Informationssicherheit bei EfA-Nachnutzung

Eigenerklärung der EfA- Dienstleister sowie Plausibilitätsprüfung durch die zentrale Stelle des bereitstellenden Landes

1. Eigenerklärung – Muster mit Inhalten und Checkliste

Gemäß § 2 Abs. 12 der Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (IT-Sicherheitsverordnung Portalverbund - ITSiV-PV) ist die Umsetzung der Maßnahmen für die IT-Komponenten im Portalverbund durch eine jährliche Eigenerklärung der für die jeweilige IT-Komponente verantwortlichen Stelle zu dokumentieren. Die nachfolgende Checkliste orientiert sich an der Eigenerklärung und passt diese zielgerichtet für die EfA-Nachnutzung an.

a. Kurzbeschreibung des hier betrachteten Informationsverbundes

In wenigen Sätzen sollen der Verbund und die Abgrenzung zu nicht betrachteten Bestandteilen vorgenommen werden.

b. Schutzbedarfseignung

Schutzziel	Schutzbedarf	Servicelevel-Ableitung
Verfügbarkeit	☐ normal ☐ hoch ☐ sehr hoch	Maximale Ausfallzeit:
Vertraulichkeit	☐ normal ☐ hoch ☐ sehr hoch	
Integrität (Authentizität – NIS2?)	☐ normal ☐ hoch ☐ sehr hoch	
Gesamt	☐ normal ☐ hoch ☐ sehr hoch	

c. Checkliste

Vorgabe für betrachteten EfA-online-Dienst	Status der Umsetzung	Bemerkungen/Begründung (sofern nicht vollständig umgesetzt)
Es liegt eine nähere Beschreibung des angebotenen Dienstes und eine Anleitung zur Nutzung öffentlich einsehbar vor.	☐ vollständig ☐ teilweise ☐ entbehrlich (zu begründen)	Bitte URL angeben:
Die ***TR-03160*** *Servicekonten* wird in der geltenden Fassung umgesetzt.	☐ vollständig ☐ teilweise ☐ entbehrlich (zu begründen)	
Die ***TR-03107-1*** *Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1* wird in der geltenden Fassung umgesetzt.	☐ vollständig ☐ teilweise ☐ entbehrlich (zu begründen)	
Die ***TR-03147*** *Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen* wird in der geltenden Fassung umgesetzt.	☐ vollständig ☐ teilweise ☐ entbehrlich (zu begründen)	
Die ***TR-03116-4*** *kryptographische Vorgaben für Projekte der Bundesregierung Teil 4* wird in der geltenden Fassung umgesetzt.	☐ vollständig ☐ teilweise ☐ entbehrlich (zu begründen)	
Der betrachtete Informationsverbund des Dienstes unterliegen einem **ISMS** gemäß der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-PLR.	☐ vollständig ☐ teilweise	Wie wird sichergestellt, dass der Dienst in das ISMS des Anbieters eingebunden ist?
Für den betrachteten Informationsverbund des Dienstes ist ein **Sicherheitskonzept** gemäß BSI-Standards (Standard-Absicherung) **erstellt und wird umgesetzt.**	☐ vollständig ☐ teilweise	Welches Datum hat die aktuelle Version?
Wann wurden die **Penetrationstests** für die in § 2 Abs. 6 IT-SiVo-PV genannten IT-Komponenten durchgeführt?	Datum des letzten Tests:	Wurden kritische schwerwiegende Mängel festgestellt und behoben?

Webchecks für die in § 2 Abs. 6 IT-SiVo-PV genannten IT-Komponenten wurden durchgeführt.	Datum des letzten Tests:	Wurden kritische schwerwiegende Mängel festgestellt und behoben?
Der betrachtete Informationsverbund des Dienstes unterliegt einem **IT-Notfallmanagement**, das die Anforderungen der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-PLR erfüllt.	☐ vollständig ☐ teilweise ☐ nicht begonnen	Anforderung wird umgesetzt bis:

d. Notwendige Ergänzungen aus anderen Compliance-Anforderungen

Vorgabe	**Status der Umsetzung**	**Bemerkungen**
Der Datenaustausch über die Verwaltungsgrenze wird gemäß den Vorgaben des IT-NetzG über das Verbindungsnetz realisiert?	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Bei kritischen ebenenübergreifenden IT-Verfahren ist im Rahmen der Notfallvorsorge ein Prozess etabliert, welcher festlegt, ob und welche gemeinsamen Rückfallebenen für das jeweilige IT-Verfahren notwendig und möglich sind. (ISLL, bestätigt durch Abs. 11 IT-SiVO-PV)	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Anforderung wird umgesetzt bis:
Der Online-Dienst MUSS über eine security.txt gemäß RFC 9116 verfügen. Ein interner Prozess zum Umgang mit Responsible-Disclosure-Meldungen muss etabliert sein.	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	
IT-Sicherheit Maßnahmen sind nach dem Stand der Technik §2 Abs.2 IT-SiV-PV für Portalverbund und unmittelbar angebundene IT-Komponenten getroffen. ***(eine Konkretisierung erfolgt in TR Portalverbund 03172 (2))***	☐ vollständig ☐ teilweise ☐ nicht begonnen ☐ entbehrlich	Einerseits Einschränkung auf PV, andererseits nochmals auf Aktualisierung/KVP drängend

Die ausgefüllte Eigenerklärung ist an Nachnutzende zu übermitteln bzw. bereitzustellen, um Transparenz für Nachnutzende zu erzeugen. Es erfolgt jedoch keine Einsichtnahme aller nachnutzender Einrichtungen in das Sicherheitskonzept o.ä. Dokumente.

Die Klassifizierung der ausgefüllten Checkliste sollte vorgenommen werden. Sie wird in der Regel VS-NUR FÜR DEN DIENSTGEBRAUCH einzustufen sein.

2. Zusatzinformationen für die Risikobewertung der Nachnutzenden

a. Angaben zu nicht umgesetzten Anforderungen aus dem Sicherheitskonzept

Nicht umgesetzte Grundschutz-Anforderungen	Anzahl	Umsetzungszeitraum
Basisanforderungen		
Standardanforderungen		

Die Darstellung der Restrisiken, die auf nachnutzende Einrichtungen aufgrund nicht umgesetzter Grundschutz-Anforderungen entfallen, sind hier als Nutzungshinweise, ggf. mit konkreten Empfehlungen zur Risikominimierung aufzunehmen.
Ebenso soll hier der Dienstleister in Abgrenzung seines Verantwortungsbereiches einen Haftungsausschluss definieren und Empfehlungen des Sicherheitskonzeptes zu dezentralen Maßnahmen darstellen. Dadurch soll eine Verantwortungsabgrenzung erfolgen, aber auch die Erkenntnisse des zentralen Sicherheitskonzepts für die nachnutzenden Einrichtungen sinnvoll aufbereiten um die Sicherheitslücken beim Übergang der Verantwortungsbereiche so gering wie möglich zu halten.

Maßnahme / Risiko / Bedeutung für Sicherheitsniveau	Empfehlung

b. Einrichtung von Kommunikationspartnern für sicherheitsrelevante Ereignisse

Um Informationsflüsse bei sicherheitsrelevanten Erkenntnissen transparent zu gestalten und gleichzeitig auch die Kommunikation des Dienstleisters an alle nachnutzenden Einrichtungen zu gewährleisten, ist eine Meldestelle beim Dienstleister für Sicherheitsvorfälle einzurichten und eine Registrierung der Empfänger für sicherheitsrelevante Hinweise zu ermöglichen.

Meldestelle für Sicherheitsvorfällen	Registrierungsadresse für Sicherheitshinweise
Bitte Kontaktmöglichkeiten eintragen	

Sicherheitsmeldungen sind parallel über den VerwaltungsCERT-Verbund (VCV) entsprechend der dort vereinbarten Systematik zu melden und zu behandeln.

3. Bestätigung der Erklärung durch vertrauenswürdige Stelle/ Prüfmechanismus

Die Eigenerklärung wird durch die zentrale Stelle i.S.v. §2 Abs. 13 ITSiV-PV entgegengenommen. Sie ist spätestens sechs Wochen nach der Durchführung des erforderlichen Penetrationstest der zentralen Stelle zu übergeben. Eine Aktualisierung der Erklärung ist jährlich vorzunehmen und der zentralen Stelle sind die Änderungen mitzuteilen.

Die zentrale Stelle im Land/Bund sammelt die zugegangenen Eigenerklärungen und führt eine Plausibilitätsprüfung durch.