern nichtautorisierter Modifikation und Manipulation der zu übertragenden Daten ist sicherzustellen. Die regelwidrige Generierung und Veränderung von Informationen, welche unter anderem die Anspruchsbelege, Abstimmungsdaten oder Signaturdaten darstellen, ist sicher zu verhindern. Es ist jederzeit sicherzustellen, dass Erzeugung, Veränderung und Löschung von sicherheitsrelevanten Informationen ausschließlich nach definierten Regeln erfolgen. Die zu implementierenden Sicherheitsmechanismen zur Bewahrung der Integrität müssen eine hohe Widerstandsfähigkeit besitzen.

- Verfügbarkeit
  Die Daten müssen, wenn sie benötigt werden, zur Verfügung stehen. Zur Verfügbarkeit zählt auch die Betriebssicherheit von EDV-Systemen und Programmen ebenso wie der Schutz vor Datenverlust. Störungen und Kompromittieren einzelner Komponenten müssen entweder in den Auswirkungen beschränkt sein oder sicher verhindert werden. Es ist jederzeit sicherzustellen, dass der Systembetrieb auch bei Störungen von Systembestandteilen (Hardware, Software und Prozesse), Ausfall von sicherheitstechnischen Einrichtungen und Verlust der Vertraulichkeit dezentraler sicherheitstechnischer Einrichtungen weitergeführt werden kann. Die zu

implementierenden Sicherheitsmechanismen zur Aufrechterhaltung der Verfügbarkeit müssen eine hohe Widerstandsfähigkeit besitzen.

- Vertraulichkeit
  Die Daten müssen den Datenschutz- und Datensicherheitsanforderungen genügen. Vertraulichkeit bedeutet, dass die Daten nur Berechtigten zur Kenntnis gelangen und nur von diesen Personen verarbeitet werden dürfen. Es ist jederzeit sicherzustellen, dass alle schutzbedürftigen Informationen und Daten vor unbefugter Preisgabe bewahrt werden.

- Authentizität
  Authentizität (auch Fälschungsschutz) bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit. Durch Authentifikation, also dem Nachweis der Authentizität, kann die Unverfälschtheit und die Urheberschaft der Daten (Informationen) nachgewiesen werden.

- Nicht-Abstreitbarkeit
  Bei der Nicht-Abstreitbarkeit (auch Verbindlichkeit) unterscheidet man zwischen Nicht-Abstreitbarkeit der Herkunft und Nicht-Abstreitbarkeit des Erhalts. In beiden Fällen geht es darum, dass der Absender der Daten oder elektronischen Informationen nicht in der Lage sein sollte, seine Urheberschaft zu bestreiten, vor allem sollte sich diese gegenüber Dritten nachweisen lassen.

- Beweissicherung
  Es ist sicherzustellen, dass die einzelnen Systeme und sicherheitsrelevanten Prozesse revisionsfähig sind. Die zu implementierenden Sicherheitsmechanismen zur Gewährleistung der Revisionsfähigkeit müssen eine mittlere Mechanismenstärke besitzen.

Diese Grundwerte (Sicherheitsziele) sowie alle mitgeltenden Unterlagen und Prozesse gelten für das gesamten Unternehmen und sind für alle Mitarbeiter des Unternehmens verbindlich.

## 2.1 Identifizierung und Authentisierung

### 2.1.1 zwischen Teilen der Systeme

Sicherheitstechnische Einrichtungen müssen sich gegenseitig bei jeder Transaktion eindeutig identifizieren und authentisieren.

Die Authentizität der sicherheitstechnischen Einrichtungen muss während der gesamten Transaktion gewährleistet sein.

### 2.1.2 gegenüber Benutzer

Das jeweilige System muss je nach Kritikalität den Zugreifenden eindeutig identifizieren und authentifizieren. Dabei ist zu beachten, dass die Identifikation und Authentisierung vor dem ersten Zugriff zu erfolgen hat. Zusätzlich ist der Zeitraum, in dem weitere Zugriffe ohne erneute Identifikation möglich sind, zu beschränken.

## 2.2 Zugriffskontrolle

Änderungen von Außerhalb müssen über eine gesicherte Schnittstelle in das System übernommen werden. Änderungen anderer sicherheitsrelevanter Informationen dürfen nur durch dazu berechtigte sicherheitstechnische Einrichtungen bzw. auf Anforderung eines berechtigten Benutzers erfolgen.

