784.131

Liechtensteinisches Landesgesetzblatt

Jahrgang 2025 Nr. 163 ausgegeben am 30. Januar 2025

# Cyber-Sicherheitsverordnung (CSV)

vom 14. Januar 2025

Aufgrund von Art. 3 Abs. 2 Bst. a Ziff. 5, Art. 4 Abs. 7, Art. 6 Abs. 6, Art. 11 Abs. 3, Art. 15 Abs. 3, Art. 19 Abs. 3, Art. 20 Abs. 4 und Art. 25 des Cyber-Sicherheitsgesetzes (CSG) vom 5. Dezember 2024, LGBl. 2025 Nr. 111, verordnet die Regierung:

## I. Allgemeine Bestimmungen

Art. 1

*Gegenstand und Zweck*

1) Diese Verordnung regelt in Durchführung des Cyber-Sicherheitsgesetzes das Nähere zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen, insbesondere:

a) die zu ergreifenden Risikomanagementmassnahmen;

b) die Berichtspflichten nach Art. 6 und 9 des Cyber-Sicherheitsgesetzes;

c) die Anforderungen an qualifizierte Dritte nach Art. 11 Abs. 2 des Cyber-Sicherheitsgesetzes;

d) die Zusammenarbeit und den Informationsaustausch der Stabsstelle Cyber-Sicherheit mit anderen inländischen Behörden und Stellen;

e) die Durchführung von Kontrollen nach Art. 19 des Cyber-Sicherheitsgesetzes.

2) Sie dient der Umsetzung bzw. Durchführung folgender EWR-Rechtsvorschriften:

a) Richtlinie (EU) 2022/2555 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union[1];

b) Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren[2];

c) Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik[3].

3) Die gültige Fassung der EWR-Rechtsvorschriften, auf die in dieser Verordnung Bezug genommen wird, ergibt sich aus der Kundmachung der Beschlüsse des Gemeinsamen EWR-Ausschusses im Liechtensteinischen Landesgesetzblatt nach Art. 3 Bst. k des Kundmachungsgesetzes.

## Art. 2

### *Bezeichnungen*

Unter den in dieser Verordnung verwendeten Personenbezeichnungen sind alle Personen unabhängig ihres Geschlechts zu verstehen, sofern sich die Personenbezeichnungen nicht ausdrücklich auf ein bestimmtes Geschlecht beziehen.

---

1 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80)

2 Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1)

3 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15)

## II. Risikomanagementmassnahmen

### Art. 3

*Grundsatz*

1) Wesentliche und wichtige Einrichtungen gewährleisten mit den technischen, operativen und organisatorischen Risikomanagementmassnahmen im Bereich der Cybersicherheit nach dem Anhang ein den bestehenden Risiken angemessenes Sicherheitsniveau der Netz- und Informationssysteme und schützen diese vor Sicherheitsvorfällen und Cyberbedrohungen.

2) Hält eine wesentliche oder wichtige Einrichtung es für nicht angemessen, nicht anwendbar oder nicht durchführbar, bestimmte im Anhang vorgesehene technische, operative und organisatorische Risikomanagementmassnahmen im Bereich der Cybersicherheit zu ergreifen, hat die betreffende Einrichtung eine diesbezügliche Begründung in verständlicher Weise zu dokumentieren.

3) Die Bestimmungen der Durchführungsverordnung (EU) 2024/2690[4] bleiben in Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmassnahmen für DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter vorbehalten.

