Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheitsrichtlinie zur IT-Nutzung

- Beispiel -

Stand: Juni 2004

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

INHALTSVERZEICHNIS

1 Einleitung

In der Sicherheitsleitlinie wird die Bedeutung von IT-Sicherheit für unsere Institution dargelegt und die grundsätzliche IT-Sicherheitsstrategie beschrieben. Die "Sicherheitsrichtlinie zur IT-Nutzung" leitet aus den Vorgaben der Sicherheitsleitlinie konkrete organisatorische und technische Anforderungen, die unabhängig von konkreten Produkten für alle Projekte und Prozesse gelten, ab. Diese Anforderungen sind die Grundlage für IT-Sicherheitsmaßnahmen und legen das angestrebte Sicherheitsniveau fest.

Diese Sicherheitsrichtlinie basiert auf dem IT-Grundschutzhandbuch des BSI. In der rechten Spalte befinden sich Verweise zu Hintergrundinformationen und zu Maßnahmenvorschlägen innerhalb des IT-Grundschutzhandbuchs.

M x.xx

Hinweis:

Bemerkungen und Hinweise, an welchen Stellen sich eine individuelle Anpassung oder Ergänzung der Musterrichtlinie besonders empfiehlt, sowie Kommentare sind gelb hinterlegt.

2 Geltungsbereich

Diese Richtlinie gilt verbindlich für alle Mitarbeiter ohne Ausnahme für die Nutzung dienstlicher IT. Verstöße gegen die Inhalte der Richtlinie können

zu arbeitsrechtlichen Konsequenzen führen.

Auch beim Abschluss von Verträgen mit externen Dienstleistern ist darauf zu achten, dass die Vorgaben dieser Richtlinie beachtet werden.

Für Anforderungen an Outsourcing-Verträge ist eine entsprechenden Sicherheitsrichtlinie (siehe Musterdokument vom BSI) zu verfassen.

Für die Pflege und Weiterentwicklung der Richtlinie ist der IT-Sicherheitsbeauftragte zuständig.

3 Umgang mit Informationen

Für Geschäftsprozesse, Informationen, Anwendungen und IT-Systeme werden Verantwortliche („Eigentümer") festgelegt. M 2.225

Alle Informationen müssen anhand ihres Schutzbedarfs klassifiziert werden. M 2.217
Die Schutzbedarfskategorien werden vom IT-Sicherheitsbeauftragten zusammen mit den Abteilungsleitern definiert und von der Leitung verabschiedet.

Ziel ist es, Informationen entsprechend ihres Schutzbedarfs zu verarbeiten. Nur wenn IT-Benutzer und Verantwortliche wissen, welche Informationen besonders schutzbedürftig sind, können sie diese auch angemessen schützen. Aus dem Schutzbedarf der Informationen leitet sich letztendlich der Schutzbedarf der IT-Systeme ab, auf denen die Informationen verarbeitet werden.

Die Verantwortlichen legen fest, wer unter welchen Bedingungen auf Informationen zugreifen bzw. Anwendungen und IT-Systeme nutzen darf.

4 Rechtsvorschriften

Beim Einsatz der IT sind einschlägige Gesetze, Vorschriften und (interne) Regelungen einzuhalten. M 2.40, M 3.2

Beispiele: Datenschutz, Urhebergesetze, Arbeitnehmervertretungsregelungen, Brandschutzvorschriften, Organisationsanweisungen oder Verträge mit Kunden.

5 Organisation

5.1 Stellen

Die organisationsweiten IT-Dienste sind durch die bestellten Administratoren zu administrieren und zu warten.

Der IT-Sicherheitsbeauftragte ist zur Erreichung der IT-Sicherheitsziele in alle IT-Projekte frühzeitig einzubeziehen. Wenn Projektziele den Sicherheitsanforderungen entgegenstehen, obliegt der Leitung die Entscheidung, welche Anforderungen eine höhere Priorität haben. M 2.193

Um Sicherheitslücken zu schließen, haben sich der IT-Sicherheitsbeauftragte und die Administratoren regelmäßig zu informieren. M 2.35

Der IT-Sicherheitsbeauftragte und die Administratoren unterstützen und beraten die IT-Benutzer. M 2.12

Neue Mitarbeiter und Mitarbeiter, die in eine vertrauensvollere Position wechseln, sind auf ihre Vertrauenswürdigkeit und Qualifikation zu überprüfen. M 3.33

