GRUNDSÄTZE ZUR GEWÄHRLEISTUNG DER NOTWENDIGEN SICHERHEIT BEIM IT-EINSATZ IN DER BERLINER VERWALTUNG

(IT-SICHERHEITSGRUNDSÄTZE)

(beschlossen vom Senat am 11.12.07)

Senatsverwaltung für Inneres und Sport

IT-Kompetenzzentrum

1. Allgemeines

1.1 Ziel

Ziel der IT-Sicherheitsgrundsätze ist es, für die eingesetzten IT-Systeme und IT-Anwendungen einschließlich der baulichen und gebäudebezogenen Komponenten ein Sicherheitsniveau zu erreichen, das den sicheren Einsatz der Informationstechnik in der Berliner Verwaltung gewährleistet.

1.2 Regelungsgegenstand

Die IT-Sicherheitsgrundsätze regeln dazu insbesondere:

- die Verantwortlichkeiten,
- die Vorgehensmethodik,
- die Umsetzung und Qualitätskontrolle sowie
- die Anforderungen an das technische und organisatorische Instrumentarium.

1.3 Geltungsbereich

Diese Regelung bezieht sich auf den Geltungsbereich der VV IT-Steuerung.

2 Grundsätze der Sicherheitspolitik

2.1 Ausgestaltung

Die Grundsätze sind von den am IT-Einsatz Beteiligten entsprechend ihrer Verantwortung durch entsprechende IT-Sicherheitskonzepte umzusetzen und anforderungsgerecht auszugestalten.
IT-Sicherheit muss geplant, realisiert und kontrolliert werden. Folgende Schritte sind hierzu notwendig (IT-Sicherheitsprozess):

- Organisatorische Bildung eines IT-Sicherheitsmanagements mit Festlegung von Verantwortlichkeiten.
- Festlegung von grundsätzlichen Zielen für die IT-Sicherheit durch Erstellen einer IT-Sicherheitsleitlinie.
- Erarbeitung von behördlichen und verfahrensspezifischen IT-Sicherheitskonzepten.
- Ständige Überprüfung der IT-Sicherheit als fortdauernder Prozess aufgrund neuer Gefährdungen und Fortentwicklung der Informationstechnik.

2.2 Standards zur IT-Sicherheit

Die IT-Sicherheitsgrundsätze werden konkretisiert durch die Festlegung von Standards zur IT-Sicherheit. Diese werden in den „IT-Standards der Berliner Verwaltung“ gemäß den IT-Standardisierungsgrundsätzen definiert.

2.3 IT-Sicherheit und Fachaufgabe

IT-Sicherheit ist integraler Bestandteil der Fachaufgabe. Damit verbleibt, ausgehend von der fachlichen Verantwortung, die letztendliche Verantwortung für IT-Sicherheit bei der jeweiligen Behörde.

2.4 IT-Sicherheit als Prozess

Die Gewährleistung von IT-Sicherheit ist als fortlaufender Prozess zu gestalten. Der Prozess betrifft insbesondere die regelmäßige (mindestens jährliche) Überprüfung der Umsetzung und Wirksamkeit von Sicherheitsmaßnahmen und die erforderliche Fortschreibung der jeweiligen IT-Sicherheitskonzepte.

2.5 Berücksichtigung von IT-Sicherheit beim IT-Einsatz

Die Gewährleistung von Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit im jeweils erforderlichen Maße ist unabdingbare Voraussetzung und Bestandteil jedes IT-Einsatzes und für den gesamten Einsatzzeitraum auf der Basis von IT-Sicherheitskonzepten sicherzustellen.
IT-Sicherheitskonzepte und die sich daraus ableitenden Maßnahmen müssen insbesondere

- die sich aus der organisatorisch-technischen Verteiltheit des IT-Einsatzes in der Berliner Verwaltung ergebenden Anforderungen
- die durch Bedrohungen von ”außen” als auch von ”innen” entstehenden Risiken
- sowie in technischer Hinsicht die Nachhaltigkeit, Standardisierung und nachgewiesene Praxistauglichkeit von Sicherheitstechnologien

berücksichtigen.
Notwendige Maßnahmen sind auch dann zu ergreifen, wenn sie den IT-Einsatz erschweren.

2.6 Ressourcen

Benötigte Ressourcen bzw. entstehende Kosten sind in allen Phasen (insbesondere der Planungsphase) zu berücksichtigen.