4 Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmassnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt (ABl. L 2024/2690 vom 18.10.2024)

## III. Berichtspflichten

Art. 4

*Erhebliche Sicherheitsvorfälle*

1) Bei der Beurteilung des Ausmasses eines Sicherheitsvorfalls als erheblich nach Art. 6 des Cyber-Sicherheitsgesetzes berücksichtigen die wesentlichen und wichtigen Einrichtungen zumindest die folgenden sektorübergreifenden Faktoren:

a) die Bedeutung der betroffenen Netz- und Informationssysteme für die Erbringung der Dienste der Einrichtung;

b) den direkten verursachten finanziellen oder allfälligen Verlust, welcher durch den Sicherheitsvorfall verursacht werden kann;

c) das Ausmass der Auswirkungen oder der Beeinträchtigung auf wirtschaftliche und gesellschaftliche Tätigkeiten;

d) die Möglichkeit oder den Eintritt der Schädigung der Gesundheit oder des Todes einer natürlichen Person;

e) die Zahl der von einem Sicherheitsvorfall betroffenen natürlichen oder juristischen Personen (Nutzer);

f) die geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte;

g) die Dauer des Sicherheitsvorfalls bzw. gegebenenfalls die Dauer der Nichtverfügbarkeit des erbrachten Dienstes der betreffenden Einrichtung;

h) dem Sicherheitsvorfall zugrunde liegende Schwachstellen.

2) Mehrere Sicherheitsvorfälle, die einzeln betrachtet nach Abs. 1 nicht als erhebliche Sicherheitsvorfälle beurteilt werden, gelten zusammen als ein erheblicher Sicherheitsvorfall, wenn sie innerhalb von sechs Monaten mindestens zwei Mal auftreten und dieselbe offensichtliche Ursache haben.

Art. 5

*Bearbeitung von Meldungen*

1) Meldungen zu Sicherheitsvorfällen, Cyberbedrohungen oder Beinahe-Vorfällen nach Art. 6 oder 9 des Cyber-Sicherheitsgesetzes werden durch das bei der Stabsstelle Cyber-Sicherheit eingerichtete Computer-Notfallteam (CSIRT) bearbeitet.

2) Informationen zu gemeldeten Sicherheitsvorfällen, Cyberbedrohungen oder Beinahe-Vorfällen, wie insbesondere Kompromittierungsindikatoren, können vom CSIRT an externe Stellen übermittelt werden, um:

a) die Kompromittierung von Systemen festzustellen;

b) herauszufinden, welche Daten oder Systeme von einer Kompromittierung betroffen sind;

c) die Schwere von Sicherheitsvorfällen einzuschätzen;

d) Hinweise zu den von Angreifern verwendeten Angriffsvektoren und Werkzeugen zur Verfügung zu stellen, damit Bedrohungen vermindert oder beseitigt werden können;

e) Schwachstellen in Systemen zu identifizieren;

f) gezielte Gegenmassnahmen zu entwickeln, damit künftige Angriffe verhindert werden können.

# IV. Organisation und Durchführung

## A. Qualifizierte Dritte

### Art. 6

*Anforderungen*

1) Qualifizierte Dritte, die mit Aufgaben der Stabsstelle Cyber-Sicherheit oder des CSIRT nach Art. 11 Abs. 2 des Cyber-Sicherheitsgesetzes, insbesondere mit der Durchführung von Kontrollen nach Art. 19 des genannten Gesetzes, beauftragt werden, müssen:

a) von den zu prüfenden wesentlichen oder wichtigen Einrichtungen unabhängig sein; und

b) über die erforderlichen Kenntnisse zur Erfüllung der ihnen auferlegten Aufgaben verfügen.

2) Sie haben die erforderlichen Kenntnisse nach Abs. 1 Bst. b durch einschlägige Qualifikationen, gegebenenfalls durch entsprechende Zertifizierungen, auf Verlangen der Stabsstelle Cyber-Sicherheit nachzuweisen.

3) Die Stabsstelle Cyber-Sicherheit kann qualifizierte Dritte verpflichten, sich einer Sicherheitsprüfung zu unterziehen, die von einer qualifizierten, unabhängigen Stelle durchgeführt wird, und deren Ergebnisse zu übermitteln. Die Kosten der Sicherheitsprüfung tragen die qualifizierten Dritten.

## B. Zusammenarbeit und Informationsaustausch mit inländischen Behörden

Art. 7

*Zusammenarbeit und Informationsaustausch mit der FMA*

1) Die Stabsstelle Cyber-Sicherheit arbeitet, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, mit der Finanzmarktaufsicht (FMA) im Hinblick auf die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen zusammen und kann zu diesem Zweck Informationen austauschen.

