Datensicherheitsmaßnahmen für Webanwendungen		**Konvention**	
		pv-dasi 2.0.0	
		Ergebnis der AG	
Kurzbeschreibung	Für die Anleitung und Verpflichtung der zugriffsberechtigten Stellen sowie der einzelnen Benutzerinnen und Benutzer 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):	Anna-Karina Hafner (Tirol) Hannes Wittmann (Wien)	Projektteam / Arbeitsgruppe	
		AG Recht und Sicherheit (AG-RS) **AG-Leiter:** Bernhard Karning (BKA) **Stellvertreter:** Alena Sirka-Bred (Wien)	
Beiträge von:			
Datum	06.11.2013	Version	2.0.0

Version 2.0.0 : **06.11.2013** Fristablauf: **tt.mm.jjjj**

Inhaltsverzeichnis

1 Einleitung

1.1 Ausgangssituation

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

1.2 Ziele

Das vorliegende Dokument soll die organisatorischen und technischen Sicherheitsmaßnahmen spezifizieren, welche von Benutzerinnen und Benutzern sowie von der zugriffsberechtigten Stelle bei der Nutzung von Anwendungen zu treffen bzw. einzuhalten sind.

Ziel dieser Maßnahmen ist die Gewährleistung von

- Vertraulichkeit (Geheimhaltung der Information),
- Integrität (Schutz vor unbefugter Veränderung der Information) und
- Zurechenbarkeit (Nachvollziehbarkeit der Verwendungsvorgänge[1]).

Dadurch soll ein Sicherheitsniveau erreicht werden, das für den normalen Schutzbedarf angemessen und ausreichend ist.

2 Begriffe

Nachfolgend werden verschiedene Begrifflichkeiten zum besseren Verständnis erläutert. Technische Begriffe werden im AG-IZ-Glossar [GLOSSAR] erklärt.

2.1 Informationen bzw. Daten

Informationen bzw. Daten werden meist über eine Datenanwendung dem Benutzer zur Verfügung gestellt. Der Umfang des Zugangs zu diesen Informationen ist durch Rechte und Rollen definiert. Somit kann sichergestellt werden, dass der jeweilige Anwender nur die ihn betreffenden Informationen erhält.

- **Recht:** Das Recht definiert in einem Gesetz, einer Verordnung, einem Vertrag, einer Nutzungsvereinbarung, einer Allgemeinen Geschäftsbedingung die Zuständigkeit bzw. den Zugriffsumfang einer Organisation oder einer bestimmten Person. Rechte werden durch Rollen an Personen zugeteilt.
- **Rolle:** Die Rolle ist das technische Zugriffsrecht auf eine bestimmte Anwendung oder ein bestimmtes Verfahren, dass der zugriffsberechtigten Person zugewiesen wird. (Beispiel: „Finanz-Online“ mit unterschiedlichen Rollen als „Bürger“ oder „Buchhalter“, „Steuerberater“ etc.)

[1] [DSG 2000] §14 Z 7 Datensicherheitsmaßnahmen

2.2 Allgemein verfügbare Daten

Daten (auch personenbezogene Daten) sind unter anderem dann „allgemein verfügbar“, wenn sie „zulässigerweise veröffentlicht“ worden sind. Diese Daten unterliegen keinem besonderen Geheimhaltungsanspruch (Beispiel: Telefonbuch).

2.3 Daten mit hohem Schutzbedarf

Der Schutzbereich des Grundrechts auf Datenschutz bezieht sich lediglich auf „personenbezogene Daten“. Je nach Art der Daten lässt sich jedoch ein darüber hinaus gehender Grad der Schutzwürdigkeit bei Datenanwendungen im Portalverbund ableiten:

- **Bestimmte oder bestimmbare personenbezogene Daten** (§4 DSG 2000 idgF): Darunter sind Angaben über Betroffene zu verstehen, deren Identität bestimmt oder bestimmbar ist.
- **Indirekt personenbezogen** (§4 DSG 2000 idgF) sind Daten dann, wenn durch einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmt werden kann.
- **Schutzwürdige Geschäftsdaten** sind Daten ohne Personenbezug, die aufgrund Ihrer Beschaffenheit oder ihres Informationsgehaltes eine geringe oder mittlere Auswirkung im Schadensfall haben.