2.7 Verhältnismäßigkeit

Bei der Auswahl und Realisierung von Sicherheitsmaßnahmen ist das Verhältnismäßigkeitsgebot (aufzuwendende Mittel im Verhältnis zum Grad der Sicherheitsverbesserung) zu beachten.

2.8 Tragbarkeit von Risiken

Die Tragbarkeit von Risiken ist in einer Schutzbedarfsfeststellung bzw. Risikoanalyse zu bewerten (vgl. 4.2). Die Entscheidung über die Tragbarkeit von Risiken ist zu dokumentieren. Wenn eine IT-Maßnahme nur unter Verbleib untragbarer Risiken durchführbar wäre, ist auf den IT-Einsatz zu verzichten.

2.9 Regelmäßige Kontrolle

Die Einhaltung der Sicherheitsmaßnahmen ist regelmäßig zu kontrollieren.
Bei festgestellten Verstößen sind durch die jeweils Verantwortlichen geeignete Maßnahmen zu initiieren bzw. durchzuführen, um den daraus entstehenden Risiken wirksam zu begegnen.

2.10 Nutzung der landeseinheitlichen IT-Infrastruktur und IT-Dienste

Um die notwendige Sicherheit zu gewährleisten, sind grundsätzlich die auf Basis von Landesvereinbarungen angebotenen Dienstleistungen des IT-Dienstleistungszentrum Berlin (ITDZ) zur Sicherheit der landeseinheitlichen IT-Infrastruktur und IT-Dienste zu nutzen. Für bestimmte dieser Dienstleistungen kann gemäß dem in der VV IT Steuerung festgelegten Verfahren eine Abnahmeverpflichtung festgelegt werden. Diese Dienstleistungen werden Bestandteil der IT-Standards der Berliner Verwaltung.

Für Bereiche mit besonderen Sicherheitsanforderungen (z. B. Polizei, Feuerwehr, Steuerverwaltung) sind Ausnahmen möglich.

Voraussetzungen für die Nutzung der landeseinheitlichen IT- Infrastruktur und IT-Dienste durch eine Behörde sind die Beachtung des entsprechenden IT-Sicherheitskonzeptes für diesen Dienst und ein umgesetztes behördliches IT-Sicherheitskonzept.
Kann der Nutzer die erforderliche Sicherheit nicht gewährleisten, haben das ITDZ bzw. der jeweilige IT-Dienstleister in Abstimmung mit der Senatsverwaltung für Inneres und Sport das Recht, die Nutzung zu verweigern.
Insbesondere darf eine Nutzung des Berliner Landesnetzes (BeLa) durch Einrichtungen, die nicht zum Geltungsbereich dieser Grundsätze gehören, nur unter Beachtung der für die Nutzung des BeLa relevanten Regelungen dieser Grundsätze erfolgen.

2.11 Anonymisierung/Pseudonymisierung

Werden personenbezogene Daten verarbeitet, ist genau zu prüfen, ob und in welchen Funktionen des IT-Verfahrens die Identität bzw. Identifizierbarkeit der jeweiligen Personen erforderlich ist. Verfahren, die keine Identität der Personen benötigen, sollen ausschließlich mit anonymisierten Daten arbeiten. Ist die Identifizierbarkeit der Personen für einzelne Funktionen erforderlich, soll mit pseudonymisierten Daten gearbeitet werden und in den erforderlichen Fällen die Identität der Person zugeordnet werden.

3. Verantwortlichkeiten

3.1 Rollen gemäß IT-Organisationsgrundsätzen

Die Grundlage für die Rollendefinition und das Rollenzusammenspiel bilden die VV IT-Steuerung und die IT-Organisationsgrundsätze. Die dortigen Regelungen sind grundsätzlich bei der Wahrnehmung der nachfolgend festgelegten spezifischen Verantwortlichkeiten zur IT-Sicherheit zu beachten und anzuwenden.

3.2 Produktverantwortliche

- verantworten die für die Einführung und den Betrieb eines IT-Verfahrens notwendige IT-Sicherheit,
- vereinbaren mit dem jeweiligen IT-Verfahrensverantwortlichen die Erstellung des verfahrensspezifischen Sicherheitskonzeptes und
- beauftragen ggf. im Rahmen der Bereitstellungsvereinbarung den jeweiligen Infrastrukturverantwortlichen mit infrastrukturbezogenen Sicherheitsmaßnahmen.