2) Vom Informationsaustausch können umfasst sein:

a) bei der FMA oder bei der Stabsstelle Cyber-Sicherheit eingegangene Meldungen zu Sicherheitsvorfällen sowie IKT-bezogenen Vorfällen oder Hinweise zu Cyberbedrohungen aus den Sektoren Bankwesen und Finanzmarktinfrastrukturen;

b) Informationen, die der FMA oder der Stabsstelle Cyber-Sicherheit im Rahmen der Erfüllung ihrer jeweiligen Aufgaben übermittelt werden;

c) Informationen über ausserordentliche Vorkommnisse im Cyberraum.

3) Die Stabsstelle Cyber-Sicherheit kann die FMA um Unterstützung bei der Überprüfung der Risikomanagementmassnahmen und der Einhaltung der Berichtspflichten nach Art. 4 und 6 des Cyber-Sicherheitsgesetzes ersuchen. Die FMA kann im Rahmen ihrer Befugnisse die Überprüfungen oder Ermittlungen selbst vornehmen oder durch beauftragte Sachverständige vornehmen lassen.

Art. 8

*Zusammenarbeit und Informationsaustausch mit dem Amt für Kommunikation*

1) Die Stabsstelle Cyber-Sicherheit arbeitet zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen mit dem Amt für Kommunikation zusammen, insbesondere:

a) hinsichtlich sämtlicher Einrichtungen in den Sektoren "Digitale Infrastruktur", "Weltraum" und "Post- und Kurierdienste";

b) in den Fachbereichen, für die das Amt für Kommunikation zuständig ist.

2) Die Amtsstellen können im Rahmen ihrer Zusammenarbeit nach Abs. 1 Informationen austauschen. Vom Informationsaustausch können umfasst sein:

a) beim Amt für Kommunikation oder bei der Stabsstelle Cyber-Sicherheit eingegangene Meldungen, Mitteilungen oder Informationen zu Sicherheitsvorfällen, Cyberbedrohungen oder Beinahe-Vorfällen in den genannten Sektoren;

b) Informationen über ausserordentliche Vorkommnisse im Cyberraum.

3) Die Stabsstelle Cyber-Sicherheit und das Amt für Kommunikation informieren sich gegenseitig innerhalb von 24 Stunden über den Eingang von Meldungen betreffend relevante Sicherheitsvorfälle bei Vertrauensdiensteanbietern.

4) Die Stabsstelle Cyber-Sicherheit kann das Amt für Kommunikation um Unterstützung bei der Überprüfung der Risikomanagementmassnahmen und der Einhaltung der Berichtspflichten nach Art. 4 und 6 des Cyber-Sicherheitsgesetzes ersuchen. Das Amt für Kommunikation kann im Rahmen ihrer Befugnisse die Überprüfungen oder Ermittlungen selbst vornehmen oder durch beauftragte Sachverständige vornehmen lassen.

## Art. 9

*Zusammenarbeit und Informationsaustausch mit der Landespolizei*

Die Stabsstelle Cyber-Sicherheit arbeitet zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen mit der Landespolizei zusammen, insbesondere:

a) beim Informationsaustausch über ausserordentliche Vorkommnisse im Cyberraum;

b) bei der technischen Unterstützung, indem vorhandene Ressourcen bei Bedarf geteilt und gegenseitig zur Verfügung gestellt werden;

c) bei der Teilnahme zu Übungen und Schulungen.

## Art. 10

*Zusammenarbeit und Informationsaustausch mit der Staatsanwaltschaft*

Die Stabsstelle Cyber-Sicherheit arbeitet zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen mit der Staatsanwaltschaft, insbesondere beim Informationsaustausch über ausserordentliche Vorkommnisse im Cyberraum, zusammen.

