Mindestanforderung der Informationssicherheit an Auftragnehmer

- Der Dienstleister SOLL sein Informationssicherheitsmanagement an einem anerkannten Standard „**orientieren" (bei Verarbeitung von Daten mit Schutzbedarf von mindestens Hoch: „muss etabliert sein")**, z.B. ISO27001, BSI Grundschutz, NIST SP 800 und Umsetzung adäquater Maßnahmen nachweisen.
    - Die beauftragte Leistung muss von den Maßnahmen abgedeckt werden.
- Der Informationssicherheitsstandard umfasst alle Aufgaben, die zur Einhaltung der Schutzziele im Informationssicherheitsmanagement erforderlich sind.
- Der Dienstleister MUSS die vertraglich vereinbarten Regelungen und Sicherheitsanforderungen ebenfalls bei der Leistungserbringung durch einen Subdienstleister gewährleisten.
- Die beauftragten Subdienstleister sind der MUL-CT bekannt zu geben.
- Der Dienstleister SOLL der MUL-CT die jeweils aktuellen Kontaktdaten der fachlich verantwortlichen Mitarbeiter in betrieblicher Hinsicht und mindestens des Informationssicherheitsbeauftragten zur Verfügung stellen.
- Der Dienstleister MUSS im Rahmen des Security-Incident-Managements:
    - Den ISB der MUL-CT unverzüglich über erkannte und die MUL-CT betreffende Informationssicherheitsvorfälle, unter Vorlage aller verfügbaren und für einen sachkundigen Dritten zur Nachvollziehbarkeit relevanten Hintergrundinformationen, zu informieren;
    - bei Gefahr im Verzug geeignete und angemessene Maßnahmen zu ergreifen, um die MUL-CT vor dieser Gefahr zu schützen und alle ergriffenen Maßnahmen nachvollziehbar zu dokumentieren und die Dokumentation der MUL-CT auf Anfrage bereitzustellen.
    - die MUL-CT auf Anfrage bei Untersuchungen von Informationssicherheitsvorfällen zu unterstützen und sicherheitsrelevante Informationen auf Anfrage an die MUL-CT herauszugeben, sofern sie für das Vertragsverhältnis relevant sind.
    - Der Dienstleister verpflichtet, geeignete Ressourcen/Reaktionszeiten zur Abwicklung von Störungen, Ereignissen oder Vorfälle bereitzustellen.
- Der Ort der Datenverarbeitung ist zu benennen und vertraglich zu dokumentieren. Der Dienstleister ist zu verpflichten, Veränderungen der MUL-CT vorab anzuzeigen.
- Die Datenverarbeitung MUSS im Einklang mit der EU Datenschutz Grundverordnung stehen.

SaaS

- Der Zugang aus öffentlichen Netzen sollte per starker Authentifizierung abgesichert werden.
- Im System bzw. beim Anbieter muss eine Mandantentrennung vorgenommen werden, sofern nicht dezidierte Leistungen für die MUL-CT erbracht werden.
- Der Serviceanbieter muss eine Möglichkeit zur Aufzeichnung sämtlicher Tätigkeiten auf der administrativen Schnittstelle (Auditprotokoll) anbieten.
- Der Leistungsumfang des Dienstleisters muss geeignete Maßnahmen zur System- und Netzwerktrennung abdecken, sofern diese nicht Bestandteil der Leistung selbst ist.

Fernwartung

- Zur Fernwartung ist die etablierte PAM Lösung der MUL-CT zu nutzen.
- Es sind grundsätzlich die Anforderung entsprechend des Vertrag Netzwerkverbindung MUL-CT (vgl. Anlage) anzuwenden

Anforderungen an beauftragte Systeme bei Verarbeitung von Daten mit sehr hohem Schutzbedarf

