Vorwort Organisationsrichtlinie ”IT-Sicherheit”

Diese Richtlinie regelt die besonderen Sicherheitsbedürfnisse und -anforderungen des Unternehmens sowie die Umsetzung beim Betrieb von IT-gestützten Verfahren bzw. den beim Unternehmen eingesetzten IT-Systemen.

Die hier vorliegende Organisationsrichtlinie ”IT-Sicherheit” ist Bestandteil des Risikomanagements des Unternehmens.

Sie verfolgt dabei diese Ziele:

- Festlegung des erforderlichen Sicherheitsniveaus der IT-Systeme des Unternehmens
- Definition der sich daraus abgeleitenden Schutzziele und Schutzmaßnahmen
- Ableitung des daraus resultierenden Handlungsbedarfs für die unterschiedlichen Rollen im IT-Sicherheitskreislauf
- Definition von einheitlichen und nachvollziehbaren Prüfkriterien beim Betrieb von IT-Systemen innerhalb des Unternehmens
- Beitrag zur Vereinheitlichung des Risikomanagements im Konzern bezüglich der Beurteilung des IT-Betriebsrisikos
- Förderung des IT-Sicherheitsbewusstseins im Unternehmens
- Bestandteil der umfassenden Dokumentation des Risikomanagements Konzern für interne und externe Stellen (Wirtschaftsprüfer, BAKred, Ratingagenturen) insbesondere im Zusammenhang mit KonTraG und "Basel II"

Die Geschäftsführung hat in seiner Sitzung am [Datum] beschlossen, als Basis für die Implementierung des IT-Sicherheitskreislaufs eine IT-Sicherheitsrichtlinie (IT-Security Policy) erstellen zu lassen, welche die bisherigen Regelungen einzelner Bereiche des Unternehmens zum sicheren Betrieb von IT-Verfahren und IT-Systemen zusammenfasst und vereinheitlicht.

Weiterhin bleiben für den IT-Bereich die Vorgaben aus dem Grundschutzhandbuch (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) immer dann verbindlich, sofern keine unternehmens-spezifischen Regelungen für das zu betrachtende IT-Verfahren existieren.

IT-Sicherheitsrichtlinie

IT-Sicherheitsleitlinien (Nr. 1 - 6)

1. Schutzziele

Alle sensiblen Informationen, Daten, IT-Systeme und IT-Ressourcen sind gemäss ihrem definierten Schutzniveau so geschützt, dass nur

- erlaubte Zugriffe und erlaubte Veröffentlichungen (Schutzziel: Vertraulichkeit),
- erlaubte Änderungen (Schutzziel: Integrität) und
- erlaubte Löschungen bzw. Unterbrechungen (Schutzziel: Verfügbarkeit) möglich sind.

Außerdem werden bei geschäftskritischen Verfahren alle sicherheitsrelevanten Vorgänge im erforderlichen Umfang protokolliert und ausgewertet (Schutzziel: Nachvollziehbarkeit).

2. Angemessenheit

Jeder Informationseigentümer - bzw. jeder von diesem Beauftragte - sorgt dafür, dass bei allen Maßnahmen zum Schutz von sensiblen Informationen, Daten, IT-Systemen und IT-Ressourcen das Wirtschaftlichkeitsprinzip angewendet wird.
Dabei sind die Auswirkungen auf das Betriebsrisiko, d.h. den IT-Betriebskreislauf einerseits und dem IT-Sicherheitskreislauf andererseits (z.B. unerlaubte Zugriffe, unerlaubte Veröffentlichung, unerlaubte Änderung oder Zerstörung von sensiblen Informationen, Daten, IT-Systeme und IT-Ressourcen) zu bewerten.
Der Aufwand zum Schutz der Informationen steht in einem wirtschaftlich vertretbaren Verhältnis zum Wert der Information für das Unternehmen.

3. Zugriffsregelung

Jeder Zugriff auf sensible Informationen, Daten, IT-Systeme und IT-Ressourcen des Unternehmens wird genehmigt, kontrolliert und protokolliert.
Der Zugriff begründet sich ausschließlich aus den betrieblichen Erfordernissen der jeweiligen Funktion innerhalb des Unternehmens.
Die Beantragung und Vergabe von Benutzerkennungen erfolgt über eine zentrale Berechtigungsverwaltung und wird in einer eigenen Richtlinie beschrieben.