Art. 11

*Zusammenarbeit und Informationsaustausch mit der Stabsstelle FIU*

1) Die Stabsstelle Cyber-Sicherheit arbeitet zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen mit der Stabsstelle FIU zusammen, insbesondere bei:

a) der strategischen Risikoanalyse;

b) der Durchsetzung internationaler Sanktionen sowie der Vermittlung von und den Handel mit Kriegsmaterial, nuklearen Gütern, radioaktiven Abfällen, doppelt verwendbaren Gütern und besonderen militärischen Gütern.

2) Für die Zwecke nach Abs. 1 übermitteln sich die Stabsstelle Cyber-Sicherheit und die Stabsstelle FIU die hierfür notwendigen Informationen und Unterlagen, einschliesslich personenbezogener Daten, soweit diese nicht von Art. 6 Abs. 2 des FIU-Gesetzes erfasst sind.

3) Die Stabsstelle Cyber-Sicherheit schliesst nach Rücksprache mit dem zuständigen Regierungsmitglied mit der Stabsstelle FIU eine Vereinbarung über die weiteren Modalitäten der Zusammenarbeit nach Art. 15 Abs. 2 des Cyber-Sicherheitsgesetzes ab.

## C. Kontrollen

Art. 12

*Allgemeines*

1) Die Stabsstelle Cyber-Sicherheit kann jederzeit Kontrollen nach Art. 19 Abs. 1 des Cyber-Sicherheitsgesetzes durchführen oder durch qualifizierte Dritte durchführen lassen.

2) Kontrollen nach Abs. 1 sind vorgängig durch die Stabsstelle Cyber-Sicherheit anzukündigen; ausgenommen bei Vorliegen von Gefahr in Verzug.

Art. 13

*Umfang und Ablauf*

1) Die Stabsstelle Cyber-Sicherheit legt vor der Durchführung einer Kontrolle deren Umfang in Abstimmung mit der zu kontrollierenden Stelle fest. Bei einer Kontrolle wird insbesondere festgestellt, ob:

a) geeignete und verhältnismässige technische, operative und organisatorische Massnahmen zum Schutz der Netz- und Informationssysteme ergriffen wurden;

b) die Risikomanagementmassnahmen nach dem Cyber-Sicherheitsgesetz und dieser Verordnung eingehalten werden;

c) die Berichtspflichten nach Art. 6 des Cyber-Sicherheitsgesetzes eingehalten wurden.

2) In begründeten Fällen kann die Stabsstelle Cyber-Sicherheit den Umfang während einer laufenden Kontrolle erweitern oder einschränken.

3) Die Stabsstelle Cyber-Sicherheit kann vertrauliche Inhalte zum Nachweis der Einhaltung von Risikomanagementmassnahmen in einer sicheren und von der kontrollierten Stelle zur Verfügung gestellten Räumlichkeit prüfen.

4) Sie erstellt über die Ergebnisse der Kontrolle jeweils einen Bericht und übermittelt diesen der kontrollierten Stelle. In Absprache mit der kontrollierten Stelle sowie in begründeten Fällen kann die Stabsstelle Cyber-Sicherheit den Bericht vollständig oder auszugsweise an Dritte weitergeben.

5) Die Arbeitspapiere, Dokumente und Datenträger sind während zehn Jahren nach Abschluss der jeweiligen Kontrollen aufzubewahren; ausgenommen sind vertrauliche Inhalte nach Abs. 3.

Art. 14

*Kontrollen durch qualifizierte Dritte*

1) Qualifizierte Dritte haben ihre Kontrollen nach den Vorgaben der Stabsstelle Cyber-Sicherheit durchzuführen. Sie sind verpflichtet:

a) bei der Stabsstelle Cyber-Sicherheit nach Abschluss der Kontrolle einen Kontrollbericht einzureichen. Hierbei dürfen wesentliche Tatsachen nicht verschwiegen werden. Die Angaben im Kontrollbericht müssen der Wahrheit entsprechen;

b) die von der Stabsstelle Cyber-Sicherheit bestimmten Grundsätze über die Kontrolltätigkeit und Durchführung der Kontrollen einzuhalten und der Stabsstelle Cyber-Sicherheit auf Verlangen sämtliche im Rahmen der Kontrolle erstellten Arbeitspapiere zur Verfügung zu stellen;

c) der Stabsstelle Cyber-Sicherheit auf deren Verlangen jederzeit einen Zwischenbericht über den aktuellen Stand der Kontrolle abzugeben.

