Senatsverwaltung für Inneres

Senatsverwaltung für Inneres, Klosterstraße 47, 10179 Berlin

„IT-Standards der Berliner Verwaltung 2007“

Vorbemerkung

Gemäß den Regelungen der IT-Standardisierungsgrundsätze (Senatsbeschluss 3794/2006 vom 1.8. 2006) wurden die „IT-Standards der Berliner Verwaltung 2007“ auf Basis der eingereichten Einzelvorschläge und den von der AG IT-Standards dazu vorgelegten Voten erarbeitet. Sie wurden im ITK am 7.9. 06 zustimmend zur Kenntnis genommen. Der Landes-IT-Ausschuss hat den IT-Standards im Oktober 2006 zugestimmt. Sie sind vom IT-Staatssekretär als landeseinheitliche Grundsätze im Sinne der „Verwaltungsvorschriften für die Steuerung des IT-Einsatzes in der Berliner Verwaltung (VV IT-Steuerung)“ festgesetzt und gelten ab dem 1. Januar 2007.

1. Prozesse (Abläufe und Modellierung)

Unter Beobachtung – ITIL - IT Infrastructure Library
Gültig*: 1/07 – 12/07*

Der IT-strategische Ansatz der Berliner Verwaltung, IT als Dienstleistung bereit zustellen und zu nutzen, kann durch den Bezug auf ITIL unterstützt werden. Das weitere Vorgehen wird im Projekt ProBetrieb untersucht.

Weitere Infos: http://www.itil.org.uk/

2. Datenmodellierung/ Datenbeschreibung

Empfohlen: Entity Relationship Diagramme – Darstellung funktionaler Datenmodelle
Gültig*: 1/07 – 12/10*

Funktionale Datenmodelle für eine fachliche Grobkonzeption sollen mit Entity Relationship Diagrammen dargestellt werden.

Empfohlen: – UML Unified Modelling Language v2.x – objektorientierte Modellierung
Gültig*: 1/07 – 12/10*

Zur Modellierung von Prozessen und Daten wird UML 2.x empfohlen.

Weitere Infos: http://www.uml.org

3. Datenaustausch (zwischen Anwendungen)

Verbindlich: XML Schema Definition (XSD) v1.0,
Extensible Markup Language (XML) v1.0 – Datenbeschreibung, Datenaustausch
Gültig*:* 1/07 – 12/08

Zur strukturierten Beschreibung von Daten sind XML-Schemata gemäß den Definitionen des World Wide Web Consortium (W3C)59 mit der XML Schema Definition (XSD) zu erstellen.
XML (Extensible Markup Language) dient als der universelle und primäre Standard für den Datenaustausch aller verwaltungstechnisch relevanten Informationssysteme.

XML fungiert als allgemeine Festlegung zur Datenbeschreibung bzw. zum Datenaustausch. Sind für spezifische Anwendungen andere Festlegungen in den IT-Standards vorhanden, haben diese Vorrang vor XML.
Für den XML-basierten Austausch in konkreten Anwendungsfällen ist die weitere Konkretisierung von XML (z. B. XMeld, XJusitz,… erforderlich).

Weitere Infos unter: http://www.w3.org/XML, http://www.w3.org/XML/Schemata

Empfohlen: Extensible Stylesheet Language Transformation (XSLT) v1.0 - Datentransformation
Gültig*: 1/07 – 12/08*

Wenn Anwendungen unterschiedliche XML-Schemata verwenden, kann bei einem Datenaustausch die Konvertierung von einem Format in ein anderes Format notwendig werden.
Diese Formatkonvertierung soll über die vom W3C definierte Sprache XSLT62 als Teil von XSL (Extensible Stylesheet Language) erfolgen.

Weitere Infos: http://www.w3.org/TR/xslt

Verbindlich: Comma Separated Value (CSV) - Tabellen
Gültig*: 1/07 – 12/08*

Abgegrenzte (delimited), kommaseparierte Tabellen sind als (.csv)-Dateien zu speichern und auszutauschen.