3.3 IT-Anwender

- haben die sie betreffenden Sicherheitsmaßnahmen konsequent und zielgerichtet umzusetzen und

- informieren entsprechend den Regelungen der jeweiligen IT-Sicherheitskonzepte über sicherheitsrelevante Ereignisse.

3.4 IT-Verfahrensverantwortliche

- planen und erstellen im Rahmen der mit dem Produktverantwortlichen getroffenen Vereinbarung das verfahrensspezifische Sicherheitskonzept,
- beziehen dabei regelmäßig den IT-Sicherheitsbeauftragten ein,
- verantworten, sofern dies im Rahmen der abgeschlossenen Vereinbarung möglich ist, die Initiierung bzw. Umsetzung der verfahrensspezifischen Sicherheitsmaßnahmen,
- beachten die im behördlichen IT-Sicherheitskonzept vorgesehenen Maßnahmen und
- initiieren die für die Sicherheit des Verfahrens erforderlichen infrastrukturbezogenen Maßnahmen.

3.5 IT-Verfahrensbetreuung

Die IT-Verfahrensbetreuung setzt im Rahmen ihrer administrativ-technischen Betreuung des IT-Verfahrens (z. B. Verwaltung der Benutzerrechte) fortlaufend diesbezügliche Sicherheitsmaßnahmen um.

3.6 IT-Management

Das IT-Management sorgt für Planung, Steuerung und Kontrolle bzgl. der Sicherheit von IT-Maßnahmen. Dies umfasst insbesondere die Initiierung und Kontrolle eines behördlichen IT-Sicherheitskonzeptes.

Das – gemäß 2.1 Ausgestaltung - zur Wahrnehmung dieser Aufgaben einzurichtende IT-Sicherheitsmanagement besteht aus einem von der Behördenleitung eingesetzten IT-Sicherheitsbeauftragten und weiteren Vertretern der relevanten Fachbereiche.
Bei der Rollenwahrnehmung ist grundsätzlich auf eine personelle Trennung zwischen IT-Sicherheitsbeauftragtem und IT-Infrastrukturanbieter zu achten.

3.7 IT-Sicherheitsbeauftragter

- begleitet die Umsetzung und Fortschreibung eines behördlichen IT-Sicherheitskonzeptes,
- organisiert die Zusammenarbeit mit anderen Bereichen der Behörde, die sicherheitsrelevante Aufgaben wahrnehmen (z. B. Brandschutzbeauftragter, Datenschutzbeauftragter usw.),
- koordiniert und kontrolliert das Zusammenspiel zwischen den verfahrensspezifischen IT-Sicherheitskonzepten und dem behördlichen IT-Sicherheitskonzept und
- moderiert, sofern eingerichtet, das IT-Sicherheitsmanagementteam. Die Einrichtung eines ständigen IT-Sicherheitsmanagementteams wird insbesondere bei großen Behörden mit vielfältigem IT-Einsatz empfohlen.

3.8 IT-Infrastrukturanbieter

IT-Infrastrukturanbieter verantworten die Umsetzung der IT-Sicherheitsmaßnahmen für die von ihnen betriebene IT-Infrastruktur. Weitere Aufgaben können ihnen im Rahmen der jeweiligen Bereitstellungsvereinbarung zugewiesen werden.

3.9 Gebäudemanagement

Das Gebäudemanagement hat dafür Sorge zu tragen, dass IT-Sicherheitsmaßnahmen entsprechend den Anforderungen der Gebäudenutzer umgesetzt werden.

3.10 IT-Dienstleister

IT-Dienstleister verantworten die Planung, Erstellung, Realisierung, Fortschreibung von IT-Sicherheitskonzepten für die von ihnen betriebenen und bereitgestellten IT-Dienstleistungen, insbesondere für das Berliner Landesnetz und sonstige landeseinheitliche IT-Infrastruktur/IT-Dienste.