5.2 Schulung und Sensibilisierung

IT-Benutzer und Administratoren sind vor der erstmaligen Nutzung der jeweiligen IT-Dienste zu schulen. Schulungsinhalte sind: M 3.11, M 3.26

- Handhabung der jeweilig verwendeten IT-Dienste M 2.12, M 3.4

- Inhalte der Sicherheitsleitlinie und der Sicherheitsrichtlinien zu verschiedenen Themen (Notfallvorsorge, Datensicherung etc.) sowie die umzusetzenden Sicherheitsmaßnahmen — M 3.5
- Sensibilisierungsmaßnahmen („Warum ist IT-Sicherheit so wichtig für mich und meinen Arbeitgeber?“) — M 2.198
- rechtliche Rahmenbedingungen — M 3.2

Wesentliche Inhalte des IT-Sicherheitskonzeptes und Verhaltensregeln sind für IT-Benutzer und Administratoren zielgruppengerecht in entsprechenden Sicherheitsrichtlinien zusammenzufassen.

5.3 Vertretungsregeln

Für den Fall der Abwesenheit (Dienstreise, Urlaub, Krankheit) sind Vertreter zu benennen, die vom Stelleninhaber einzuweisen und zu informieren sind. — M 2.26

6 Verwaltung und Nutzung von IT-Diensten

Hinweis: Besonders dieses Kapitel ist an individuelle Prozesse und Organisationsstrukturen anzupassen.

6.1 Beschaffung

Für die Beschaffung von Soft- und Hardware ist als Grundlage ein Anforderungsprofil zu erstellen, das neben fachlichen und technischen Ausstattungsmerkmalen sowie ergonomischen Aspekten auch Anforderungen an die IT-Sicherheit beschreibt. Nach Möglichkeit sollten Arbeitsplätze standardisiert ausgestattet werden, um Verwaltung und Administration zu erleichtern. — M 2.80, M 3.9, M 2.69

Es ist zu beachten, dass die Integration in die vorhandene oder geplante, informationstechnische Infrastruktur gewährleistet ist. Es sind die für den jeweiligen Bereich geltenden Normen (ISO, DIN) zu berücksichtigen. — M 2.66, M 2.80

Es sind im Rahmen der Kommunikation und Archivierung bevorzugt Programme zu beschaffen, die eine Verschlüsselung ermöglichen.

6.2 Einsatz

Vor dem Einsatz ist neue Soft- und Hardware zu testen. Dabei sollten nach Möglichkeit Testsystem und Produktivbetrieb getrennt werden. — M 4.65

Es sind Test- und Freigabeverfahren innerhalb der IT-Abteilung und zwischen der IT-Abteilung und den Fachbereichen abzusprechen zu beachten. Nicht freigegebene Hard- und Software ist nicht einzusetzen. — M 2.62, M 2.216, M 2.9

Softwareänderungen machen eine erneute Freigabe erforderlich. — M 2.62

Die IT-Dienste sind nur für die festgelegten Aufgaben zu nutzen. Die Nutzung für private Zwecke ist nicht zulässig. Der Anschluss privater Hardware an dienstliche IT-Systeme und die Nutzung privater Software zu dienstlichen Zwecken ist nur mit Genehmigung durch den IT-Sicherheitsbeauftragten zulässig. — M 2.9

Die Nutzung aller nicht ausdrücklich erlaubten Dienste ist technisch zu unterdrücken. Dienste und Berechtigungen, die nicht oder nicht mehr benötigt werden, sind durch den Administrator zu deaktivieren. — M 4.12, M 4.17

Soft- und Hardware sind durch die Administratoren möglichst so zu konfigurieren, dass ohne weiteres Zutun der IT-Benutzer optimale Sicherheit erreicht werden kann. Default-Einstellungen sind zu überprüfen und Default-Passwörter zu ändern. — M 2.87, M 4.30, M 4.79, M 2.11

Es sind angemessene Sicherheitsprodukte einzusetzen. — M 4.41

6.3 Wartung

Die mit Pflege und Wartung verbundenen Maßnahmen sind nach Art, Inhalt und Zeitpunkt zu protokollieren. M 2.4, M 4.106

Der Zugriff auf Daten durch Wartungstechniker ist soweit wie möglich zu vermeiden. Die eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen. Bei Arbeiten an organisationsweiten IT-Diensten mit sensiblen Informationen ist das Vier-Augen-Prinzip anzuwenden. M 2.220, M 4.16, M 4.17

Arbeiten am System sind gegenüber den betroffenen Mitarbeitern rechtzeitig anzukündigen. M 2.4

Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten IT-Systeme zu überprüfen. M 2.62

6.4 Revision

Alle Maßnahmen an IT-Diensten sind revisionssicher zu dokumentieren. Administratortätigkeiten sind zu protokollieren. M 2.25, M 2.201, M 2.4

Es ist eine regelmäßige Kontrolle der Funktionalität der IT-Dienste, der IT-Sicherheit und der Einhaltung der Richtlinien durchzuführen. M 2.182

Es sind sicherheitsrelevante Ereignisse und Zugriffe auf kritische Bereiche automatisch zu protokollieren und durch Administratoren regelmäßig zu überprüfen. M 4.47, M 4.106, M 4.123, M 4.167

Bei der Protokollierung sind Datenschutzaspekte zu beachten. Ermöglicht die Auswertung der Daten eine Verhaltens- und Leistungskontrolle, ist sie mitbestimmungspflichtig. M 2.110

6.5 Weitergaberegelungen

Bei der Weitergabe von Informationen ist ihr Schutzbedarf zu beachten und eine geeignete Versandart zu wählen. Vertrauliche Informationen oder Datenträger (Diskette, CD-ROM etc.) mit vertraulichen Informationen dürfen erst dann versendet werden, wenn die Vertraulichkeit beim Versand gewährleistet ist. Der Empfänger der Informationen ist zur vertraulichen Behandlung zu verpflichten. M 2.42, M 5.23

Wird Hardware außer Haus gegeben, sind – sofern möglich – alle vertraulichen Informationen, die sich in Datenspeichern befinden, vorher sicher zu löschen. Ist dies nicht möglich, so ist der Vertragspartner auf Geheimhaltung zu verpflichten. Die Übergabe bzw. der Transport ist sicher zu gestalten. M 2.218, M 2.167, M 1.36, M 2.44

6.6 Entsorgung

Belege und Druckausgaben, die vertrauliche Informationen beinhalten, müssen getrennt vom übrigen Abfall entsorgt werden. M 2.13

Elektronische Datenträger mit vertraulichen Informationen, die nicht weiter benötigt werden, sind vor der Entsorgung sicher zu löschen. M 2.167

Sofern keine sichere Entsorgung durchgeführt werden kann, ist mit der Entsorgung ein externes Unternehmen zu beauftragen. M 2.13

7 Sicherheitsmaßnahmen

7.1 Allgemeines

Durch wirksame Maßnahmen ist zu gewährleisten, dass die Sicherungsziele M 4.30, M 4.42

realisiert werden und ihre Einhaltung kontrolliert werden können. M 2.182, M 2.199

Alle IT-Systeme und Anwendungen sind sorgfältig zu konfigurieren und zu sichern. Wesentliche Punkte sind nachvollziehbar zu dokumentieren. M 1.37f, M 5.32

Die Gebäude und Räume sind gegen fahrlässig, vorsätzlich oder durch höhere Gewalt herbeigeführte Störungen zu schützen (z. B. Brandschutz). M 1.8 , M 1.48

Für Tele(heim)arbeit und mobile Arbeit sind Regelungen zu erstellen. M 2.213

7.2 Zutritts- und Zugangsregelungen

Der Zutritt zu den Räumlichkeiten bzw. der Zugang zu den IT-Diensten ist gegen Unbefugte zu schützen und zu kontrollieren. Hierbei sind verschiedene Rollen festzulegen. M 1.17, M 2.6, M 2.7, M 4.2

Für jeden Mitarbeiter sind Berechtigungen für den Zutritt zu Räumlichkeiten, den Zugang zu IT-Diensten und den Zugriff auf Informationen festzulegen. Alle Rechte sind restriktiv zu vergeben und zu dokumentieren. Hierbei sind die zwingenden dienstlichen Erfordernisse zugrunde zu legen. M 2.220, M 2.30 M 2.8, M 2.31 M 4.16, M 4.17

Die Authentisierung der Zugangsberechtigung ist durch Passwörter sicherzustellen. Es sind Passwortregeln zu erstellen. Diese werden allen Betroffenen durch *Sicherheitshinweise für Benutzer* mitgeteilt. M 4.1 M 2.11

Der Zugang der Administratoren ist speziell zu sichern. Die Passwörter der Administratoren sind sicher zu verwahren. Den Stellvertretern ist eine eigene Administratoren-Kennung zuzuteilen. M 4.21 M 2.22, M 4.21

Besucher, Handwerker und andere fremde Personen dürfen sich nicht frei und unkontrolliert im Gebäude bewegen.