Weitere Infos: http://www.ietf.org/rfc/rfc4180.txt

Verbindlich: „plain text"- unstrukturierte einfache Textinformationen
Gültig*: 1/07 – 12/08*

Einfacher unstrukturierter Text ist als „plain Text" (Dateityp meist „.txt") auszutauschen. Zeichensätze sind unter Tz. 4.5 festgelegt.

4. Dokumentenbearbeitung/Dokumentenaustausch

4.1 Dokumentenmanagement

Verbindlich: DOMEA 2.1 - Dokumentenmanagement.
Gültig*: 1/07 – 12/08*

DMS-Systeme müssen dem Konzept DOMEA in der Fassung 2.1 in Verbindung mit dem Anforderungskatalog 2.0 entsprechen.

Weitere Infos: www.domea.de

Empfohlen: pdf/a - Langzeitarchivierung von Dokumenten
Gültig*: 1/07 – 12/08*

Für die Langzeitarchivierung von Dokumenten soll das Format pdf/a verwendet werden.

Weitere Infos: www.adobe.de/products/acrobat/pdfs/pdfarchiving.pdf

4.2 Dokumentenaustausch

Verbindlich: Tiff – Textdokumente als Grafik / Bild
Gültig*: 1/07 – 12/08*

Für Textdokumente, die in Form einer Grafik / Bild ausgetauscht werden und nicht weiterverarbeitet werden müssen, ist tiff in der Untermenge Baseline-TIFF zu verwenden.
Weitere Infos: http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf

Verbindlich: pdf 1.4 –Textdokumente m Internet
Gültig*: 1/07 – 12/07*

Für Textdokumente, die im Internet veröffentlicht werden und nicht weiterverarbeitet werden müssen, ist pdf 1.4 zu verwenden.

Weitere Infos: http://partners.adobe.com/public/developer/pdf/index_reference.html

Verbindlich: pdf 1.5 – Textdokumente allgemein
Gültig*: 1/07 – 12/08*

Für Textdokumente, die nicht weiterverarbeitet werden müssen (mit Ausnahme von Grafiken/Bildern und Dokumenten für das Internet), ist pdf 1.5 zu verwenden.
Die Festlegung gilt auch für in Tabellenkalkulationen erzeugte Tabellen, die nicht weiterbearbeitet werden müssen, sowie für Präsentationen, die nicht weiterbearbeitet werden müssen.

Weitere Infos: http://partners.adobe.com/public/developer/pdf/index_reference.html

Empfohlen: rtf – Textdokumente zur Weiterbearbeitung.
Gültig*: 1/07 – 12/07*

Textdokumente, die vom Empfänger weiterverarbeitet werden sollen, sollen in rtf übermittelt werden.

Weitere Infos: http://msdn.microsoft.com/library/en-us/dnrtfspec/html/rtfspec.asp

Unter Beobachtung: excel97 –Tabellen zur Weiterbearbeitung
Gültig*: 1/07 – 12/07*

Für den Austausch von Tabellen ohne eingebettete Makros und Grafiken, die weiterbearbeitet werden sollen, kann excel 97 verwendet werden.

Weitere Infos: www.microsoft.de

Unter Beobachtung: Open Document 1.0– Officedokumente
Gültig*: 1/07 – 12/07*

Open Document ist herstellerunabhängig und als umfassendes Dokumentenaustauschformat geeignet. Die weitere Entwicklung ist zu beobachten.

Weitere Infos: ISO Norm ISO/IEC 26300

Verbindlich:: Graphics Interchange Format (GIF) - Grafiken
Gültig*: 1/07 – 12/07*

Für den Austausch von Grafiken und Schaubildern ist das Format Graphics Interchange Format (.gif) zu wählen.

Weitere Infos: http://www.w3.org/Graphics/GIF/spec-gif89a.txt

Empfohlen: TIFF (.tif) – verlustfreie Grafik
Gültig*: 1/07 – 12/07*

Für den Austausch von Grafikinformationen, die keinen Informationsverlust erlauben soll das Format TIFF (.tif) benutzt werden. Dabei ist Baseline-TIFF zu unterstützen.

Weitere Infos: http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf

Unter Beobachtung:: Portable Network Graphics (PNG) - ISO/IEC 15948:2003
Gültig*: 1/07 – 12/07*

Wenn möglich, kann das Grafikformat Portable Network Graphics96 (.png) verwendet werden.