2) Qualifizierte Dritte unterliegen der Geheimhaltungspflicht. Vorbehalten bleiben die Berichterstattungs- und Auskunftspflicht nach Abs. 1.

3) Qualifizierte Dritte müssen bei der Durchführung einer Kontrolle von den zu kontrollierenden Stellen unabhängig sein. Sie dürfen insbesondere in den letzten 18 Monaten für die kontrollierende Stelle nicht beratend tätig gewesen sein.

## V. Übergangs- und Schlussbestimmungen

Art. 15

*Aufhebung bisherigen Rechts*

Die Cyber-Sicherheitsverordnung (CSV) vom 4. September 2023, LGBl. 2023 Nr. 359, wird aufgehoben.

Art. 16

*Übergangsbestimmung*

Einrichtungen, die zum Zeitpunkt des Inkrafttretens dieser Verordnung als Betreiber wesentlicher Dienste nach bisherigem Recht eingestuft sind, gelten als wesentliche Einrichtung nach Art. 3 Abs. 2 Bst. a Ziff. 5 des Cyber-Sicherheitsgesetzes.

Art. 17

*Inkrafttreten*

1) Diese Verordnung tritt vorbehaltlich Abs. 2 am 1. Februar 2025 in Kraft.

2) Art. 1 Abs. 2 Bst. a tritt gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses betreffend die Übernahme der Richtlinie (EU) 2022/2555 in das EWR-Abkommen in Kraft.

Fürstliche Regierung:
gez. *Dr. Daniel Risch*
Fürstlicher Regierungschef

**Anhang**
(Art. 3)

# Risikomanagementmassnahmen

| **1.** | **Risikoanalyse und Sicherheit von Netz- und Informationssystemen** |
|---|---|
| 1.1 | Risikoanalyse:<br>Eine Risikoanalyse der Netz- und Informationssysteme ist periodisch durchzuführen, um die Risiken für die Sicherheit von Netz- und Informationssystemen zu ermitteln, zu beurteilen und zu behandeln. Die Ergebnisse der Risikoanalyse sind zu dokumentieren. Auf Grundlage der Ergebnisse ist ein Risikobehandlungsplan zu erstellen, umzusetzen und zu überwachen. |
| 1.2 | Sicherheitsrichtlinie:<br>Eine Sicherheitsrichtlinie ist zu erstellen, periodisch zu überprüfen und gegebenenfalls zu aktualisieren. |
| 1.3 | Überprüfungsplan der Netz- und Informationssysteme:<br>Die periodische Überprüfung der Sicherheit der Netz- und Informationssysteme ist zu planen und durchzuführen. |
| 1.4 | Ressourcenmanagement/Asset Management:<br>Ein vollständiges, genaues, aktuelles und kohärentes Inventar der Netz- und Informationssysteme und anderer zugehöriger Anlagen und Werte, die die Abläufe und die Dienste der betreffenden Einrichtung unterstützen, ist zu führen. Alle Ressourcen, die erforderlich sind, um die Sicherheit von Netz- und Informationssystemen zu gewährleisten, sind im Hinblick auf kurz-, mittel- und langfristige Kapazitätsanforderungen einzuplanen und auf einem festgelegten Schutzniveau sicherzustellen. |
| 1.5 | Personal, Cyberhygiene und Schulungen:<br>Sicherheitsrelevante Aspekte, einschliesslich allfälliger Zuverlässigkeitsüberprüfungen, sind in den Prozessen des Personalwesens zu berücksichtigen und umzusetzen. Regelmässig sind Sensibilisierungsmassnahmen und Schulungen in den Bereichen der Cybersicherheit und Cyberhygiene bei den Mitarbeitenden durchzuführen. |