Bereiche, in denen hoch vertrauliche Informationen verarbeitet werden, sind besonders zu sichern. Nur berechtigte, namentlich benannte Personen haben Zutritt zu diesen Bereichen.

IT-Systeme im Eingangs- und Empfangsbereich sind so zu sichern, dass Unbefugte keinen unbeobachteten Zugriff nehmen und Informationen nicht eingesehen werden können.

7.3 Verschlüsselung

Vertrauliche und andere sicherheitsrelevante Daten sind verschlüsselt zu speichern. Sofern im Klartext gespeichert wird, ist beim Netzzugriff die Übertragung zu verschlüsseln. M 4.72

Zur Verschlüsselung ist IT-Benutzern auf Antrag ein Programm zur Verfügung zu stellen. Berechtigten IT-Benutzern sind ein öffentlicher und ein geheimer Schlüssel zur Verfügung zu stellen. M 2.46, M 2.164, M 5.36, M 5.63, M 5.68

7.4 Schadsoftware

Es ist ein Viren-Schutzprogramm zu installieren. Es sind regelmäßig Updates durchzuführen und die Viren-Signaturen zu aktualisieren. M 4.3, M 2.159

Hinweis: Für mittlere und größere Unternehmen und Behörden:

Es ist ein Virenschutzkonzept zu erstellen. M 2.154

7.5 Datensicherung/ Archivierung

Es sind regelmäßig Datensicherungen durchzuführen. Die IT-Benutzer sind dabei zu unterstützen. M 6.32

Hinweis: Für mittlere und größere Unternehmen und Behörden:

Es ist ein Datensicherungskonzept zu erstellen. M 6.33

Informationen sind einheitlich und dokumentiert aufzubewahren, so dass sie problemlos wieder aufgefunden werden können. M 6.20

Sicherungskopien sind in gesicherten Behältnissen in einem anderen Brandabschnitt aufzubewahren. Die Datenträger sind eindeutig zu kennzeichnen. M 6.20, M 2.3

Die Archivierung ist ein Teil des Dokumentenmanagement-Prozesses und dient der dauerhaften und unveränderbaren Speicherung von elektronischen Dokumenten und anderen Daten. Innerhalb eines Archivierungssystems aufbewahrte Daten sind konsistent so zu indizieren, dass sie eindeutig und schnell gefunden werden können. Die Speicherressourcen sind zu überwachen. Durch regelmäßig Funktions- und Recovery-Tests ist einem Datenverlust auf den Datenträgern entgegen zu wirken. M 2.258 M 2.257 M 4.173

Hinweis: Für mittlere und größere Unternehmen/Behörden:

Es ist ein Archivierungskonzept zu erstellen. M 2.243

7.6 Notfallvorsorge

Alle Probleme, die IT-Dienste betreffen, müssen dem IT-Sicherheitsbeauftragten und den Administratoren gemeldet werden. M 2.215

Es sind Verhaltensregeln und Handlungsanweisungen für relevante Schadensereignisse zu definieren und den Mitarbeitern mitzuteilen. M 6.60, M 6.62 M 6.23

Für mittlere und größere Unternehmen/Behörden:

Es ist ein Notfallvorsorgekonzept zu erstellen und Notfall-Übungen durchzuführen M 6.3

8 Regelungen für spezifische IT-Dienste

8.1 Kommunikationsspezifische Regelungen

Informationen, die elektronisch übermittelt werden (Fax, Telefonanlage, Internet etc.), sind zu schützen. Hierbei sind die technikspezifischen Sicherheitsprobleme zu berücksichtigen.

Für eine sichere Internet-Anbindung ist eine "Sicherheitsrichtlinie für die Internetnutzung" zu erstellen.

8.2 Fernzugriff auf das interne Netz

Generell ist der „Zugriff vor Ort“ dem „Fernzugriff“ vorzuziehen. M 2.102

Eine externe Anbindung an das interne Netz ist speziell zu regeln. Sofern möglich, ist der Fernzugriff auf ein isoliertes Netz zu beschränken. Der Fernzugriff ist sicher zu konfigurieren. M 5.87, M 2.184, M 2.187, M 2.204, M 5.33

Für besonders sensitive Bereiche ist entweder ein Fernzugriff auszuschließen oder auf Notfälle zu beschränken. Der Notfall und die Verfahrensweise während des Notfalls ist genau zu definieren.