Der schreibende bzw. modifizierende Zugriff auf sicherheitsrelevante Informationen darf nur identifizierten und authentisierten Teilen im System mittels festgelegter Prozesse nach einer Rechte-Prüfung möglich sein.

Der lesende Zugriff auf sonstige Protokollinformationen darf nur identifizierten und autorisierten Benutzern möglich sein.

Der erfolglose Versuch einer Identifikation oder Autorisierung darf keine für Angriffe verwertbaren Informationen über Identifikation- oder Autorisierung bzw. die dahinterstehenden Personen oder Einrichtung erbringen.

## 2.3 Beweissicherung

Für jeden aktiven sicherheitskritischen Teil eines Systems muss eine Protokollierungskomponente vorhanden sein, die jede versuchte oder durchgeführte Generierung, Änderung oder Löschung von sicherheitsrelevanten Informationen protokolliert.

Der Umfang der protokollierten Daten muss den Zwecken der Aufklärung von Zweifelsfällen in angemessener Zeit nach einer Interaktion und Behebung von Störungen genügen.

Die Systeme müssen Mechanismen enthalten, welche Ausfälle bzw. Störungen von Teilen des Systems und Übertragungskanälen erkennen und protokollieren. Änderung und vorzeitige Löschung von Protokollinformation muss zuverlässig verhindert werden.

Zentrale Komponenten müssen eine Protokollierungskomponente erhalten, die alle sicherheitsrelevanten Aktionen von Systembetreuern und Wartungstechnikern aufzeichnet.

Bei allen Protokollen ist mit geeigneten Methoden die Authentizität sicherzustellen.

## 2.4 Protokollauswertung

Werkzeuge zur Auswertung und Verwaltung von Protokolldaten müssen vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer oder Teile des Systems zu identifizieren.

Es muss einen Mechanismus zur Überwachung von Ereignissen geben, die entweder besonders sicherheitsrelevant sind oder aufgrund der Häufigkeit ihres Auftretens zu einer kritischen Bedrohung der Sicherheit des Systems führen könnten.

## 2.5 Wiederaufbereitung

Alle Speicherobjekte mit entsprechendem Schutzbedarf, die den Systemen wieder zur Verfügung gestellt werden, müssen vor einer Wiederverwendung durch andere Benutzer oder Prozesse so aufbereitet werden, dass keine Rückschlüsse auf ihren früheren Inhalt möglich sind.

## 2.6 Unverfälschtheit

Das Regelsystem zur Generierung, Veränderung und Löschung von sicherheitsrelevanten Informationen ist explizit zu formulieren und auf Sinnhaftigkeit und Widerspruchsfreiheit zu prüfen.

Für Entwicklung, Produktion, Test und nachträgliche Veränderung von sicherheitstechnischen Einrichtungen sind explizite Regeln zur Sicherstellung der Einhaltung der Sicherheitsziele zu formulieren und deren Einhaltung zu verifizieren.

Es sind Mechanismen zu implementieren, welche die Integrität jeder sicherheitsrelevanten Information und jeder sicherheitstechnischen Einrichtung vor

ihrer Verwendung verifizieren. Die Konfiguration jeder sicherheitstechnischen Einrichtung muss identifizierbar, überprüfbar und gesichert sein.

## 2.7 Zuverlässigkeit der Dienstleistung

Es müssen Mechanismen vorhanden sein, die im Fall des Verlustes der Vertraulichkeit von dezentralen Komponenten eine sichere Fortführung des Betriebes innerhalb einer festgelegten Zeit ermöglichen. Zentrale Komponenten sind physisch zu sichern.

Es müssen geeignete technische und organisatorische Maßnahmen vorgesehen sein, um Ausfälle und Teilausfälle von Komponenten des jeweiligen Systems so zu überbrücken, dass alle fortlaufend benötigten Funktionen auch im Rest-System zur Verfügung stehen.

Nach der Behebung eines solchen Ausfalls muss die Komponente wieder so in das System integriert werden können, dass ein kontinuierlicher Betrieb der fortlaufend benötigten Funktionen auch im Rest-System gewährleistet ist. Sobald ausgefallene Online-Komponenten wieder verfügbar werden, wiederholen die vom Ausfall betroffenen sicherheitstechnischen Einrichtungen die als fehlerhaft protokollierten Nachrichten und Prozesse, bis der Zustand wiederhergestellt ist, den das System ohne Ausfall eingenommen hätte. Kann dieser Zustand innerhalb einer vorgegebenen Zeit nicht wiederhergestellt werden, meldet das System einen gravierenden Systemfehler. Werden Komponenten auch für andere Anwendungen genützt, ist zuverlässig sicherzustellen, dass dadurch keine Beeinträchtigung der Sicherheit eintritt.