4. Akzeptanz und Verpflichtung

Alle natürlichen Personen, die Zugriff auf Informationen, Daten, IT-Systeme und IT-Ressourcen des Unternehmens erhalten sollen, akzeptieren formal die Notwendigkeit, die Informationen, Daten, IT-Systeme und IT- Ressourcen des Unternehmens zu schützen.
Alle MitarbeiterInnen, Auftragnehmer und andere Dritte sind individuell verpflichtet, diese Anforderung im Rahmen ihrer jeweiligen Funktion aktiv zu unterstützen.

5. Sensibilisierung

Die Führungskräfte des Unternehmens schaffen die erforderlichen Rahmenbedingungen, damit alle betroffenen MitarbeiterInnen, Auftragnehmer und andere Dritte die IT-Sicherheitsrichtlinie des Unternehmens kennen, verstehen und befolgen.

6. Gesetze und Auflagen

Die Maßnahmen zum Schutz von sensiblen Informationen, Daten, IT-Systemen und IT-Ressourcen entsprechen den jeweils gültigen gesetzlichen Auflagen und Verordnungen.

IT-Sicherheitsvorgaben (Nr. 10 - 29)

10. Umgang mit vertraulichen Informationen

Vertrauliche Informationen, Daten und IT-Ressourcen werden so erfasst, verarbeitet und gespeichert, dass ein unerlaubter Zugriff oder Missbrauch ausgeschlossen ist.
Die Erfassung, Verarbeitung und Speicherung von personenbezogenen Daten werden im Unternehmens in einer eigenen Richtlinie geregelt.

11. Integrität der Geschäftsdaten

Die Integrität der zu verarbeitenden, geschäftskritischen Daten und Informationen ist durch geeignete technische und organisatorische Maßnahmen während der

- Verarbeitung,
- Speicherung und
- Übertragung

zu gewährleisten.

Dies ist z.B. dann der Fall, wenn nach Abschluss eines Verarbeitungsschrittes die Daten zu einem Dritten übertragen, an ein anderes Verfahren übergeben oder auf ein anderes Medium gespeichert werden (z.B.: Backup/Archivierung).
Die Prüfung der fachlichen Korrektheit und Zulässigkeit der

- Dateneingabe,
- Verarbeitung dieser Informationen und
- der daraus resultierenden Ergebnisse

sind in den jeweiligen Verfahrensbeschreibungen festgelegt und nicht Bestandteil dieser Organisationsrichtline.

12. Verantwortung des Informationseigentümers

Jede Information, jede Datei, jedes Verfahren, jedes IT-System und jede IT-Ressource hat einen eindeutig zugeordneten Informationseigentümer.
Dieser ist für die Einstufung des Schutzbedarfs und die Vergabe der Zugriffsberechtigungen verantwortlich.

13. Zugriff entsprechend der Funktion

Für die Vergabe von Zugriffsrechten gibt es unternehmensweit einheitliche Regelungen.
Der Zugriff auf sensible Informationen, Daten, IT-Systeme und IT-Ressourcen wird entsprechend der jeweiligen Funktion innerhalb des Unternehmens vergeben.

14. Unterweisung und Sensibilisierung

Das erforderliche Wissen zur Anwendung der IT-Sicherheitsrichtlinie im Unternehmen wird den verschiedenen Zielgruppen (Nutzer, Betreuer, Führungskräfte usw.) in Art und Umfang angemessen zur Verfügung gestellt.
Alle MitarbeiterInnen, Auftragnehmer und andere Dritte, die Zugriff auf sensible Informationen, Daten, IT-Systeme und IT-Ressourcen des Unternehmens haben, sind darüber informiert, wie sie IT-Sicherheitsvorfälle erkennen und diese entsprechend eskalieren.

15. Integrität des IT-Betriebs- und IT-Sicherheitskreislaufs

Alle relevanten Teile des IT-Betriebskreislaufs und des IT-Sicherheitskreislaufs im Unternehmen werden nach einem geregelten und prüfbaren Verfahren entwickelt oder beschafft, getestet, eingeführt, betrieben, geändert und abgebaut.

16. Erkennen von IT-Sicherheitsverletzungen

Für alle geschäftskritischen Informationen, Daten, Verfahren, IT-Systeme und IT-Ressourcen im Unternehmen sind Mechanismen und Prozesse implementiert, die unberechtigten Zugriffe bzw. unberechtigte Zugriffsversuche zeitnah erkennen.