2.4 Daten mit besonders hohem Schutzbedarf

Besonders schutzwürdige Daten sind Informationen die auf Grund ihrer Beschaffenheit bzw. ihres Inhaltes nur unter Einhaltung von besonderen Sicherheitsmaßnahmen verwendet werden dürfen. Auch hier reicht die Skala der Schutzwürdigkeit bei Datenanwendungen im Portalverbund über die des DSG 2000 hinaus.

- **Sensible Daten** (§4 DSG 2000 idgF): Besonders schutzwürdig sind Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.
- **Strafrechtsbezogene Daten** sind zwar keine sensiblen Daten, für diese sind allerdings im DSG 2000 Sonderbestimmungen vorgesehen (§8 und 18 DSG 2000 idgF).
- **Besonders schutzwürdige Geschäftsdaten** sind Daten ohne Personenbezug, die aufgrund Ihrer Beschaffenheit oder ihres Informationsgehaltes eine hohe oder sehr hohe Auswirkung im Schadensfall haben.

2.5 Sicherheitsklassen

Die Sicherheitsklassen regeln die Informationssicherheit für den Portalverbund in den Bereichen Vertraulichkeit und Integrität für die Dauer der Nutzung einer Datenanwendung durch Benutzerinnen und Benutzer.

Wird eine Anwendung zur Verfügung gestellt, so legt der Anwendungsverantwortliche durch die Klassifizierung der Anwendungsrollen mittels Sicherheitsklassen fest, welche Sicherheitsmaßnahmen beim Zugriff auf die Anwendung in der entsprechenden Rolle eingehalten werden müssen.

2.6 Wissen und Besitz

Für den Zugriff auf Anwendungen und Verfahren sind entsprechend der vorgegebenen Sicherheitsklasse unterschiedliche Authentifizierungsmethoden zu verwenden.

- **Wissen:** z.B. Benutzername und Passwort, PIN-Verfahren
- **Wissen und Besitz:** z.B. Hardwaretoken (bspw. Dienstkarte/Bürgerkarte) i.V. mit PIN oder Passwort

3 Umsetzung von Sicherheitsmaßnahmen

3.1 Allgemeine Sorgfaltspflicht

Für vertrauliche Informationen (wie personenbezogene Daten, Passwörter, Geschäftsdaten etc.) besteht die inhärente Gefahr, dass diese durch technisches Versagen, Unachtsamkeit oder auch durch vorsätzliche Handlungen offengelegt werden. Dabei kann auf diese vertraulichen Informationen an unterschiedlicher Stelle zugegriffen werden.

3.2 Technische Vorgaben

Technische Vorgaben, welche durch die entsprechenden Stellen (unter anderem durch den Stammportalbetreiber) vorgegeben werden, wie z.B. Virenschutz bzw. Firewall sowie andere technische Maßnahmen, welche der Datensicherheit auf dem Endgerät dienen, dürfen nicht deaktiviert werden. Ist durch technische Mängel ein einwandfreier Betrieb nicht möglich oder sichergestellt, so ist umgehend die zuständige technische Stelle zu informieren.

3.3 Organisatorische Maßnahmen

3.3.1 Benutzerkonten und Passwörter

Verantwortlich: zugriffsberechtigte Stelle, Benutzer

Die Anlage von Benutzerkonten (Benutzerregistrierung) in den einzelnen personalführenden Stellen erfolgt durch die jeweils nominierten Benutzerverwalter. Benutzerkonten sind personenbezogen, daher darf nur der Eigentümer das jeweilige Konto benutzen. 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.