| | |
|---|---|
| 1.6 | Bewertung der Wirksamkeit der Risikomanagementmassnahmen:<br>Konzepte liegen vor und Verfahren legen fest, um zu bewerten, ob die ergriffenen Risikomanagementmassnahmen im Bereich der Cybersicherheit wirksam umgesetzt sind. |
| **2.** | **Berechtigungsmanagement (Identitäts- und Zugriffsmanagement)** |
| 2.1 | Identifikation und Authentifikation:<br>Es sind Verfahren umzusetzen und Technologien einzusetzen, die die logische und physische Kontrolle des Zugangs zu den Netz- und Informationssystemen mittels Identifikation und Authentifikation von Nutzern und Diensten gewährleisten. Die Zuweisungen von Zugangs- und Zugriffsrechten sind periodisch zu überprüfen und gegebenenfalls anzupassen. |
| 2.2 | Privilegierte Konten:<br>Administrative Zugangs- und Zugriffsrechte sind eingeschränkt nach dem Minimalrechtsprinzip zuzuweisen. Diese Zuweisungen sind periodisch zu überprüfen und gegebenenfalls anzupassen. |
| 2.3 | Systeme und Anwendungen zur Systemadministration:<br>Systeme und Anwendungen zur Systemadministration sind ausschliesslich für Tätigkeiten zum Zweck der Systemadministration zu verwenden. |
| 2.4 | Multi-Faktor-Authentifizierung:<br>Authentifizierungsmethoden sind der Kritikalität der Netz- und Informationssysteme angemessen. Dies umfasst unter anderem eine Multi-Faktor-Authentifizierung. |
| **3.** | **Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung** |
| 3.1 | Sicherheit der Netz- und Informationssysteme:<br>Technische, operative und organisatorische Massnahmen zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen sind einzuführen und periodisch zu überprüfen. Diese Massnahmen umfassen unter anderem den Schutz gegen Schadsoftware. |

| | |
|---|---|
| 3.2 | Fernzugriff:<br>Fernzugriffe sind eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten. |
| 3.3 | Konfigurationsmanagement:<br>Netz- und Informationssysteme sind sicher zu konfigurieren. Die Konfigurationen sind zu dokumentieren. Die Dokumentation ist aktuell zu halten. |
| 3.4 | Netzwerksegmentierung:<br>Eine Segmentierung der Netzwerke ist innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf vorzunehmen. |
| 3.5 | Kryptographie:<br>Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen. |
| 3.6 | Updatemanagement:<br>Verfügbare Sicherheitsupdates sind zeitnah zu testen, zu bewerten und einzuspielen. |
| 3.7 | Schwachstellenmanagement:<br>Mögliche Datenlecks sowie öffentlich bekannte Sicherheitslücken in eingesetzter Software und Hardware sind zu identifizieren. Gegen Verwundbarkeiten und bekannte Schwachstellen der Netz- und Informationssysteme sind im laufenden Betrieb geeignete Massnahmen zu ergreifen. |
| **4.** | **Sicherheitsmassnahmen bei Erwerb und Entwicklung** |
| 4.1 | Beschaffungsmanagement:<br>Es sind Verfahren und Massnahmen für das Management der Risiken festzulegen und periodisch zu überprüfen, die sich aus der Beschaffung von IKT-Diensten oder IKT-Produkten ergeben, die auf die Sicherheit der Netz- und Informationssysteme der betreffenden Einrichtungen einen Einfluss haben. |