17. Urheberschaft

Es werden bei den Verfahren und IT-Systemen des Unternehmens nur solche Authentifizierungsmethoden eingesetzt, die eine juristisch eindeutige Zuordnung zu einer Person oder zu einem Dienst gewährleisten.

18. Anmelde-/Abmeldeprozess

Vor und nach dem erfolgreichen Zugriff auf sensible Informationen, Daten, Verfahren, IT-Systeme und IT-Ressourcen wird jeweils ein standardisierter Anmelde- und Abmeldeprozess durchlaufen.

19. Netzwerksicherheit

Für jedes - als vertrauenswürdig eingestuftes - Netzwerksegment des Unternehmens sind Sicherheitsmechanismen implementiert, die den Zugriff in und von nichtvertrauenswürdigen Netzwerksegmenten überwachen und/oder verhindern.

20. Virenschutz

"Schädliche/schadhafte" Softwarekomponenten (z.B. Viren) werden auf den IT-Systemen des Unternehmens erkannt und unverzüglich entfernt.

21. Protokollierung

Alle IT-sicherheitsrelevanten Vorgänge werden protokolliert.

22. Integrität der Protokolldateien

Alle Protokolldateien, die IT-sicherheitsrelevante Vorgänge enthalten, werden so erstellt, im laufenden Betrieb gepflegt und gespeichert, dass unerlaubte Zugriffe, Veränderungen, Löschungen oder Zerstörungen verhindert werden.

23. Reaktion auf IT-Sicherheitsvorfälle

Alle Vorfälle, die Auswirkungen auf die Schutzziele der IT-Sicherheitsrichtlinie haben, werden dokumentiert, berichtet und in angemessener Art und Weise behandelt.

24. Schwachstellen

Alle geschäftskritischen Verfahren, IT-Systeme und IT-Ressourcen werden regelmäßig auf Sicherheitsschwachstellen untersucht.

25. Einhaltung der IT- Sicherheitsrichtlinie

Alle Vorgaben der IT-Sicherheitsrichtlinie werden regelmäßig überprüft, um sicherzustellen, dass diese - wie vorgesehen - funktionieren und zum Zeitpunkt der Prüfung noch ausreichend

sind, um die aktuellen Anforderungen zum Schutz der betroffenen sensiblen Informationen, Daten, IT-Systeme und IT-Ressourcen zu erfüllen.

26. IT-Sicherheitsberichtswesen

Die automatisiert erstellten Protokolle der IT-sicherheitsrelevanten Vorgänge werden regelmäßig und bei Verdacht bzw. einem erkannten Sicherheitsvorfall ausgewertet. Die Ergebnisse der Auswertung werden im Rahmen eines definierten und abgestimmten Prozesses intern berichtet.
Alle anderen IT-sicherheitsrelevanten Vorfälle, werden manuell erfasst, dokumentiert, kontrolliert und ausgewertet und im Rahmen eines definierten und abgestimmten Prozesses intern berichtet.

27. Notfallplanung

Für die geschäftskritischen IT-Systeme und Verfahren des Unternehmens sind die erforderlichen Vorkehrungen getroffen, um das IT-Betriebsrisiko zu minimieren.

28. Ausnahmen

Aufgrund technischer oder organisatorischer Gegebenheiten gibt es bei den IT-Systemen und Verfahren des Unternehmens Ausnahmen zu den IT-Sicherheits-vorgaben und IT-Sicherheitsumsetzungsanforderungen.
Diese Ausnahmen werden in einem geregelten Prozess entschieden und genehmigt, dokumentiert und nachverfolgt.

29. IT-Sicherheitsumsetzungsanforderungen

Die weitere Detailierung der IT-Sicherheitsvorgaben findet in den IT-Sicherheitsumsetzungsanforderungen statt.

Prozessbeschreibung "Ausnahmen"

Diese Verfahrensbeschreibung regelt die in der IT-Sicherheitsvorgabe "Ausnahmen" genannten Sachverhalte im Unternehmen.