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

Die Anmeldung mit Wissen und Besitz (siehe Kapitel 2.6) ersetzt die Eingabe von Benutzerkennung und Passwort und wird für höhere Sicherheitsanforderungen verwendet. Für den Zugriff auf Anwendungen der Sicherheitsklasse 3 (wird für die jeweilige Anwendung festgelegt und kundgemacht) wird auf die „SecClass“-Dokumente verwiesen. Die Anmeldung mit Wissen und Besitz an einem PC in einem sicheren Netz erfüllt diese Anforderungen.

Die Benutzer dürfen Berechtigungsnachweise bzw. Zugangsdaten (Passwörter, Hardware-Token, Dienstkarten,…) unter keinen Umständen anderen Personen bekannt- bzw. weitergeben. Im Vertretungsfall muss der Vertreter/die Vertreterin selbst entsprechend berechtigt werden. Je nach Art der Anwendung sind Stellvertreterberechtigungen einzurichten.

Weiters gelten die folgenden Bestimmungen für Passwörter:

- Für die Verwendung und den Wechsel von Passwörtern sind dem Stand der Technik entsprechende Regelungen einzuhalten bzw. zu treffen. Passwörter müssen entsprechende Vorgaben erfüllen (Passwortlänge, Verwendung von Sonderzeichen bzw. Zahlen).
- Es ist darauf zu achten, dass die Eingabe des Passwortes unbeobachtet erfolgt.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden. Die Speicherfunktion des Browsers für Passwörter darf ebenfalls nicht verwendet werden.
- Passwörter dürfen nicht notiert werden.

3.3.2 Unbefugter Zugang bzw. Zugriff

Verantwortlich: Benutzer

Folgende **Maßnahmen** sind jedenfalls zu beachten**:**

- Verbindungen sind zu trennen, sobald sie nicht mehr benötigt werden.
- Räume mit IT-Arbeitsplätzen sind beim Verlassen zu versperren. Dies ist während der Regelarbeitszeit dann nicht erforderlich, wenn aufgrund geeigneter Vorkehrungen davon auszugehen ist, dass nicht zur Organisationseinheit gehörige Personen den Raum nicht betreten können.
- Bildschirmsperren sind zur Absicherung des Zugriffes auf die IT-Infrastruktur durch unberechtigte Personen entsprechend dem vorgegebenen Standard zu verwenden.
- Bildschirme sind so aufzustellen, dass keine unbefugte Einsicht möglich ist.
- Datenträger, Ausdrucke sind vor Einsichtnahme zu schützen.

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.

3.3.3 Maßnahmen bei Sicherheitsverletzungen

Verantwortlich: zugriffsberechtigte Stelle, Benutzer

Organisatorische Sicherheitsvorfälle und –probleme sind zur Schadenminimierung oder -prävention unverzüglich von den Benutzern oder Betroffenen innerhalb der zugriffsberechtigten Stelle zu melden. Sind innerhalb der zugriffsberechtigten Stelle keine Prozesse zur Meldung von (vermuteten) Sicherheitsverletzungen vorhanden, so sind diese direkt dem Vorgesetzen zu melden.

3.3.4 Soziale Medien

Verantwortlich: zugriffsberechtigte Stelle, Benutzer

Der Umgang mit sozialen Medien wie Facebook, Twitter oder ähnlich im beruflichen Umfeld muss durch die Organisation geregelt werden. Der Umgang mit Sozialen Medien wird in den Leitfäden

„BeamteZweiNull“ bzw. „Soziale Medien & Netzwerken in der Verwaltung“ geregelt [SOZMED].

Werden soziale Medien durch Benutzerinnen und Benutzer im privaten Umfeld verwendet, so ist darauf zu achten, dass im Sinne der Amtsverschwiegenheit und des Datenschutzes keine dienstliche Informationen weitergegeben werden.

3.4 Organisatorische Maßnahmen für Benutzer- und Rechteverwalter

3.4.1 Verwaltung von Rechten

Verantwortlich: zugriffsberechtigte Stelle, 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) bzw. dem „Need-to-Know- Prinzip“ 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 zeitnah nach sich zu ziehen. Jährlich muss überprüft werden, ob die von einer Person verfügbaren Zugriffsrechte noch deren Tätigkeitsprofil entsprechen oder ob Einschränkungen zweckmäßig sind.
- 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) 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.