Weitere Infos: http://www.w3.org/TR/PNG/

Verbindlich: Joint Photographic Experts Group (JPEG) - Bilder
Gültig: 1/06-12/08

Für den Austausch von Bildern ist das Format Joint Photographic Experts Group (.jpg) zu wählen.

Weitere Infos: ISO/IEC IS 10918-1, http://www.jpeg.org/index.html?langsel=de

Unter Beobachtung: Joint Photographic Experts Group (JPEG2000)
Gültig: 1/07-12/08

Für den (verlustfreien oder verlustbehafteten) Austausch von Bildern kann das Format JPEG2000 (.j2k , .jp2) genutzt werden.

Weitere Infos: ISO/IEC IS 15444-1, http://www.jpeg.org/jpeg2000/index.html?langsel=de

Empfohlen: zip 2.0 - Datenkompression
Gültig: 1/06-12/08

Große Dokumente ab ca. 2 MB bzw. mehrere gemeinsam zu übertragende kleinere Dateien sollen komprimiert übertragen werden. Als Austauschformat soll das Format ZIP Version 2.0 verwendet werden.

Weitere Infos: http://www.pkware.com/business_and_developers/developer/appnote/

Empfohlen: gzip 4.3 – Datenkompression
Gültig: 1/06-12/08

Alternativ zu zip kann auch das Format GZIP in der Version 4.3, spezifiziert in RFC 1952, als (.gz)-Dateien verwendet werden.

Weitere Infos: http://www.ietf.org/rfc/rfc1952.txt

4.3 Dokumentenbearbeitung

Gegenwärtig keine Festlegungen

4.4 Dokumentensicherheit

Gegenwärtig keine Festlegungen

4.5 Zeichensätze

Verbindlich: ISO 10646-1:2000 / Unicode v3.0 UTF-8
Gültig: 1/07-12/09

Um ausreichend Zeichen für die verschiedenen, weltweit existierenden Buchstaben, Ziffern und Symbole zur Verfügung zu haben, ist als Zeichensatz für Dokumente im HTML-Format ISO 10646-1:2000 / Unicode v3.0 in der UTF-8 Kodierung zu verwenden.

Weitere Infos: http://www.unicode.org

Empfohlen: ISO 8859-1 – erweiterter ASCI Zeichensatz
ISO 8859-15 – erweiterter ASCII Zeichensatz mit „€“
Gültig: 1/07-12/08

Der Zeichensatz ISO 8859-1 beinhaltet ASCII plus westeuropäische Sonderzeichen, wie die deutschen Umlaute. Er ist identisch mit den ersten 256 Zeichen des Unicode-Zeichensatzes.

ISO 8859-15 ist derzeit noch verbreitet und enthält zusätzlich zum Zeichensatz ISO 8859-1 z. B. das Euro-Zeichen „€“.

Weitere Infos: ISO/IEC 8859

5. Kommunikationsdienste

5.1 E-Mail

Verbindlich: E-Mail- Clients mit POP3/IMAP, SMTP, MIME
Gültig: 1/07-12/09

Zum Senden und Empfangen von E-Mails sind E-Mail-Clients einzusetzen, die zumindest den Austausch von unformatiertem Text gewährleisten und das Post Office Protocol 3 (POP3) bzw. das Internet Mailaccess Protocol (IMAP) unterstützen. Hierfür ist der Standard Simple Mail Trans-fer Protocol (SMTP) in Verbindung mit dem Standard Multipurpose Internet Mail Extensions (MI-ME) einzuhalten.

Weitere Infos: smtp. http://www.ietf.org/rfc/rfc821.txt
POP3. http://www.ietf.org/rfc/rfc1939.txt
IMAP. http://www.ietf.org/rfc/rfc3501.txt
MIME. http://www.ietf.org/rfc/rfc2045.txt

5.2 Sichere Online-Transaktionen

Verbindlich – Online Service Computer Interface (OSCI) – Transport v1.x
Gültigkeit: 1/07-12/08

Zur sicheren Abwicklung von Transaktionen im Rahmen von E-Government-Anwendungen ist OSCI einzusetzen.