## 2.8 Übertragungssicherung

### 2.8.1 Datenvertraulichkeit

Die Systeme müssen sicherheitsrelevante Informationen zwischen den sicherheitstechnischen Einrichtungen mittels eines hinreichend sicheren Algorithmus verschlüsselt übertragen.

### 2.8.2 Datenintegrität

Die Systeme müssen so entworfen sein, dass Übertragungsfehler und Verletzungen der Integrität sicher als solche erkannt und korrigiert werden können.

Die Kommunikationsprotokolle zu anderen sicherheitstechnischen Einrichtungen/technischen Einrichtungen enthalten Mechanismen, die Verletzungen der Integrität im System durch zufällige oder beabsichtigte Beeinflussung am Kommunikationsweg sicher erkennen lassen oder verhindern.

Es muss ein Mechanismus existieren, der im Fall der Verletzung der Integrität den ursprünglichen Zustand der Daten wiederherstellt und die Wiederholung des Datenaustausches ermöglicht.

Das System muss Mechanismen hoher Wirksamkeit enthalten, die unbefugte Manipulationen von sicherheitsrelevanten Informationen erkennen lassen. Die Manipulation von Protokolldaten soll mit mittlerer Wirksamkeit erkannt werden können.

Das System muss Mechanismen hoher Wirksamkeit enthalten, die das Wiedereinspielen von Daten erkennen lassen.

### 2.8.3 Sende- und Empfangsnachweise

Übertragene Informationen sind so zu kennzeichnen, dass der Empfänger den Absender eindeutig verifizieren kann. Es ist ein Mechanismus einzusetzen, der es dem Absender von Informationen ermöglicht, den Empfang durch einen eindeutig identifizierten und authentisierten Empfänger festzustellen.

## 2.9 Wissensteilung

Informationen über die Systeme und Produktionsmittel sind so zwischen Organisationseinheiten aufzuteilen, dass keine Organisationseinheit allein in der Lage ist, sicherheitstechnische Einrichtungen oder sicherheitsrelevante Informationen zu erzeugen oder zu verfälschen. Die Mitglieder der Organisationseinheit sind über Sinn und Wirkung und Handhabung der Wissensteilung nachweislich zu belehren.

## 2.10 Nachweis der Wirksamkeit/ Revision

Die Wirksamkeit der obligatorischen Mechanismen ist in regelabhängigen Zeitabständen nachzuweisen.

## 2.11 Kryptografisches Konzept

Sofern die Sicherung der Integrität, Verfügbarkeit oder Beweissicherung auf ein kryptografisches Konzept aufbaut, ist ein solches explizit zu definieren und auf Konsistenz mit der Information Security Policy zu prüfen.

## 2.12 Rechtssicherheit

Es ist sicherzustellen, dass unbefugte Manipulationen strafrechtlich verfolgt werden können.

# 3 Verantwortlichkeiten

## 3.1 Geschäftsführung

Die Gesamtverantwortung für Informationssicherheit im Unternehmen liegt bei der Geschäftsführung.

Die Geschäftsführung ist insbesondere verantwortlich für (siehe dazu auch ISO 27000ff)

- die Überprüfung und die Abnahme der Information Security Policy,
- das Vertreten der Information Security Policy nach innen und außen,
- die Informationssicherheits-Organisation sowie
- die strategische Ausrichtung der Informationssicherheit.

Diese Verantwortung ist nicht delegierbar. Die Geschäftsführung bedient sich jedoch in der Umsetzung des Informationssicherheits-Management-Teams.

## 3.2 Chief Information Security Officer (CISO)

Der Chief Information Security Officer (CISO) des Unternehmens bildet das zentrale und unternehmensweite Steuerungsorgan für Informationssicherheit.

Der CISO ist im Besonderen verantwortlich für die

- Erstellung von Sicherheitsrichtlinien
- Planung und Umsetzung der Sicherheitsmaßnahmen

und berichtet direkt an die Geschäftsführung über sicherheitsrelevante Themen und Projektanträge.