Gegenstand dieser Verfahrensbeschreibung sind:
1. Ausnahmen zu der IT-Sicherheitsrichtlinie
2. Beantragung von Ausnahmen
3. Gültigkeit und Dokumentation der Ausnahmeanträge
4. Ablehnung von Ausnahmeanträgen

1. Ausnahmen zu der IT-Sicherheitsrichtlinie

(1.1) In begründeten Fällen können die in (2.1) genannten Verantwortlichen für Verfahren und IT-Systeme entsprechende Ausnahmegenehmigungen für die Umsetzung der IT-Sicherheitsvorgaben und IT-Sicherheitsumsetzungsanforderungen der IT-Sicherheitsrichtlinie beantragen, falls folgende Punkte zutreffen:
- Die Erfüllung der IT-Sicherheitsvorgaben steht im Widerspruch zu dem in der IT-Sicherheitsleitlinie "Angemessenheit" genannten Wirtschaftlichkeitsprinzip.
- Die Erfüllung der IT-Sicherheitsvorgaben verhindert oder beeinträchtigt erforderliche Geschäftsprozesse in einem nicht vertretbaren Rahmen.
- Die Erfüllung der IT-Sicherheitsvorgaben ist aus rechtlichen, organisatorischen oder technischen Gegebenheiten nicht möglich.

(1.2) Zu den IT-Sicherheitsleitlinien sind generell keine Ausnahmeregelungen vorgesehen.

2. Beantragung von Ausnahmen

(2.1) Der Ausnahmeantrag kann von den
- Projektverantwortlichen für das jeweilige Projekt oder
- Führungskräften für den jeweiligen Verantwortungsbereich gestellt werden.

(2.2) Ausnahmeanträge sind von den in (2.1) genannten MitarbeiterInnen schriftlich oder per Email an das IT-Sicherheitsmanagement (IT-SM) zu stellen (Formblatt siehe Anlage).
Dabei sind zwingend folgende Angaben zu machen:
- Autor bzw. Ansprechpartner und Funktionsbeschreibung
- Angaben über den betroffenen Bereich/Verfahren
- Verantwortliche Führungskraft des betroffenen Bereichs
- Beschreibung der beantragten Ausnahme unter Nennung der betroffenen IT-Sicherheitsvorgaben oder IT-Sicherheitsumsetzungsanforderungen.
- Begründung, warum diese Ausnahme erforderlich ist, z.B.: Angaben über erforderliche Maßnahmen, um die Vorgaben der IT-Sicherheitsrichtlinie zu erfüllen
- Angaben über die erforderliche zeitliche Dauer der Ausnahme
- Auswirkungen für das Unternehmen bei Nichtgenehmigung der Ausnahme.

(2.3) Bestandteil des Ausnahmeantrags ist in jedem Fall eine Risikoanalyse gemäß den Vorgaben des Risikocontrollings im Unternehmen.

(2.4) Sollten keine Vorgaben des Risikocontrollings vorliegen, gibt das IT-Sicherheitsmanagent übergangsweise entsprechende Kriterien vor.

(2.5) Eine Ausnahme darf nur beantragt und genehmigt werden, wenn das sich daraus ergebende Risiko für das Unternehmen als tragbar eingestuft wird.

(2.6) Pro Verfahren können mehrere Ausnahmen in einem Antrag zusammengefasst werden.

3. Gültigkeit und Dokumentation der Ausnahmeanträge

(3.1) Das IT-Sicherheitsmanagent wird den Ausnahmeantrag unverzüglich prüfen und einen entsprechenden schriftlichen Entscheid erstellen. Dieser enthält eine entsprechende fachliche Stellungnahme.

(3.2) Bei einer positiven Entscheidung ist die Ausnahme zeitlich befristet (maximal 12 Monate). Im Bedarfsfall kann eine verkürzte Prüffrist vereinbart werden; die Fristen werden bei der Prüfung durch das IT-Sicherheitsmanagent festgelegt.
Der Entscheid enthält deshalb konkrete Angaben zu der

- definierten Gültigkeitsdauer der Ausnahmegenehmigung und der
- jeweils festgesetzten Überprüfungsfrist.

(3.3) Das IT-Sicherheitsmanagent ist für die Erfassung und die zentrale Ablage aller Ausnahmeanträge, Ausnahmegenehmigungen und Ablehnungen zum Zwecke der

- Dokumentation innerhalb des IT-Sicherheitsberichtswesens
- Überprüfung der Gültigkeit
- Überprüfung der Prüffristen

verantwortlich.

4. Ablehnung von Ausnahmeanträgen

(4.1) Bei einer negativen Entscheidung hat der Antragsteller die Möglichkeit, bei Vorliegen neuer Erkenntnisse oder Informationen, jederzeit einen erneuten Antrag zur Erteilung einer Ausnahmegenehmigung zu stellen, um die Entscheidung durch das IT-Sicherheitsmanagent nochmals überprüfen zu lassen.

(4.2) In jedem Fall steht dem Antragsteller der interne Eskalationsweg innerhalb des Unternehmens frei.