Weitere Infos: www.osci.de

Verbindlich – Governikus
Gültigkeit: 1/07-12/08

Zur sicheren Kommunikation auf Basis von OSCI ist das Produkt Governikus einzusetzen. Governikus steht im Rahmen des vom Land Berlin abgeschlossenen Pflegevertrages allen Behörden der Berliner Verwaltung zur Nutzung zur Verfügung.

Weitere Infos: ITDZ

5.3 Verzeichnisdienst

Verbindlich: LDAP v3 – Protokoll für Zugriff auf Verzeichnisdienste
Gültig: 1/07-12/09

Zum Zugriff auf Verzeichnisdienste ist das Protokoll LDAP v3 zu verwenden. Verzeichnisdienste müssen dieses Protokoll unterstützen.

Weitere Infos: http://www.ietf.org/rfc/rfc2251.txt

5.4 FileTransfer

Verbindlich - ftp – Protokoll für Übertragung von Dateien
Gültig: 1/07-12/10

Für die Dateiübertragung gilt das File Transfer Protocol (FTP, RFC 959, RFC 1123, RFC 2228, RFC 2640) als Standard.

Weitere Infos: http://www.ietf.org/rfc/rfc959.txt

5.5 Zugang zum Internet

Empfohlen – Internetzugang über Grenznetz ITDZ
Gültigkeit: 1/07-12/09

Der Zugang von an das Berliner Landesnetz angeschlossenen Systemen zum Internet soll nur über das Grenznetz des ITDZ erfolgen. Eine entsprechende Landesvereinbarung ist mit dem ITDZ abzuschließen.

Weitere Infos: ITDZ: http://www.itdz.verwalt-berlin.de/BVC/kiss/produkte/zugang.htm
(Zur sicheren Nutzung des Internet vgl. auch Tz. 10.2)

Verbindlich – Standardkommunikationsprotokoll http
Gültig: 01/06 - 12/10

Für die Kommunikation zwischen Client und Web-Server ist http einzusetzen.

Weitere Infos: http://www.ietf.org/rfc/rfc1945.txt (v1.0)
http://www.ietf.org/rfc/rfc2616.txt (v1.1)

Verbindlich - Hypertext Markup Language (HTML) 4.01
Gültig: 1/07-12/08

Für Hypertext-Dokumente ist das HTML-Format als (.html)-Datei zu nutzen.

Weitere Infos: http://www.w3.org/TR/html401/

Empfohlen: Cascading Style Sheets Language Level 2 (CSS2)
Gültig: 1/07-12/08

Zur Gestaltung von HTML-Seiten soll die Cascading Style Sheets Language Level 2 (CSS2) verwendet werden.

Weitere Infos: http://www.edition-w3c.de/TR/REC-CSS2

Empfohlen: Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
Siehe Abschnitt 10.5

5.6 Weitere Dienste (File Service, PrintService …)

Gegenwärtig noch keine Festlegungen

6. Architektur IT-Verfahren, Middleware

6.1 Dienstearchitektur (SOA)

Verbindlich: Simple Object Access Protocol (SOAP) v1.1
Gültig: 1/07-12/09

Für die Kommunikation zwischen Anwendungen und insbesondere für den Zugriff auf E-Government-Dienste ist SOAP v 1.1 zu verwenden.

Weitere Infos: http://www.w3.org/TR/SOAP/

Verbindlich: Web Services Description Language (WSDL) v1.1
Gültig: 1/07-12/09

Zur Servicedefinition von WebServices ist die Web Services Description Language (WSDL) einzusetzen.

Weitere Infos: http://www.w3.org/TR/wsdl

6.2 Browserbasierte Anwendungen

Gegenwärtig noch keine Festlegungen

7. Datenbanken

Verbindlich –: Java Database Connectivity (JDBC) v3.0
Gültig: 1/07-12/09

Für Zugriffe auf Datenbanken ist von Java basierten Anwendungen JDBC zu nutzen.

Weitere Infos: http://java.sun.com/products/jdbc/

Empfohlen –: Open Database Connectivity (ODBC)
Gültig: 1/07-12/09

Für Zugriffe auf Datenbanken soll von nicht Java basierten Anwendungen ODBC genutzt werden.