3.5 Technische Maßnahmen

3.5.1 Mobile Datenspeicher

Verantwortlich: zugriffsberechtigte Stelle, Benutzer

Durch die Verwendung von mobilen Datenspeichern (z.B. USB-Stick) existieren eine Menge potentieller Gefährdungen für die zugriffsberechtigte Stelle (u.a. die Gefahr des Vertraulichkeits- oder Integritätsverlustes von Daten).

Folgende **Maßnahmen** werden daher **dringend empfohlen**:

- Die Verwendung von privaten Datenspeichern (vertrauenswürdige Geräte) bedarf Regelungen durch die zugriffsberechtigte Stelle. Sind solche Regelungen nicht vorhanden, dürfen grundsätzlich keine privaten Datenspeicher verwendet werden. Daten über Datenträger der Organisation dürfen nur nach Auftrag durch den Dateneigentümer weitergegeben werden.

- Ist die Herkunft eines USB-Datenträgers nicht bekannt, so handelt es sich um ein „nicht vertrauenswürdiges Gerät“ und die Verwendung ist nicht gestattet, da sich Schadprogramme auf diesem Weg verbreiten können.

3.5.2 Mobile Endgeräte

Verantwortlich: zugriffsberechtigte Stelle, Benutzer

Zu den wichtigsten mobilen Hardwareplattformen zählen derzeit Mobiltelefone, Smartphones, PDAs, Laptops und Tablet-PCs. Im Sinne der IT-Sicherheit muss die bereitstellende Stelle (Organisation) ein Regelwerk vorgeben, das beschreibt, was erlaubt ist und was nicht, und das Anforderungen an die Einsatzumgebung stellt (bspw. Vorgehen bei Verlust des Gerätes oder Regeln für Installation neuer/fremder Software).

Der Einsatz eigener IT-Geräte von Mitarbeitern zur dienstlichen Nutzung ist grundsätzlich nicht gestattet; in Ausnahmefällen kann die Organisation dies allerdings zulassen (BYOD [Bring Your Own Device]-Strategie).

3.5.3 Schadprogramme

Verantwortlich: zugriffsberechtigte Stelle, Benutzer- und Rechteverwalter, Benutzer

Zu den typischen Arten von Schadprogrammen gehören Viren, Würmer und Trojaner. Diese Schadprogramme, welche eine Vielzahl von Funktionen enthalten, können durch das verdeckte Eindringen in den ordnungsgemäßen Betrieb bzw. durch Manipulation, Ausspionieren oder Entwendung von Daten zur Beeinträchtigung von Funktionalitäten führen sowie unkontrollierbare Schäden anrichten. 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,
- Regelmäßige sicherheitsrelevante Updates,
- Überprüfung aller ein- und ausgehenden Datenträger,
- Sicherheitsvorfälle, insbesondere von Schadprogramm-Infektionen, bzw. der Verdacht eines solchen müssen zeitnah an den Stammportalbetreiber gemeldet werden.

Literaturverzeichnis

[Datenschutzrecht]	Jahnel D. , Datenschutzrecht, Jan Sramek Verlag, 2010
[DSG 2000]	Pollierer H.-J., Weiss E., Knyrim R., DSG Datenschutzgesetz, Manz Verlag, 2010
[SecClass]	Hörbe R., Spezifikation Sicherheitsklassen 2.1, 2007
[PVV]	Connert, Grandits, Kotschy, Posch, Siegl, Portalverbundvereinbarung, 2002
[GLOSSAR]	Stradal H., AG-IZ Glossar, 2010
[SOZMED]	http://reference.e-government.gv.at/uploads/media/BeamteZweiNull_1-0-0_20101019.pdf

Anlage: Dokumentenhistorie

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.
Version 2.0:	Anpassung des Dokumentes an den aktuellen Stand der Technik sowie Einarbeitung von Änderungen aufgrund Rückmeldungen der Arbeitsgruppe Recht und Sicherheit