## 3.3 Informationssicherheits-Management-Team

Das Informationssicherheits-Management-Team (SMMT) besteht aus der Geschäftsführung, dem Vertreter für rechtliche Angelegenheiten, den

Bereichsleiterinnen und Bereichsleitern, dem Datenschutzbeauftragten und dem Chief Information Security Officer.

## 3.4 Mitarbeiterinnen und Mitarbeiter

Die Mitarbeiterinnen und Mitarbeiter, die Führungskräfte und die Informationssicherheits-Organisation sind die Basis für eine angemessene Informationssicherheit im Unternehmen. Erreicht wird das geforderte Maß an Informationssicherheit dadurch, dass alle Mitarbeiterinnen und Mitarbeiter für die vorliegende Information Security Policy sensibilisiert sind, die daraus abgeleiteten Sicherheitsrichtlinien und Sicherheitsmaßnahmen beachten und die jeweiligen Tätigkeiten danach ausrichten.

## 3.5 Externe Partner

Die Bedeutung der Informationssicherheit für das Unternehmen wird externen Partnern verdeutlicht. Sie sind verpflichtet, bei der Erbringung ihrer Dienstleistung für das Unternehmen die vorliegende Information Security Policy und die auf die zu erbringende Dienstleistung zutreffenden gültigen Sicherheitsstandards und -richtlinien einzuhalten.

Wenn notwendig, ist mit dem externen Partner ein Geheimhaltungsvertrag, (auch Geheimhaltungserklärung, Geheimhaltungsvereinbarung, Vertraulichkeitsvereinbarung, Verschwiegenheitsvereinbarung, NDA (Abkürzung für englisch non-disclosure agreement) oder CDA (Abk. für englisch confidential disclosure agreement)) abzuschließen, welcher regelt, wie der externe Partner mit ihm zugänglich gemachten Informationen umzugehen hat.

# 4 Umsetzung

Die Umsetzung des ISMS des Unternehmens erfolgt durch hierarchisch erstellte Sicherheitsrichtlinien und Sicherheitsmaßnahmen (siehe Abb.1) welche nach ISO 27000ff erstellt werden.

## 4.1 Informationssicherheits-Architektur

In der Informationssicherheits-Architektur wird festgelegt, wie die Informationssicherheit beim Unternehmen umgesetzt wird.


Abbildung 1 Informationssicherheits-Architektur

Auf der obersten Ebene der Informationssicherheits-Architektur findet sich die Information Security Policy, welche die Sicherheitsziele und Verantwortlichkeiten festlegt und unternehmensweit Gültigkeit hat. Die Information Security Policy bildet den Rahmen für die Sicherheitsrichtlinien und Sicherheitsmaßnahmen. Die Sicherheitsrichtlinien beschreiben die grundlegenden Sicherheitsanforderungen auf Basis der definierten Information Security Policy. Diese Sicherheitsrichtlinien werden, sofern dies notwendig ist, durch spezielle Sicherheitsmaßnahmen spezifiziert, die im Detail technische bzw. organisatorische Durchführungsbestimmungen enthalten. Sicherheitsmaßnahmen können auf Unternehmensebene festgelegt, aber auch in

einzelnen Bereichen oder Projekten nach den jeweiligen Anforderungen definiert werden.

## 4.2 Geltungsbereich

Zum direkten Geltungsbereich der Information Security Policy zählen alle Bereiche im direkten Einfluss des Unternehmens. Zusätzlich zu diesem Bereich gehören noch all jene Objekte, welche zwar nicht im Einflussbereich des Unternehmens stehen, aber einen essentiellen Einfluss für die Erfüllung der Kernaufgaben des Unternehmens haben (indirekter Geltungsbereich). Für all jene Objekte, welche zwar nicht im Einflussbereich des Unternehmens sind, aber im physikalischen oder logischen Bereich des Unternehmens stehen (z.B. Fremd-Netzwerk-Anschluss), gilt als Grenze des Geltungsbereichs der jeweilige Übergabepunkt. Informationssicherheit ist im gesamten - im direkten und indirekten - Geltungsbereich des Unternehmens zu berücksichtigen.

## 4.3 Kontrolle

Der Umgang mit sicherheitsrelevanten Ressourcen ist so zu gestalten, dass Verstöße gegen die Sicherheitsziele und ihre Verursacher feststellbar und zuordenbar sind (Grundsatz der Nachvollziehbarkeit und Revisionsfähigkeit). Dabei ist sicherzustellen, dass diese Maßnahmen der Informationssicherheit im Einklang mit gesetzlichen und arbeitsrechtlichen Vorschriften erfolgen und ein Missbrauch dieser Maßnahmen für andere Zwecke, insbesondere solche, welche die Menschenwürde verletzen, ausgeschlossen wird.