Weitere Infos: http://msdn.microsoft.com/library/en-us/odbc/htm/dasdkodbcoverview.asp

Verbindlich –: SQL -2 (Structured Query Language) - ISO/IEC 9075:1992
Gültig: 1/07-12/09

Als Abfrage-, Verarbeitungs- und Definitionssprache für relationale Datenbanken ist SQL 2 (SQL-92) zu benutzen.

Weitere Infos: http://www.iso.org/

8. Netzwerkdienste

Verbindlich: TCP i.V.m. Internet Protocol (IP) v4
Gültig: 1/07-12/10

Als Kommunikationsprotokoll im Netzwerk (BeLa) ist IP v4 (RFC 0791, RFC 1700) in Verbindung mit TCP (Transmission Control Protocol, RFC 793) und UDP (User Datagram Protocol, RFC 768) zu verwenden.

Weitere Infos: http://www.ietf.org/rfc/rfc793.txt, http://www.ietf.org/rfc/rfc791.txt

Unter Beobachtung – ip v6 – Netzwerkprotokoll
Gültig: 1/07-12/08

Bei der Neubeschaffung von Systemkomponenten sollten solche beschafft werden, die neben IP v4 auch IP v6 unterstützen, um eine zukünftige Migration zu ermöglichen.

Weitere Infos: http://www.ietf.org/rfc/rfc2460.txt

Verbindlich – dns – Namensdienst
Gültig: 1/07-12/09

Als Name Server Dienst ist DNS zu verwenden.

Weitere Infos: http://www.ietf.org/rfc/rfc882.txt, http://www.ietf.org/rfc/rfc1035.txt,
http://www.ietf.org/rfc/rfc1034.txt

Verbindlich – snmp v2 – Netzwerkmanagementprotokoll
Gültig: 1/07-12/09

Als Netzwerkmanagementprotokoll ist SNMP v2 zu unterstützen.

Weitere Infos: http://www.ietf.org/rfc/rfc1157.txt, http://www.ietf.org/rfc/rfc3410.txt

9. Geo-Daten

Unter Beobachtung – Geodateninfrastruktur
Gültig: 1/07-12/09

In einem gemeinsamen Projekt der Länder Berlin und Brandenburg wird zur Zeit ein Umsetzungskonzept für den Aufbau einer gemeinsamen Geodateninfrastruktur (GDI Berlin-Brandenburg) erarbeitet. Dabei werden die einschlägigen Standards und Empfehlungen des OpenGisConsortiums (OGC) sowie der Initiative GDI-DE berücksichtigt, die gleichzeitig Basis der SAGA-Festlegungen sind.

Nähere Informationen zum Stand des Projekts im Intranetangebot Geodaten der Senstadt unter http://www.senstadt.verwalt-berlin.de/ebene2/fis/index.shtml)“.

10. IT-Sicherheit

10.1 Sicherheitskonzepte

Verbindlich: IT-Grundschutzkatalog, BSI-Standards 100x
Gültig: 01/07 – 12/09

Der IT-Grundschutz ist auf Basis der Sicherheitsmaßnahmen gemäß dem Grundschutzkatalog des BSI in der jeweils aktuellen Fassung zu gewährleisten. Für das Erstellen von Sicherheitskonzepten sind die methodischen Vorgaben des BSI (BSI-Standards 100x) zu beachten.

Weitere Infos: www.bsi.bund.de

Empfohlen: Modellhaftes IT-Sicherheitskonzept (ModellSiKo) für die Behörden der Berliner Verwaltung
Gültig: 01/07 – 12/09

Das ModellSiKo konkretisiert die Maßnahmen des Grundschutzkatalogs und unterstützt die Realisierung behördlicher IT-Sicherheitskonzepte. Im ModellSiKo finden sich zu allen nachfolgenden Regelungen weiterführende Maßnahmen.

Weitere Infos: http://www.verwalt-berlin.de/seninn/itk/sicherheit/modellsiko.html

10.2 Sichere Nutzung Fremdnetze/Internet

Fremdnetze sind alle IT-und TK-Netzstrukturen außerhalb des Geltungsbereiches der IT-Sicherheitsrichtlinie des Landes Berlin.

