Revisionsleitfaden Portalverbund	**Best practise**
	Rev_pv_1.0
	Ergebnis der AG

Gemäß § 6 Absatz 6 PVV haben Stammportalbetreiber mindestens einmal jährlich eine Sicherheitsrevision durchzuführen oder zu veranlassen.

Um einen einheitlichen Standard bei allen Portalverbundteilnehmern zu erreichen, sind in diesem Revisionsleitfaden, der benutzerfreundlich in Form einer Checkliste gestaltet wurde, alle Verpflichtungen der Portalbetreiber (Stamm- und Anwendungsportalbetreiber) so aufgearbeitet, dass damit eine regelmäßige Revision erleichtert werden soll.

Autor(en):	Franz Fahrngruber, Rainer Hörbe, Peter Pfläging, Alena Sirka	Projektteam / Arbeitsgruppe AG Recht und Sicherheit AG Integration und Zugänge
Beiträge von:	Robert Glock, Martin Spitzenberger, Mirjam Jilka	

Version: **28.9.2009**

Freigegeben von AG Recht und Sicherheit mit 19.10.2009

Fristablauf: **TT.MM.JJJJ**
(Länderangabe bei ablehnender Stellungnahme)

Unter-Version … : **TT.MM.JJJJ**

Fristablauf: **TT.MM.JJJJ**
(Länderangabe bei ablehnender Stellungnahme)

Detail-Version … : **TT.MM.JJJJ**

Freigabe: **TT.MM.JJJJ**
(Detailangaben zur Freigabe)

Revisionsleitfaden Portalverbund

Die jeweils gültige Antwort bitte anhaken oder ankreuzen.
(Alle geschlechtsbezogenen Formulierungen treffen auf beide Geschlechter zu).

Dieser Leitfaden soll Sie bei der Revision Ihres Stammportals bzw. Ihres Anwendungsportals unterstützen. Die Checkliste orientiert sich an den Pflichten, die sich aus der Portalverbundvereinbarung (PVV), dem Portalverbundprotokoll (PVP), der Konvention Sicherheitsklassen für den Zugriff von Benutzern auf Anwendungen – (SecClass) sowie der Konvention Datensicherheitsmaßnahmen für Web-Anwendungen (pv-dasi) für die Stamm- bzw. Anwendungsportale ergeben.

Die Umsetzung dieser Verpflichtungen wird notwendigerweise in den einzelnen Organisationen unterschiedlich geregelt sein. Eine Revision der Portale wird daher sinnvollerweise unter Einbeziehung dieser internen Umsetzungsregeln erfolgen müssen.

0. Organisationsinterne Sicherheitsrichtlinien

0.1	Gibt es in Ihrer Organisation ein Informations-sicherheits-Management-System (ISMS), das auch den Portalverbund berücksichtigt?	Ja	Nein
0.2	Wo ist die Dokumentation aufbewahrt bzw. wo steht sie zur Verfügung?	.....	
0.3.1	Werden zeitliche und finanzielle Ressourcen für die IT-Sicherheitsbeauftragten budgetiert?	Ja	Nein
0.3.2	Sind den IT-Sicherheitsbeauftragten die wesentlichen rechtlichen Vorschriften bekannt?	Ja	Nein
0.3.3	Wie und in welchem Umfang erfolgt die Weiterbildung der IT-Sicherheitsbeauftragten?	.....	

I. Das Stammportal:

1. Die Publikation von Informationen über das Stammportal (Betriebshandbuch)[1]

1.1	Gibt es für das Portal festgelegte Betriebszeiten?	Ja	Nein
1.1.1	Wenn ja:	Von:	Bis: .....
1.2	Wer ist der Portalbetreiber des Stammportals:	.....	
1.3	Wer ist Ansprechpartner des Stammportals?	Name: ..... E-mail:	
1.4	Hat eine Überprüfung der Publikation auf Aktualität innerhalb des letzten Jahres stattgefunden?	Ja	Nein
1.5	Ist die Publikation richtig und aktuell?	Ja	Nein

2. Dienstleister für Aufgaben des Stammportalbetreibers [2]

(entfällt, wenn kein Dienstleister für den Betrieb des Stammportals herangezogen wird)