Verstöße gegen die Informationssicherheitsziele sind insbesondere:

- die unautorisierte Preisgabe von Geschäfts- und Betriebsgeheimnissen,
- die Abfrage von Daten für nicht dienstliche Zwecke,
- die ungesicherte Verwahrung von Daten,
- die unautorisierte Weitergabe von Daten,
- die Verfälschung von Daten,
- die unautorisierte Veränderung sicherheitsrelevanter Ressourcen,
- die tatsächliche oder potenzielle finanzielle Schädigung des Unternehmens durch Nichterfüllung von Sicherheitsmaßnahmen und
- die tatsächliche oder potenzielle Beeinträchtigung/Schädigung der Sicherheit von Mutterunternehmen und Vertragspartnern durch Nichterfüllung von Sicherheitsmaßnahmen.

# 5 Gesetzliche und normative Rahmenbedingungen

Folgende Gesetze und Verordnungen in der jeweils geltenden Fassung beeinflussen die Information Security Policy:

| | |
|---|---|
| Datenschutzgesetz (DSG 2000) | Schutz von personenbezogenen Daten |
| Standard- und Musterverordnung zum Datenschutzgesetz | Vom Unternehmen genutzte Standardverarbeitungen |
| Urheberrechtsgesetz | Schutz von geistigem Eigentum, Software-Lizenzen |
| Strafgesetzbuch §§ 118-124, § 126a, § 148a | Strafbestimmungen für Verletzung der Verschwiegenheit, Computerkriminalität und Datenmissbrauch |
| Signaturgesetz (SigG) | Verwendung elektronischer Signaturen |
| Signaturverordnung | Verwendung elektronsicher Signaturen |
| Verbandsverantwortlichkeitsgesetz (VbVG), BGBl. 151/2005 | Verpflichtet zu klaren Regelungen, auch im Bereich Datenschutz |
| Electronic Commerce Gesetz (ECG) | Elektronische Geschäftsabwicklung |
| E-Government-Gesetz (E-GovG) | Kundenservices über das Internet, Umsetzung der Amtssignatur |
| Bundes-Vergabegesetz 2006 | Vertrauliche Behandlung von Bieter-Informationen |
| Telekommunikationsgesetz 2003 (TKG 2003) | Förderung des Wettbewerbes im Bereich der elektronischen Kommunikation |
| Informationssicherheitsgesetz (InfoSiG) | Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen |
| Bundesabgabenordnung (BAO), BGBL. 14/2013 | Angelegenheiten der öffentlichen Abgaben |
| Gesetz über Gesellschaften mit beschränkter Haftung 1906 (GmbH-Gesetz) | Allgemeine Rechtsvorschrift |
| Bundesgesetz über besondere zivilrechtliche Vorschriften für Unternehmen 1987 (UGB) | Allgemeine Rechtsvorschrift |
| Unternehmensrecht-Änderungsgesetz | Änderung des GmbH-Gesetzes |

| | |
|---|---|
| 2008 (URÄG) | |
| Arbeitsverfassungsgesetz | Einschaurechte / Mitwirkungsrechte des Betriebsrates |
| Arbeitnehmerschutzgesetze | Schutz der Arbeitnehmer |
| Zustellgesetz (ZustG) | Zustellung behördlicher Dokumente |
| ISO27000ff | Normenreihe für Informationssicherheits-Managementsysteme, Quelle: Austrian Standards Institute (ASI) vormals ÖNORM |
| GrundschutzBSI | Empfehlungen des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI), Quelle: www.bsi.bund.de |
| ÖstSiHandbuch | österr. Informationssicherheitshandbuch, Quelle: www.sicherheitshandbuch.gv.at |

# 6 Gültigkeitsbereich

Dieses Dokument in der Version <Versionsnummer> ist ab dem <Datum> verbindlich und integraler Bestandteil der Allgemeinen Geschäftsbedingungen.

Dieses Dokument ist in der jeweils aktuellen Version auf der Homepage <URL> für alle interessierten Parteien verfügbar.

Dieses Dokument ist in der jeweils aktuellen Version Bestandteil jeder Einladung zur Angebotslegung.

Zusätzlich werden folgende Dokumente außer Kraft gesetzt:

- Alle früheren Versionen