Verbindlich: Sicherheitskonzepte für Nutzung Internet
Gültig: 01/07 – 12/09

Die Nutzung der Fremdnetze einschließlich des Internet ist durch geeignete Maßnahmen auf das für die dienstliche Aufgabenwahrnehmung unbedingt erforderliche Maß zu begrenzen. Die vorzusehenden Kommunikationsmöglichkeiten haben sich an einem restriktiv zu definierenden Kommunikationsbedarf zu orientieren.

Voraussetzung für den Anschluss an Fremdnetze einschließlich Internet ist das Vorliegen eines schlüssigen Sicherheitskonzeptes und dessen konsequente Umsetzung.

Der Übergang in Fremdnetze einschließlich Internet soll nur über das Grenznetz des ITDZ (vgl. Tz. 5.5) erfolgen.
Ist in Ausnahmefällen wegen besonderer Anforderungen der Behörde der zentrale Übergang nicht nutzbar und ein ”eigener” Übergang notwendig, müssen durch die Behörde (mindestens) gleichwertige Sicherheitsmechanismen in Abhängigkeit vom vorhandenen Schutzbedarf realisiert werden.
Verbleibt trotz der realisierbaren Sicherheitsmaßnahmen ein unvertretbares Restrisiko darf der Zugriff nur von isolierten, nicht ins Berliner Landesnetz eingebundenen Systemen, auf denen keine schützenswerten Daten verarbeitet werden, erfolgen.

10.3 Nutzung Aktiver Komponenten

Bei der Nutzung von Aktiven Komponenten entsteht ein besonderes Risiko des unkontrollierten Datenabflusses.

Empfohlen: Verzicht auf Active X, Einrichtung „vertrauenswürdiger sites“
Gültig: 01/07 – 12/07

Active X soll geblockt werden. IT-Verfahren sollen keine Active X Elemente verwenden.

Arbeitsplätze mit Zugang zum Internet, die Aktive Komponenten benötigen, sollen physisch oder logisch getrennt vom Netz betrieben werden (stand alone Betrieb).

Falls für bestimmte Internetangebote die Nutzung Aktiver Komponenten auch von vernetzten Arbeitsplätzen aus zwingend erforderlich ist, können durch den dezentralen Infrastrukturbetreiber die entsprechenden Adressen freigeschaltet werden (“vertrauenswürdige Sites”).

10.4 Virenschutz

Verbindlich: gestaffelter Virenschutz
Gültig: 01/07 – 12/09

Virenschutzsoftware ist in mehreren Ebenen sowohl als Bestandteil der zentralen als auch der dezentralen IT-Infrastruktur einzusetzen.

Empfohlen: On-Demand und On-Access-Scanner
Gültig: 01/07 – 12/08

Die zur Ergänzung des zentralen Virenscanner im ITDZ erforderlichen dezentralen Systeme sollen sowohl auf den einzelnen PC als auch auf den Kommunikationsservern vorhanden sein. Hierbei ist es sinnvoll, On-Demand-Scanner (Virensuche auf Befehl des Benutzers) und On-Access-Scanner (ständig im Hintergrund aktiv) einzusetzen.
In den unterschiedlichen Ebenen sollen möglichst verschiedene Produkte zum Einsatz kommen.

10.5 Sichere Datenübertragung

Verbindlich: Schutz von Daten mit hohem Schutzbedarf
Gültig: 01/07 – 12/09

Daten mit hohem Schutzbedarf sind grundsätzlich verschlüsselt zu übertragen, es sei denn, durch andere Maßnahmen kann ein anforderungsgerechter Schutz gewährleistet werden. Mögliche gleichwertige Maßnahmen finden sich im ModellsiKo.

Empfohlen: Nutzung Standardnetzzugang
Gültig: 01/07 – 12/08

Zur verschlüsselten Übertragung von Daten mit hohem Schutzbedarf über das BeLa soll der Standardnetzzugang (SNZ) des ITDZ genutzt werden. Hierzu ist eine Landesvereinbarung abzuschließen.