2.1	Gibt es mit dem Dienstleister eine vertragliche Vereinbarung?	Ja	Nein
2.1.1	Wo ist sie abgelegt/gespeichert?	.....	
2.1.2	Wurde die Vereinbarung schriftlich abgeschlossen?	Ja	Nein
2.1.3	Wurde die Vereinbarung unter Einbeziehung der verantwortlichen Stellen abgeschlossen?	Ja	Nein

[1] § 8 PVV
[2] § 10 PVV, § 11 DSG 2000

2.1.4	**Zum Inhalt der Vereinbarung:**		
2.1.4.1	Wurde der Dienstleister darauf hingewiesen, dass die Daten nur im Rahmen des Auftrages verwendet werden dürfen?	Ja	Nein
2.1.4.2	Welche Datensicherheitsmaßnahmen wurden seitens des Dienstleisters eingerichtet?		
2.1.4.3	Welche Kontrollmechanismen für den Auftraggeber wurden festgelegt?		
2.1.4.4	Wurde der Dienstleister darauf hingewiesen, dass Subdienstleister nur nach Genehmigung einbezogen werden dürfen und eine entsprechende Vereinbarung vorhanden sein muss?	Ja	Nein
2.1.4.5	Sind Vorkehrungen getroffen worden, damit die Pflichten des Stammportalbetreibers erfüllt werden können?	Ja	Nein
2.1.4.6	Wurde die Rückgabe aller Unterlagen bei Dienstleistungsende terminlich fixiert/überprüft?	Ja	Nein

3. Die Organisation der Benutzerverwaltung [3]

3.1	Wurde eine dokumentierte Organisation der Abläufe im Bereich der Benutzerverwaltung eingerichtet?	Ja	Nein
3.2	Wurde eine dokumentierte Organisation der Benutzerverwaltung in den zugriffsberechtigten Stellen eingerichtet?	Ja	Nein

[3] § 6 (1) PVV

4. Die Rechteverwaltung [4]

4.1	Ist die Nachvollziehbarkeit von Anforderung und Vergabe von PVP-Rechten gegeben?	Ja	Nein
4.2	**Für jede Anwendung gesondert durchzuführen:**		
4.2.1	Bezeichnung der Anwendung laut Publikation am Reference Server:	.....	
4.2.2	Welche der vom Anwendungsverantwortlichen zur Verfügung gestellten PVP-Rechte mit welchen Rechteparametern der Anwendung wurden im Stammportal definiert?	.....	
4.2.3	Welche Sicherheitsklasse wurde für die jeweiligen PVP-Rechte der Anwendung im Stammportal definiert (zumindest die vom Anwendungsverantwortlichen für die Anwendung publizierte!)?	.....	
4.2.4	Wurden die entsprechenden Maßnahmen für die definierte Sicherheitsklasse eingerichtet und sind sie noch aktuell?	Ja	Nein
4.2.5	Gibt es eine zusätzliche Nutzungsvereinbarung für diese Anwendung?	Ja	Nein
	Wenn Ja:		
4.2.5.1	Wurde die Vereinbarung schriftlich abgeschlossen?	Ja	Nein
4.2.5.2	Wo ist sie abgelegt/gespeichert?	.....	
4.2.6	Wie erfolgt die Rechteverwaltung?	Zentral ☐	Dezentral ☐

[4] § 6 (1) PVV

4.2.7	Wurden die erforderlichen PVP-Rechte und Rechteparameter eingerichtet?	Ja	Nein
4.2.7.1	Werden die erforderlichen Rechteprofile (PVP-Rechte und Rechteparameter) zumindest einmal jährlich überprüft?	Ja	Nein
4.2.7.2	Wann war die letzte Überprüfung?	.....	
4.2.7.2	Wurde die Struktur und Zuteilung der Rechte-profile (PVP-Rechte und Rechteparameter) schriftlich abgelegt/gespeichert?	Ja	Nein
4.2.7.3	Ist für die Rechteverwaltung der Zugriff auf die Dokumentation der verfügbaren PVP-Rechte und Rechteparameter eingerichtet?	Ja	Nein

