Datensicherheitsmaßnahmen für Web-Anwendungen	**Konvention** **pv-dasi 1.2.1** **25.1.2006** **Empfehlung**

Kurzbeschreibung	Für die Anleitung und Verpflichtung der einzelnen zugriffsberechtigten Stellen auf die Einhaltung konkreter Datensicherheitsmaßnahmen ist ein allgemein abgestimmtes Muster vorteilhaft. Dieses Dokument enthält ein solches Muster, das einer Vereinbarung zwischen Stammportalbetreiber und zugriffsberechtigter Stelle angeschlossen werden soll.	
Autor(en):	Wilfried Connert Claudia Springer-Knam	Projektteam / Arbeitsgruppe

Stelle	Vorgelegt am	Angenommen am	Abgelehnt am
IKT-Board	6.12.2005	10.1.2006	
Länder	6.12.2005	10.1.2006	
Gemeindebund	6.12.2005	10.1.2006	
Städtebund	6.12.2005	10.1.2006	

Dokumentklasse:
Konvention
Erläuterung
Information

Doku-Stadium:
Entwurf intern
Entwurf öffentlich
Empfehlung

Datensicherheitsmaßnahmen für Web-Anwendungen

Generelle Bestimmungen

Zur Gewährleistung einer sicheren elektronischen Kommunikation zwischen Kommunikationspartnern sind Sicherheitsmaßnahmen auf mehreren Ebenen zu treffen. Die Einhaltung dieser Bestimmungen ist Voraussetzung für einen ordnungsgemäßen Betrieb und daher verpflichtend für alle Partner.

In Abhängigkeit von der Sicherheitsklassifizierung der jeweiligen Anwendung können neben den hier beschriebenen *Allgemeinen Bestimmungen* noch weitere Vorschriften – wie etwa die Nutzung von SSL-Clientzertifikaten – hinzukommen. Diese zusätzlichen Anforderungen werden im Bedarfsfall in einem gesonderten Dokument festgehalten.

Die unter dem Punkt „Allgemeine Sorgfaltspflicht“ beschriebenen Maßnahmen gelten für alle Benutzer, unabhängig von ihrer Funktion. Benutzer- und Rechteverwalter müssen darüber hinaus auch noch die unter dem Punkt „Besondere Bestimmungen für Benutzer- und Rechteverwalter“ beachten.

Allgemeine Sorgfaltspflicht

Benutzerkonten und Passworte

Die Anlage von Benutzerkonten (Benutzerregistrierung) in den einzelnen personalführenden Stellen erfolgt **durch die jeweils nominierten Benutzerverwalter**. Beim Einrichten der Benutzerkonten wird ein **Einmal-Passwort** festgelegt, welches dem berechtigten Benutzer übermittelt wird. Dieser muss das Einmal-Passwort bei der ersten Anmeldung **umgehend ändern** und ein **neues, persönliches Passwort vergeben.**

Die Anmeldung mit einer Bürgerkarte ersetzt die Eingabe von Benutzerkennung und Passwort.

Für den Zugriff auf Anwendungen der Sicherheitsklasse 3 (wird für die jeweilige Anwendung festgelegt und kundgemacht) wird auf das Dokument SecClass verwiesen.

Die Anmeldung mit **Bürgerkarte** an einem PC in einem sicheren Netz erfüllt diese Anforderungen.

Benutzerkonten sind **personenbezogen**, daher darf nur der Eigentümer das jeweilige Konto benutzen. Die Benutzer dürfen das Passwort **unter keinen Umständen** anderen Personen **bekannt geben**. Das Passwort sollte nach Möglichkeit nicht schriftlich fixiert werden. Wird es doch aufgeschrieben, so ist für die Sicherheit dieser Aufzeichnungen besonders Sorge zu tragen.

Weiters gelten die folgenden Bestimmungen für Passworte:

- Ein **Passwort** muss aus **mindestens 6 Zeichen** bestehen. Es muss regelmäßig gewechselt werden (zB. alle 90 Tage). Sollte der Verdacht bestehen, dass das Passwort auch unautorisierten Personen bekannt geworden ist, so ist es sofort zu wechseln.
- Die Verwendung von **Trivial-Passwörtern** ist unbedingt zu **unterlassen**. (Trivial-Passwörter sind solche Passwörter mit spezieller Bedeutung, welche leicht auch von Außenstehenden erraten oder bestimmt werden können. Also z.B. Namen (eigene, aus der Familie, von Prominenten), Geburtsdaten, Firmen- und Abteilungsbezeichnungen, Kfz-Kennzeichen usw.. Ebenfalls in diese Gruppe fallen Standardausdrücke wie etwa TEST, SYSTEM, Tastatur- und Zeichenmuster, wie ABCDEF, QWERTZ, 123456,...)
- Innerhalb eines Passwortes sollte mindestens 1 Zeichen verwendet werden, das kein Buchstabe ist (**Zahl oder Sonderzeichen**).
- Ganz allgemein ist darauf zu achten, dass die **Eingabe** des Passwortes **unbeobachtet** erfolgt.
- Passwörter dürfen **nicht** auf programmierbaren Funktionstasten **gespeichert** werden. Die Speicherfunktion des Browsers für Passworte soll nicht verwendet werden

Soweit es das jeweilige Betriebssystem zulässt, ist die Einhaltung dieser Richtlinien durch entsprechende Einstellungen des Betriebssystems sicherzustellen.