| | |
|---|---|
| 4.2 | Projekt- und Entwicklungsmanagement:<br>Die Sicherheit von Netz- und Informationssystemen ist in den Prozessen des Projektmanagements, insbesondere bei der Entwicklung, entsprechend zu berücksichtigen. |
| 4.3 | Änderungsmanagement:<br>Die Sicherheit der Netz- und Informationssysteme ist in den Prozessen des Änderungsmanagements entsprechend zu berücksichtigen. Änderungen an den Netz- und Informationssystemen, insbesondere auch sicherheitsrelevante Konfigurationsänderungen, werden dokumentiert, bewertet, getestet, genehmigt, umgesetzt und überprüft. |
| **5.** | **Sicherheit der Lieferkette** |
| 5.1 | Verzeichnis der Lieferanten, Anbieter und Diensteanbieter:<br>Es ist ein Verzeichnis zu führen und laufend zu aktualisieren, welches die Lieferanten, die unmittelbaren Anbieter und Diensteanbieter samt Kontaktdaten enthält. |
| 5.2 | Beziehungen zu unmittelbaren Anbietern und Diensteanbietern:<br>Anforderungen an unmittelbare Anbieter und Diensteanbieter für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen. |
| 5.3 | Leistungsvereinbarungen mit Lieferanten, Anbietern und Diensteanbietern:<br>Die Leistungsvereinbarungen mit Lieferanten, unmittelbaren Anbietern und Diensteanbietern sind periodisch zu überprüfen und zu überwachen. |
| **6.** | **Physische Sicherheit** |
| | Der physische Schutz der Netz- und Informationssysteme, insbesondere der physische Schutz vor Naturkatastrophen oder unbefugtem Zutritt und Zugang, ist zu gewährleisten. |
| **7.** | **Bewältigung von Sicherheitsvorfällen (Erkennung und Bewältigung)** |
| 7.1 | Protokollierung und Monitoring:<br>Mechanismen zur Protokollierung und zum Monitoring von Aktivitäten in den Netz- und Informationssystemen sind umzusetzen. |

| | |
|---|---|
| 7.2 | Erkennung, Korrelation und Analyse:<br>Mechanismen zur Erkennung und Bewertung von Sicherheitsvorfällen, gegebenenfalls durch die Korrelation und Analyse der ermittelten Protokolldaten, sind umzusetzen. |
| 7.3 | Sicherheitsvorfallsreaktion:<br>Prozesse zur Reaktion auf Sicherheitsvorfälle sind zu erstellen (Konzept für die Bewältigung von Sicherheitsvorfällen), periodisch zu überprüfen, gegebenenfalls zu aktualisieren sowie zu erproben. |
| 7.4 | Sicherheitsvorfallsmeldung:<br>Prozesse zur internen und externen Meldung von Sicherheitsvorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben. |
| 7.5 | Sicherheitsvorfallsanalyse:<br>Prozesse zur Analyse und Bewertung von Sicherheitsvorfällen und zur Sammlung relevanter Informationen sind zu erstellen, aufrechtzuerhalten und zu erproben, um den kontinuierlichen Verbesserungsprozess zu fördern. |
| **8.** | **Aufrechterhaltung des Betriebs und Wiederherstellung nach einem Notfall** |
| 8.1 | Unterstützende Versorgungsleistungen:<br>Verluste, Schäden oder Beeinträchtigungen von Netz- und Informationssystemen oder Unterbrechungen ihres Betriebs aufgrund des Ausfalls oder der Störung unterstützender Versorgungsleistungen sind zu verhindern. |
| 8.2 | Betriebskontinuitätsmanagement:<br>Die Wiederherstellung der Netz- und Informationssysteme auf einem zuvor festgelegten Qualitätsniveau nach einem Sicherheitsvorfall ist zu gewährleisten. |
| 8.3 | Notfallmanagement:<br>Notfallpläne für die Aufrechterhaltung und Wiederherstellung des Betriebs nach einem Sicherheitsvorfall sind zu erstellen, anzuwenden, regelmässig zu bewerten und zu erproben. |

| | |
|---|---|
| 8.4 | Backup-Management:<br>Sicherungskopien sämtlicher relevanter Daten (einschliesslich Konfigurationsdaten) sind zu erstellen. Die Wiederherstellung innerhalb eines festzulegenden Zeitraums ist gewährleistet. Es werden regelmässig Integritätsprüfungen der Sicherungskopien durchgeführt. |
| **9.** | **Krisenmanagement** |
| | Rahmenbedingungen und Verfahren des Krisenmanagements sind für die Netz- und Informationssysteme vor und während eines Sicherheitsvorfalls zu definieren, umzusetzen, zu erproben und periodisch zu überprüfen. |