1. Verbindlichkeit der Standards

Die Staatskanzlei und die Geschäftsbereiche verwirklichen ihre Vorhaben der Informations- und Kommunikationstechnik (IKT-Vorhaben) im Einklang mit den nachfolgenden Standards und Richtlinien.

1.1 Verbindliche IKT-Standards

Die folgenden IKT-Standards sind von den Behörden, Gerichts- und Hochschulverwaltungen des Freistaates Bayern bei der Verwirklichung ihrer IKT-Vorhaben zu beachten:

a) BayITS-01 Definitionen

b) BayITS-02 Austausch von Dokumenten

c) BayITS-07 Betriebssystem für Server

d) BayITS-08 Datenbanksystem

e) BayITS-11 Standardarbeitsplatz und mobile Endgeräte

f) BayITS-12 Terminalserver

g) BayITS-14 Softwareverteilung

h) BayITS-16 Aktive Netzwerkkomponenten

i) BayITS-17 Werkzeuggestützte Modellierungssprachen

j) BayITS-18 Verzeichnisdiensteinträge

k) BayITS-19 Verschlüsselung mobiler Endgeräte und Datenträger

l) BayITS-20 Interoperabilität zwischen E-Akten-/Dokumentenmanagement- und Langzeitarchivierungssystemen

m) BayITS-21 Geoinformationssysteme/Geodaten

1.2 Verbindliche allgemeine IKT-Richtlinien

Die folgenden allgemeinen IKT-Richtlinien sind von den Behörden, Gerichts- und Hochschulverwaltungen des Freistaates Bayern bei der Verwirklichung ihrer IKT-Vorhaben zu beachten:

a) BayITR-01 Richtlinie für die Anzeige von IKT-Vorhaben

b) BayITR-02 Durchführung von IKT-Projekten

c) BayITR-03 Planungsrichtlinien für Kommunikationsnetze (KomNet)

d) BayITR-04 Rahmenrichtlinie für die Betriebsdienstleistungen der staatlichen Rechenzentren (RZ-DLR)

e) BayITR-05 Richtlinie über die Nutzung von Internet und E-Mail in der bayerischen Staatsverwaltung

f) BayITR-06 Softwarekonfigurationsmanagement

g) BayITR-07 Wirtschaftlichkeitsrechnungen im IKT-Bereich

h) BayITR-08 Anwendung der Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Dienstleistungen (EVB-IT)

i) BayITR-09 Sicherer E-Mail-Verkehr

1.3 Verbindliche Richtlinien für die IKT-Sicherheit

[1]Die folgenden Richtlinien für die IKT-Sicherheit sind von den Behörden, Gerichts- und Hochschulverwaltungen des Freistaates Bayern zu beachten. [2]Soweit Städte, Gemeinden, Landkreise und Bezirke am Bayerischen Behördennetz teilnehmen und die Regelungen sich auf dieses beziehen, haben sie folgende Richtlinien zu beachten:

a) BayITSiLL Leitlinie zur Informationssicherheit (IT Security Policy) für die bayerische Staatsverwaltung

b) BayITSiR-O Richtlinie zur Informationssicherheitsorganisation der bayerischen Staatsverwaltung

c) BayITSiR-GL Rahmenrichtlinie IT-Sicherheitsprozess

d) BayITSiR-01 Grundlagen Behördennetz

e) BayITSiR-02 Übergang in Fremdnetze

f) BayITSiR-03 Einsatz drahtloser Netze

g) BayITSiR-04 Betrieb von IP-basierenden Virtuellen Privaten Netzen (IP-VPN)

h) BayITSiR-05 Telearbeits- und mobile Arbeitsplätze

i) BayITSiR-06 Fernwartung und externe Anwendungen

j) BayITSiR-07 Einsatz mobiler Geräte

k) BayITSiR-08 Durchführung von Penetrationstests

l) BayITSiR-09 Extranet-/Dienstleister-VPN

m) BayITSiR-10 Sicherheitsrichtlinie für Wählverbindungen im Bayerischen Behördennetz

n) BayITSiR-11 Nutzung von Anwendungen über das Internet unter Verwendung von SSL/TLS

o) BayITSiR-12 E-Mail-Verkehr im Bayerischen Behördennetz

p) BayITSiR-13 Sicherheit von IT-unterstützten Endgeräten

q) BayITSiR-14 Sicherheit von Web-Anwendungen der Bayerischen Staatsverwaltung