- Identitäts- und Berechtigungskontrolle:
    - Das System muss sich dem MUL-CT-Berechtigungsprozess und -konventionen unterordnen. Das Rollen- und Berechtigungsmodell muss die Entitäten des zentralen Berechtigungssystems der MUL-CT als Grundlage nehmen.
    - Berechtigungen, insbesondere Rollen und Rechte des IT-Systems, müssen den Prinzipien: Need-to-Know und Least Privilege gerecht werden.
- Systemaudit / Protokollierung
    - Ereignisse, welche für das IT-System betrieblich kritisch oder maßgeblich einschränkend sind, müssen definiert und kontinuierlich überwacht werden.
    - Die notwendigen betrieblichen Zustände sollen zur Überwachung in das Betriebsmonitoring der MUL-CT integriert sein.
    - Jegliche Änderungen an „hoch schützenswerten Daten" müssen integer überprüfbar und auswertbar sein.
    - Es müssen geeignete Maßnahmen ergriffen werden, damit Protokolldaten integer und zeitsynchron verarbeitet werden.
- Kommunikation / Netzwerk
    - Kommunikationsverbindungen müssen anwendungsorientiert im Sinne des Netzwerktrennungskonzeptes der MUL-CT getrennt werden.
    - Kommunikationsverbindungen müssen immer nach aktuellem Stand der Technik transportverschlüsselt werden (derzeit min. TLS 1.2, IPSEC oder vergleichbar).
    - Extern gerichtete Schnittstellen, welche den Informationsraum der MUL-CT verlassen, müssen immer über das mehrstufige Sicherheitsgateway der MUL-CT geführt werden.
    - Remote-Zugriff erfolgt grundsätzlich über einen VPN-Zugang und richtet sich nach den technischen Vorgaben der MUL-CT: Verfahren und Software müssen mit der MUL-CT abgestimmt werden.
- Das System muss einen Anti-Malware-Schutz etablieren und in die Anti-Malware-Architektur der MUL-CT eingliedern. Signaturen müssen mindestens einmal täglich aktualisiert werden.
- Systemkomponenten müssen nach Schutzbedarf geeignet getrennt werden.
- Systemhärtung nach Stand der Technik: Grundsätzlich sollen nur Dienste und Kommunikationsbeziehungen ermöglicht werden, welche im Betrieb benötigt werden.
    - Systemhärtungskonzepte der MUL-CT, insbesondere für Server und Clients, müssen berücksichtigt werden. (vgl. SOP Härtung von IT-Systemen)

    - Schutz verarbeiteter Daten und der Kommunikation durch geeignete Kryptographische Verfahren (vgl. SOP Kryptographische Verwendung und Schlüsselverwaltung)
    - Die Konfiguration der Komponenten des IT-Systems soll nach Herstellervorgaben vorgenommen und unter Sicherheitsgesichtspunkten bewertet und dokumentiert bzw. durch den ISB abgenommen werden.
    - Sind für das zu härtende System CIS Benchmarks vorhanden, sind die Anforderungen der Profile CIS Level 1 und Level 2 umzusetzen.
- Es müssen geeignete Maßnahmen getroffen werden, damit ein Datenverlust über den tolerierbaren Datenverlust hinaus vermieden wird.
- Maßnahmen zur Umsetzung des sicheren Löschens von Daten müssen etabliert sein.
- Zentraler Betrieb:
    - Das IT-System muss den Anforderungen hinsichtlich Verfügbarkeit unter Berücksichtigung der zentralen Basis-IT-Architektur gerecht werden.
    - Der Betrieb der zentralen Komponenten des IT-Systems muss in der RZ-Umgebung der MUL-CT erfolgen.
- Die Verträglichkeit zum eingesetzten Intrusion Detection System der MUL-CT muss geprüft werden und Rahmenbedingungen zu deren Einsatz definiert werden.
- Mobile Client – Infrastruktur:
    - Eine Verarbeitung von hoch schützenswerten Informationen auf mobilen Clients muss in einer geschützten Umgebung erfolgen.
    - Die Clients des IT-Systems müssen zentral verwaltet sein.
- Der Datenabfluss muss durch geeignete Maßnahmen überwacht und auf ein Mindestmaß reduziert werden. Nicht erforderliche Kopier- oder Abruftransaktionen müssen technisch unterbunden werden.
- Ein Zugriff aus fremden Netzwerken auf hoch schützenswerte Informationen bedarf:
    - einer Multi-Faktor-Authentisierung oder Conditional Access
    - eines kontrollierten Zugriffs über eine mehrstufige Sicherheitsarchitektur (Ein direkter Zugriff auf Nutzdaten mit sehr hohem Schutzgehalt darf von extern nicht erfolgen.)
    - eines regelmäßigen Penetrationstests, insbesondere vor der Freigabe des IT-Systems