Bei schwerwiegenden Gefährdungen der Sicherheit dieser IT-Dienstleistungen durch eine Behörde sind in Abstimmung mit dem IT-Kompetenzzentrum geeignete Maßnahmen zur Gewährleistung der IT-Sicherheit zu ergreifen. Die Art der Maßnahmen (insbesondere die Möglichkeit des Ausschlusses von der Nutzung der Dienstleistung), zeitliche und sachliche Abläufe und Fristen zur Umsetzung der Maßnahmen sind durch das IT-Kompetenzzentrum unter aktiver Einbeziehung der betroffenen Behörde und des IT-Dienstleisters festzulegen.

3.11 IT-Kompetenzzentrum

- verantwortet die Erstellung, Umsetzung und Kontrolle der IT-Sicherheitsgrundsätze,
- initiiert geeignete Maßnahmen, um bei festgestellten Verstößen gegen die IT-Sicherheitsgrundsätze, die behördenübergreifend zu erheblichen Risiken führen (können), die notwendige Sicherheit wieder herzustellen,
- schließt mit IT-Dienstleistern Landesvereinbarungen zur Bereitstellung von Dienstleistungen zur IT-Sicherheit ab,
- legt dem IT-Koordinierungsgremium und dem Landes IT-Ausschuss jährlich einen IT-Sicherheitsbericht zur Beratung vor und legt nach Maßgabe der Beratungsergebnisse im LIA die im IT-Sicherheitsbericht enthaltenen Maßnahmen fest (vgl. 5 Umsetzung / Berichtswesen)
- verantwortet in Abstimmung mit den IT-Dienstleistern geeignete Maßnahmen bei schwerwiegenden Gefährdungen für die Sicherheit der landeseinheitlichen IT-Infrastruktur/IT-Dienste und
- erstellt und aktualisiert ein „Modellsicherheitskonzept“ (vgl. 4 Methodisches Vorgehen)

3.12 IT-Koordinierungsgremium

Das IT-Koordinierungsgremium (ITK)

- dient der fachlichen Vorabstimmung bzgl. Fragen der IT-Sicherheit
- stimmt dazu insbesondere den jährlichen IT-Sicherheitsbericht fachlich ab
- richtet eine ständige Arbeitsgruppe ”IT-Sicherheit” ein und
- erteilt dieser AG Arbeitsaufträge und berät über die Ergebnisse.

3.13 Landes IT-Ausschuss

Der Landes IT-Ausschuss (LIA)

- berät die IT-Sicherheitsgrundsätze,
- berät den IT-Sicherheitsbericht und gibt Empfehlungen zu notwendigen Maßnahmen ab und
- gibt Empfehlungen zum Abschluss von Landesvereinbarungen mit Abnahmeverpflichtung im Bereich IT-Sicherheit

4 Methodisches Vorgehen

4.1 Sicherheitsdomänen

Als Sicherheitsdomäne wird ein logisch, organisatorisch oder räumlich zusammengehöriger Bereich mit einheitlichen Sicherheitsanforderungen bezeichnet.
IT-Sicherheitskonzepte beziehen sich immer auf eine bestimmte Sicherheitsdomäne.

4.2 IT-Grundschutz

Für alle Sicherheitsdomänen ist mindestens ein IT-Grundschutz durch Anwendung des IT-Grundschutzkatalogs (IT-GSKat) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der jeweils aktuellen Fassung zu realisieren.
Für Sicherheitsdomänen mit einem hohen bis sehr hohen Schutzbedarf oder mit sonstigen Risiken, die durch den IT-Grundschutz nicht ausreichend reduziert werden, sind i. A. ergänzende Sicherheitsmaßnahmen erforderlich. Diese sind auf Grundlage einer ergänzenden Risikoanalyse (z. B. gem. dem „IT-Sicherheitshandbuch“ des BSI oder gem. Risikoanalyse auf der Basis von IT-Grundschutz (BSI-Standard 100-3)) zu ermitteln und umzusetzen.

4.3 IT-Sicherheitskonzepte

IT-Sicherheitskonzepte müssen zu folgenden Themen Aussagen enthalten:
a) Anwendungsbereich (Behörde, Verfahren)
b) Schutzbedarfsfeststellung
c) Risikoanalyse (ab hohem Schutzbedarf)
d) Maßnahmen
e) Restrisikoanalyse (ab hohem Schutzbedarf)
f) Verantwortlichkeiten (Rechte, Pflichten, Qualitätssicherung/Kontrolle)
g) Umsetzung (Zeitplan mit Prioritäten und Fortschreibung, Kosten)

4.4 IT-Infrastruktur/IT-Dienste

Die IT-Sicherheitskonzepte für landeseinheitliche IT-Infrastruktur und IT-Dienste

- gelten für die Sicherheitsdomäne landeseinheitliche IT-Infrastruktur /IT-Dienste
- gehen generell von einem hohen Schutzbedarf der landeseinheitlichen IT-Infrastruktur /IT-Dienste aus und
- definieren auch den von den Nutzern der landeseinheitlichen IT-Infrastruktur /IT-Dienste einzuhaltenden Sicherheitsstandard..

