Nr. 26b

Verordnung über die Informatiksicherheit

vom 2. Februar 2010* (Stand 1. März 2010)

Der Regierungsrat des Kantons Luzern,

gestützt auf § 19 Absatz 3 des Informatikgesetzes vom 7. März 2005[1] und § 7 Absatz 2 des Datenschutzgesetzes vom 2. Juli 1990[2],
auf Antrag des Finanzdepartementes,

beschliesst:

I. Zweck und Geltungsbereich

§ 1 *Gegenstand und Zweck*

[1] Die Verordnung bestimmt

a. die Sicherheitsanforderungen, die bei der Bearbeitung von Daten mit Informatikmitteln einzuhalten sind, sowie
b. das Verfahren, die Zuständigkeiten und Verantwortlichkeiten zur Gewährleistung der Sicherheit von Daten, die mit Informatikmitteln bearbeitet werden.

[2] Sie bezweckt eine geordnete, wirksame und wirtschaftliche Informatiksicherheit.

§ 2 *Geltungsbereich*

[1] