Anlage 1: Zusätzliche Anforderungen für Dienstleistercluster „DL01 Beratung und Projektmanagement“

Die folgenden Dienstleistungen sind dem Dienstleistercluster DL01 zugeordnet:

- IKT-Projektmanagement
- IKT-Beratung
- IKT-Helpdesk und Unterstützung auf erster Ebene
- IKT-Risikomanagement
- Beratung

1 Einleitung

Folgende Anforderungen gelten für Mitarbeitende des Auftragnehmers, insofern diese IKT-Assets der ILB nutzen oder auf diese zugreifen.

2 Generelle Sicherheitsthemen

2.1 Vorfallmanagement

1. Der Auftragnehmer verpflichtet seine Mitarbeitende, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit und anomale Verhaltensweisen rechtzeitig zu melden. Die mit der ILB vereinbarten Meldemechanismen sind zu kennen und einzuhalten.
2. Der Dienstleister informiert die ILB umgehend, sobald potenzielle Sicherheitsvorfälle gemeldet werden, die die Informationssicherheit der ILB beinträchtigen könnten und stellt der ILB alle relevanten Unterlagen zur Verfügung.
3. Der Dienstleister hat standardisierte Protokolle und Berichte zur Meldung von Sicherheitsvorfällen zu etablieren.
4. Für Erst-, Folge- und Erledigungsmeldungen zu Informationssicherheitsvorfällen gelten folgende formalen Anforderungen:
   - Kurzbeschreibung
   - Betroffener Service / Asset
   - Bearbeitungsstatus
   - Detailbeschreibung
   - Betroffenes Schutzziel
   - Ursachenbeschreibung
   - Datenschutzbeurteilung
   - Eingeleitete Sofortmaßnahmen
   - Lessons Learned

2.2 Personalsicherheit

1. Der Dienstleister verpflichtet seine Mitarbeitende zur Einhaltung der Vertraulichkeitspflichten und zur Bewahrung etwaiger Geschäftsgeheimnisse während und nach der Durchführung von Aufgaben für die ILB.
2. Der Dienstleister muss einen Ansprechpartner benennen, der für alle Fragen der Einbindung bei der ILB aussagefähig ist und bei Bedarf Aktionen zur Sicherstellung der sicheren Einbindung initiieren kann.
3. Die Beschäftigten des Dienstleisters müssen schriftlich verpflichtet werden, einschlägige Gesetze, Vorschriften sowie die Regelungen der ILB einzuhalten.
4. Der Auftragnehmer verpflichtet sich, dass seine Mitarbeitende die Richtlinien, Verfahren und Protokolle der ILB zur Informations- und IKT-Sicherheit einhalten.
5. Der Auftragnehmer stellt für seine eingesetzten Mitarbeiter sicher, dass es Vertretungsregelungen existieren.

6. Der Auftragnehmer verpflichtet sich, sofern zutreffend, dass seine Mitarbeitende alle verwendeten IKT-Assets und materiellen Informationswerte im Eigentum der ILB nach Beendigung der Dienstleistung aushändigen.

ab Schutzbedarf „hoch“

7. Der Dienstleister stellt sicher, dass die Beschäftigten geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit unterrichtet wurden.
8. Der Dienstleister stellt sicher, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird.

2.3 Schutz vor Schadprogrammen

1. Der Dienstleister stellt auf allen Systemen seiner eingesetzten Mitarbeiter einen Schutz vor Schadsoftware sicher.
2. Jede Datei, die auf dieses System übertragen wird, muss durch einen On-Access-Scanner sofort untersucht werden.
3. Zusätzlich sind regelmäßig bzw. mindestens wöchentlich Scans aller gespeicherten Daten durchzuführen.
4. Die Muster für die Schadprogrammerkennung sind nach den Vorgaben des Herstellers zu aktualisieren.

ab Schutzbedarf „hoch“

5. Der für die ILB relevante Netzverkehr muss auf Schadsoftware hin untersucht werden.
6. Alle Meldungen über erkannte Schadsoftware sind an die ILB zu übermitteln.

2.4 Fernzugriff

1. Für den Fernzugriff auf die für die ILB relevanten Systeme muss der Dienstleister sicherstellen, dass sichere Authentisierungsmechanismen genutzt werden und jeder Nutzer eindeutig identifizierbar ist.
2. Die Außenverbindung muss bei einem Fernzugriff auf die für die ILB relevanten Systeme verschlüsselt sein.
3. Es muss sichergestellt werden, dass die Dienstleister nur Zugriff auf die für sie relevanten Dienste, IT-Systeme, Anwendungen und Netzbereiche haben.
4. Alle versuchten und erfolgreichen Fernzugriffe auf die für die ILB relevanten Systeme müssen durch den Dienstleister protokolliert werden.

ab Schutzbedarf „hoch“

5. Ein Fernzugriff auf die für die ILB relevanten Systeme darf nur nach erfolgter 2-Faktor-Authentifizierung erfolgen.

2.5 Austausch von Informationen/Daten

1. Beim Austausch von Daten zwischen dem Dienstleister und der ILB müssen die für den Schutz der Daten notwendigen Aspekte vereinbart werden.

   Dies betrifft insbesondere:

   - Art der Daten
   - Zweck der Nutzung der Daten
   - erlaubte Kommunikationspartner pro Art der Daten
   - Datenformate
   - Vorgehensweisen zum sicheren Datenaustausch
   - Verfügbarkeiten
   - Reaktionszeiten

2.6 Einbindung des Dienstleisters

1. Wenn das Datennetz der ILB an das Datennetz des Dienstleisters angebunden wird, müssen alle sicherheitsrelevanten Aspekte vereinbart werden.
2. Es muss durch den Dienstleister dokumentiert werden, wie die Vereinbarungen für die Netzanbindung eingehalten werden.
3. Es muss sichergestellt werden, dass alle ggf. notwendigen Anpassungen der Schnittstellen, der Netzanbindung, des Administrationsmodells sowie des Datenmanagementmodells dokumentiert werden.
4. Es muss sichergestellt werden, dass alle Schnittstellen zwischen der ILB und dem Dienstleister ausreichend Bandbreite haben.

2.7 Löschung und Vernichtung

5. Es muss festgelegt werden, wie alle Informationen, Daten und ggf. Hardware der ILB vom Dienstleister zurückgegeben werden.
6. Im Falle einer Beendigung des Vertrages muss der Dienstleister sicherstellen, dass alle Daten der ILB vernichtet oder an die ILB zurückgegeben werden. Hierbei sind gesetzliche Vorgaben zur Aufbewahrung von Daten zu beachten.

ab Schutzbedarf „hoch“

7. Alle Datenträger, die Daten der ILB enthalten und nicht mehr benötigt werden oder defekt sind, sind durch den Dienstleister angemessen zu vernichten. Die ILB erhält entsprechende Nachweise der Vernichtung.