4.5 Behördliches IT-Sicherheitskonzept

Das Behördliche IT-Sicherheitskonzept

- gilt für die Sicherheitsdomäne Behörde und
- gewährleistet auf Grundlage des IT-GSKat den IT-Grundschutz für die behördliche IT-Infrastuktur.

Die Sicherheitsdomäne Behörde kann u. U. aus mehreren Teildomänen mit unterschiedlichen Sicherheitsanforderungen bestehen. Das behördliche IT-Sicherheitskonzept muss die ggf. für diese Teildomänen erforderlichen eigenständigen IT-Sicherheitskonzepte in geeigneter und abgestimmter Weise berücksichtigen bzw. enthalten.

4.6 Modellsicherheitskonzept

Zur vereinfachten und vereinheitlichten Umsetzung des IT-GSKat für **behördenübergreifend einheitliche** Sicherheitsanforderungen erstellt und aktualisiert das IT-Kompetenzzentrum ein ”Modellsicherheitskonzept”.

4.7 Verfahrensspezifisches IT-Sicherheitskonzept

Das verfahrensspezifische IT-Sicherheitskonzept

- gilt für die Sicherheitsdomäne IT-Verfahren,
- berücksichtigt alle verfahrensspezifischen IT-Komponenten (u. a. Infrastruktur, organisatorischen und personellen Rahmenbedingungen, IT-Systeme, Kommunikationsverbindungen, Anwendungen),
- stützt sich auf den in der Behörde realisierten IT-Grundschutz ab und
- realisiert bei Bedarf zusätzliche verfahrensspezifische Sicherheitsmaßnahmen.

5 Umsetzung / Berichtswesen

5.1 IT-Sicherheitsbericht

Das IT-Kompetenzzentrum erarbeitet bis zum März des laufenden Jahres einen IT-Sicherheitsbericht zum vorher gehenden Jahr und legt diesen nach fachlicher Abstimmung im ITK dem LIA vor.
Der IT-Sicherheitsbericht enthält mindestens Aussagen zu den Punkten

- Wirksamkeit durchgeführter Sicherheitsmaßnahmen,
- Analyse neuer Risiken und
- Erforderliche Maßnahmen

5.2 Umsetzung

Umgesetzte IT-Sicherheitskonzepte sind die Voraussetzung für einen neuen bzw. wesentlich geänderten IT-Einsatz.
Bei laufendem IT-Einsatz sind entsprechende IT-Sicherheitskonzepte - falls noch nicht oder nicht entsprechend den Anforderungen dieser Grundsätze vorhanden - schrittweise in einem möglichst engen Zeitrahmen zu erarbeiten und umzusetzen.

Bei Entwicklung und Einsatz neuer Verfahren mit Partnern, die nicht zum Geltungsbereich dieser Grundsätze gehören, ist unter Berücksichtigung tatsächlicher oder rechtlicher Bedingungen auf eine weitestgehende Berücksichtigung dieser Grundsätze hinzuwirken. Bei wesentlichen Abweichungen ist das IT-Kompetenzzentrum zu beteiligen.

5.3 AG IT-Sicherheit

Das ITK richtet eine ständige Arbeitsgruppe „IT-Sicherheit“ unter der Federführung des IT-Kompetenzzentrum mit folgenden Aufgaben ein:

- Mitarbeit am jährlichen IT-Sicherheitsbericht
- Bearbeitung konkreter Aufträge des ITK zu Fragen der IT-Sicherheit
- Mitwirkung an der Fortschreibung der Standards zur IT-Sicherheit
- Regelmäßiger Informations- und Erfahrungsaustausch zu allen relevanten Fragen der IT-Sicherheit.

Weitere Aufgaben können der AG bei Bedarf zugewiesen werden.