Weitere Infos: ITDZ

Empfohlen: SSL/TLS
Gültig: 01/07 – 12/09

Zur Sicherung der Integrität, Vertraulichkeit und Authentizität einer Kommunikationsverbindung mit einem WebServer im Intranet soll SSL/TLS eingesetzt werden, sofern die Kommunikation nicht bereits über SNZ geschützt ist. Bei der Kommunikation im Internet ist auf die Anwendung von ssl hinzuwirken.

Weitere Infos: http://www.ietf.org/rfc/rfc2246.txt

Empfohlen: AES, 3DES
Gültig: 01/07 – 12/08

Zur (symmetrischen) Verschlüsselung sollen die Algorithmen AES und 3DES benutzt werden.

Weitere Infos: http://www.csrc.nist.gov/

10.6 Firewall

Verbindlich: Einsatz von Firewalls
Gültig: 01/07 – 12/08

Firewalls sind sowohl als Bestandteil der zentralen als auch der dezentralen IT-Infrastruktur einzusetzen. Dabei werden die Sicherheitsdomänen entsprechend ihrem Schutzbedarf durch eine Firewall gesichert und besitzen einen definierten und gesicherten Übergang ins Berliner Landesnetz. Bei der Implementierung von Zugangs- und Zugriffsregeln ist dabei für den Übergang in eine andere Sicherheitsdomäne von dem Grundsatz: ”Es ist alles verboten, was nicht explizit erlaubt ist” auszugehen.
Eingesetzte Firewalls müssen mindestens die funktionalen Anforderungen gemäß ModellSiKo erfüllen.
Server, die Dienste für anderen Sicherheitsdomänen anbieten, sind nicht im LAN, sondern in einer oder mehreren DMZ´n aufzustellen.

10.7 Fernwartung

Verbindlich Besondere Schutzmaßnahmen
Gültig: 01/07 – 12/09

Fernwartung bedarf besonderer Schutzmaßnahmen.

10.8 Laufwerke/Wechselmedien

Verbindlich: Verzicht auf Laufwerke für externe Datenträger
Gültig: 01/07 – 12/09

Bei PCs, die über einen festen Anschluss an das Berliner Landesnetz verfügen, dürfen keine Laufwerke für externe Datenträger vorhanden sein bzw. ist der Zugriff auf diese (und auf sonstige Schnittstellen für Wechselmedien) zu verhindern, sofern ihre Nutzung nicht für die Aufgabenerfüllung zwingend erforderlich ist.

10.9 IT-Verfahren

Verbindlich: Auflistung der verwendeten Kommunikationsprotokolle bzw. -dienste
Gültig: 01/07 – 12/09

Neue Verfahren und Programme dürfen die IT-Sicherheit bereits freigegebener Verfahren nicht reduzieren. Das sichere Zusammenwirken des freizugebenden mit den bereits eingesetzten IT-Verfahren ist daher im verfahrensspezifischen Sicherheitskonzept und bei der Freigabe zu berücksichtigen. Bei IT-Verfahren welche die zentrale IT-Infrastruktur nutzen gehört dazu insbesondere die Auflistung der dafür verwendeten Kommunikationsprotokolle bzw. -dienste, sowie deren Risikobetrachtung in dem entsprechenden verfahrensspezifischen Sicherheitskonzept.

Verbindlich: Keine lokalen Administratorrechte
Gültig: 01/07 – 12/09

IT-Verfahren dürfen für Installation und Betrieb nicht voraussetzen, dass der/die IT-Anwender(in) über lokale Administratorrechte verfügen muss.

10.10 Elektronische Signatur

Empfohlen: ISO/IEC 7816
Gültig: 01/07 – 12/09

Wenn IT-Verfahren den Einsatz von Smartcards planen, soll der Standard ISO/IEC 7816 beachtet werden.

Empfohlen: Algorithmen der Bundesnetzagentur
Gültig: 01/07 – 12/09

Beim Einsatz elektronischer Signatur sollen die von der Bundesnetzagentur veröffentlichten Algorithmen verwendet werden. Diese erfüllen die Anforderungen des Signaturgesetzes.

Weitere Infos:
http://www.bundesnetzagentur.de/enid/1606571333ef28439ca125393b17cfdf,0/Veroeffentlichungen/Algorithmen_sw.html).

11. Einführungs- und Änderungsmanagement IT-Verfahren

Gegenwärtig noch keine Festlegungen.