Eine fünfmalige **Fehleingabe** des Passwortes führt zur **Sperrung der Zugangsberechtigung**, welche nur durch den zuständigen Benutzerverwalter (oder von der Hotline) wieder aufgehoben werden kann.

Virenschutz

Viren, ebenso wie Trojaner, Würmer u.a.m., sind Programme, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige

Veränderungen **unkontrollierbare Schäden an Daten und Programmen** anrichten können. Um diese Schäden und die damit verbundenen oft erheblichen Kosten und Aufwendungen zu vermeiden, sind insbesondere die **folgenden vorbeugenden Maßnahmen** zu treffen:

- Einsatz eines marktgängigen **Anti-Viren Programms**
- **Regelmäßiges Update** der Virendatenbank.
- **Überprüfung** aller ein- und ausgehenden **Datenträger**.

Zugriffsschutz und Raumsicherheit

Zusätzlich zu den schon genannten Maßnahmen ist es notwendig, den Zutritt zu den Räumen und Geräten zu regeln, in denen sich Kommunikationsendpunkte (also in der Regel PCs) befinden.

Folgende Maßnahmen werden dringend empfohlen:

- **Verbindungen** sind zu **trennen**, sobald sie nicht mehr benötigt werden.
- Bei **kurzer Abwesenheit** ist **immer ein Bildschirmschoner** mit **Passwortschutz** zu verwenden (**Wartezeit 5 Minuten).**
- Bei **längerer Abwesenheit** ist der PC / die Workstation **zu sperren.**
- **Räume** sind beim Verlassen **abzusperren**, wo immer das möglich ist.
- **Bildschirme** sind **so aufzustellen**, dass **keine unbefugte Einsicht möglich** ist.
- **Datenträger**, **Ausdrucke** sind vor Einsichtnahme zu **schützen**.

Besondere Bestimmungen für Benutzer- und Rechteverwalter

Die registrierten Benutzer- und Rechteverwalter tragen über die „allgemeine Sorgfaltspflicht“ hinausgehende Verantwortung bei der Erfüllung ihrer besonderen Aufgaben. Sie haben daher neben den oben angeführten Maßnahmen noch folgende Bestimmungen zu beachten:

- Nur **berechtigte Personen** dürfen als Benutzer **erfasst** werden.
- Dem Datenschutzgesetz (DSG 2000) entsprechend dürfen Benutzern **nur jene Rechte** zugewiesen werden, die sie zur **Erfüllung** der ihnen übertragenen **Aufgaben** benötigen.

- Die Vergabe von Rechten hat nach den **Vorgaben** der jeweiligen **Anwendung** zu erfolgen.
- Einer **Änderung in der Aufgabenzuordnung** hat eine entsprechende **Anpassung der Rechte** nach sich zu ziehen.
- Der Benutzerverwalter und Rechteverwalter wird bei Verdacht auf Missbrauch aufgefordert, seinen Möglichkeiten entsprechend bei der **Aufklärung** mitzuwirken.

Die gesamte Rechteverwaltung (also etwa das Erfassen, Ändern, Entziehen/Löschen von Rechten bzw. von Personen) wird im Stammportal **protokolliert**, sodass sämtliche Bearbeitungen **nachvollziehbar** werden.

Die Benutzer- und Rechteverwalter tragen die **Verantwortung für die Einhaltung der Datenschutzmaßnahmen** im jeweiligen Zuständigkeitsbereich, sie haben daher die von Ihnen betreuten Benutzer über diese Richtlinien aufzuklären.

Im Zuge der Meldung der Benutzer- und Rechteverwalter ist auch eine von diesen unterfertigte **Verpflichtungserklärung** die Einhaltung der Datensicherheitsbestimmungen betreffend zu übermitteln.

Anlage:

Version 1.1: Einarbeitung der Anregungen und Bemerkungen aus Rückmeldungen der Länderarbeitsgruppe

Version 1.2: Einarbeiten von Änderungen nach Einspruch im Aussendungsverfahren

Version 1.2.1: Einarbeiten einer Anregung des IKT-Boards auf Seite 3.