5. Datensicherheitsmaßnahmen [5]

5.0	Wurden Datensicherheitsvorschriften (zumindest nach PV-dasi) für den Betrieb des Stammportals erlassen?	Ja	Nein
5.0.1	Wird die Einhaltung der Datensicherheitsvor-schriften regelmäßig, mindestens aber einmal jährlich überprüft?	Ja	Nein
5.0.2	Wann war die letzte Überprüfung?	.....	
5.1	Wer ist für die Einhaltung der Datensicherheits-maßnahmen im Stammportal verantwortlich (Organisationseinheit, MitarbeiterInnen)?	.....	
5.2	Wer ist für die Verwaltung der Benutzer, PVP-Rechte und Rechteparameter verantwortlich?	.....	
5.3	Gibt es dokumentierte Aufträge für Mitarbeiter, die Tätigkeiten im Stammportal ausüben (wie z.B. Betrieb, Wartung, Weiterentwicklung, Benutzer- und Rechteverwaltung)	Ja	Nein
5.3.1	Erfolgte eine Belehrung dieser Mitarbeiter über die Konventionen PVV und PV-dasi?	Ja	Nein

[5] **PV-dasi, §§ 14, 15 DSG 2000**

5.3.2	Haben diese Mitarbeiter eine Verpflichtungs-erklärung über die Einhaltung der Daten-sicherheitsbestimmungen unterfertigt? [6]	Ja	Nein
5.4	Welche Zutrittsberechtigungen zu den technischen Einrichtungen des Portals (wie z.B. Server) wurden vergeben?	.....	
5.4.1	Werden die Zutritte protokolliert?	Ja	Nein
5.4.2	In welchen Abständen erfolgt die Kontrolle?	.....	
5.4.2.1	Wann war die letzte Überprüfung?	.....	
5.5	Welche Zugriffsberechtigungen zur Administration des Stammportals wurden vergeben und wo sind sie dokumentiert?	.....	
5.5.1	Werden die Zugriffe protokolliert?	Ja	Nein
5.5.2	Sind diese Protokolle für die Verantwortlichen (Stammportalbetreiber, Anwendungsportalbe-treiber, Anwendungsverantwortlicher) verfügbar?	Ja	Nein
5.5.3	Wird die Vergabe der Zugriffsberechtigungen kontrolliert?	Ja	Nein
5.6	In welchen Abständen erfolgt eine Kontrolle der Zugriffe?	.....	
5.6.1	Wann war die letzte Überprüfung?	.....	
5.7	Wurden alle Portalbenutzer bezüglich ihrer Rechte und Pflichten belehrt (gemäß §6 Abs. 4 PVV)?	Ja	Nein
5.8	Gibt es einen Aktionsplan für sicherheitsrele-vante Ereignisse?	Ja	Nein
5.9	Ist eine Vorgangsweise für die nachträgliche Kontrolle von Zugriffen auf Anwendungen festgelegt (z.B. stichprobenartige Überprüfung von Zugriffsprotokollen)?	Ja	Nein

[6] PV-dasi letzter Absatz

6. Die Rechtevergabe für Endanwender und autonome Systemdienste [7]

6.1	Wurden nur die zur Aufgabenerfüllung unbedingt notwendigen PVP-Rechte und –parameter vergeben?	Ja	Nein
6.2	Ist eine Vorgangsweise für die Neuanlage bzw. Änderung eines Benutzers festgelegt?	Ja	Nein
6.2.1	Wo ist diese Vorgangsweise dokumentiert?	.....	
6.3	Ist eine Vorgangsweise für das Ausscheiden eines Benutzers aus der Organisationseinheit bzw. bei einer Änderung des Aufgabenbereichs des Benutzers festgelegt?	Ja	Nein
6.3.1	Wo ist diese Vorgangsweise dokumentiert?	.....	
6.4	Ist die Vorgangsweise beim Entzug der Zugriffsberechtigung festgelegt? [8]	Ja	Nein
6.4.1	Wo ist diese Vorgangsweise dokumentiert?	.....	

7. Umfang der Protokollierung im Stammportal

7.1	Werden Fehler in der Portalkommunikation protokolliert?	Ja	Nein
7.2	Werden die Nutzerdaten mit der Zutritts- bzw. Zugriffshistorie sowie den PVP-Header-Daten protokolliert?	Ja	Nein
7.3	Ist die verwendete Authentifizierung aus dem Protokoll ersichtlich?	Ja	Nein

[7] §§ 6(1), 14 DSG 2000
[8] §11 Abs. 1 PVV

II. Das Anwendungsportal

Obwohl keine ausdrückliche Verpflichtung zur Revision besteht, empfiehlt sich auch für die Anwendungsportale eine Überprüfung, ob die Vorgaben der PVV und PV-DASI eingehalten werden. Dieser Leitfaden hat daher auch eine Checkliste für die Revision von Anwendungsportalen aufgenommen.

8. Die Publikation allgemeiner Informationen und Informationen über den Betrieb des Anwendungsportals (Betriebshandbuch) [9]

(für jedes Anwendungsportal gesondert durchzuführen)

8.1	Gibt es für das Anwendungsportal festgelegte und am Reference Server publizierte Betriebszeiten?	Ja	Nein
8.1.1	Wenn ja:	Von:	Bis: .....
8.2	Wer ist der Portalbetreiber des Anwendungs-portals?	.....	
8.3	Wer ist der Ansprechpartner des Anwendungsportals:	Name: ..... E-mail:	
8.4	Hat eine Überprüfung der Aktualität der Publikation über das Angebot des Portals innerhalb des letzten Jahres stattgefunden?	Ja	Nein
8.5	Ist die Publikation richtig und aktuell?	Ja	Nein

9. Dienstleister für Aufgaben des Anwendungsportalbetreibers [10]

(entfällt, wenn kein Dienstleister für den Betrieb des Anwendungsportals herangezogen wird)

9.1	Gibt es mit dem Dienstleister eine vertragliche Vereinbarung?	Ja	Nein
9.1.1	Wo ist sie abgelegt/gespeichert?	.....	

[9] § 8 PVV
[10] § 10 PVV, § 11 DSG 2000

9.1.2	Wurde die Vereinbarung schriftlich abgeschlossen?	Ja	Nein
9.1.3	Wurde die Vereinbarung unter Einbeziehung der verantwortlichen Stellen abgeschlossen?	Ja	Nein
9.1.4	**Zum Inhalt der Vereinbarung:**		
9.1.4.1	Wurde der Dienstleister darauf hingewiesen, dass die Daten nur im Rahmen des Auftrages verwendet werden dürfen?	Ja	Nein
9.1.4.2	Welche Datensicherheitsmaßnahmen wurden seitens des Dienstleisters eingerichtet?		
9.1.4.3	Welche Kontrollmechanismen für den Auftraggeber wurden festgelegt?		
9.1.4.4	Wurde der Dienstleister darauf hingewiesen, dass Subdienstleister nur nach Genehmigung einbezogen werden dürfen und eine entsprechende Vereinbarung vorhanden sein muss?	Ja	Nein
9.1.4.5	Sind Vorkehrungen getroffen worden, damit die Pflichten des Anwendungsportalbetreibers erfüllt werden können?	Ja	Nein
9.1.4.6	Wurde die Rückgabe aller Unterlagen bei Dienstleistungsende terminlich fixiert/überprüft?	Ja	Nein

10. Protokollierung und Datensicherheitsmaßnahmen des Anwendungsportal-betreibers [11]

10.1	Wurden die Datensicherheitsmaßnahmen für die Systemkomponenten eingerichtet und dokumentiert (zumindest nach PV-dasi)?	Ja	Nein
10.2	Wurde eine Verteilung der Aufgaben zwischen Organisationseinheit und den Mitarbeitern, die im Anwendungsportal Tätigkeiten ausüben, getroffen?	Ja	Nein
10.3	Besteht eine direkte Verbindung zwischen Auftrag an diese Mitarbeiter und Datenverwendung (Rollenzuteilung)?	Ja	Nein
10.4	Welche Berechtigungen für den Zugriff auf welche Anwendungsportal-Server wurden an Portaladministratoren vergeben?		
10.5	Werden die Zugriffe der Portaladministratoren protokolliert?	Ja	Nein
10.6	Können die Protokolle für die Verantwortlichen (Stammportalbetreiber, Anwendungsportal-betreiber, Anwendungsverantwortlicher) zur Verfügung gestellt werden?	Ja	Nein
10.7.	Wird die Berechtigungsvergabe an die Portal-administratoren kontrolliert?	Ja	Nein
10.8	Erfolgte eine Belehrung dieser Mitarbeiter über die Konventionen PVV und die PV-Dasi?	Ja	Nein
10.9	Haben diese Mitarbeiter eine Verpflichtungs-erklärung über die Einhaltung der Daten-sicherheitsbestimmungen unterfertigt? [12]	Ja	Nein
10.10	Welche Zutrittsberechtigungen zu den technischen Einrichtungen des Portals (wie z.B. Server) wurden vergeben?	Ja	Nein
10.10.1	Werden die Zutritte protokolliert?	Ja	Nein

[11] § 5 PVV, PV-dasi, §§ 14, 15 DSG 2000
[12] PV-dasi letzter Absatz

10.10.2	In welchen Abständen erfolgt die Kontrolle?	.....	
10.10.3	Wann war die letzte Überprüfung?	.....	
10.11	Welche Stammportale wurden für den Zugriff auf das Anwendungsportal berechtigt?	.....	
10.11.1	Welche PVP-Rechte und -parameter wurden für diese Stammportale zur Verfügung gestellt?	.....	
10.11.2	Werden die Zugriffe des Stammportals protokolliert?	Ja	Nein
10.11.3	Können die Protokolle für die Verantwortlichen (Stammportalbetreiber, Anwendungsportal-betreiber, Anwendungsverantwortlicher) in einer zur Auswertung geeigneten Form zur Verfügung gestellt werden?	Ja	Nein
10.11.4	Wird die Vergabe von Berechtigungen an Stammportale kontrolliert?	Ja	Nein
10.11.4.1	Wann war die letzte Kontrolle?	.....	
10.11.5	Ist eine anlassbezogene Analyse der Zugriffe und BenutzerInnen anhand der Protokolldaten möglich?	Ja	Nein
10.12	Wurden die für den Betrieb des Anwendungs-portals erforderlichen Datensicherheits-vorschriften (zumindest nach PV-Dasi) erlassen?	Ja	Nein
10.13	Wird der Einhalt der Datensicherheitsvorschriften regelmäßig, mindestens aber einmal jährlich überprüft?	Ja	Nein
10.13.1	Wann war die letzte Überprüfung?	.....	
10.14	Werden Fehler bei Admin-Logins auf den Server des Anwendungsportals mitprotokolliert?	Ja	Nein

10.15	Gibt es einen Aktionsplan mit Informationspflicht der Ansprechpartner der Stammportale bei Störfällen?	Ja	Nein
10.16	Wird das abgerufene Datenvolumen regelmäßig nach auffälligen Abweichungen untersucht?	Ja	Nein
10.16.1	Wann war die letzte Überprüfung?	.....	

11. Rechte und Pflichten der Anwendungsverantwortlichen [13]

11.1	Sind die für die Anwendung vorgeschriebenen Informationen über die Anwendung publiziert? [14]	Ja	Nein
11.1.1	Wurde für die Anwendung ein Betriebshandbuch zur Verfügung gestellt?	Ja	Nein
11.1.2	Sind die publizierten Informationen aktuell?	Ja	Nein
11.2	Ist die Vorgangsweise betreffend den Entzug von Zugriffsberechtigungen geregelt? [15]	Ja	Nein
11.2.1	Vorgangsweise beim Ausschluss einzelner Benutzer von der weiteren Kommunikation mit dem Anwendungsportal?	Ja	Nein
11.2.2	Vorgangsweise beim Ausschluss einzelner Benutzer vom Zugriff auf eine Anwendung?	Ja	Nein
11.2.3	Vorgangsweise beim Ausschluss eines Stammportals von der weiteren Kommunikation mit dem Anwendungsportal?	Ja	Nein
11.2.4	Wo ist dies dokumentiert?	.....	

[13] §§ 4, 11 PVV
[14] § 4 (5) PVV
[15] §11 PVV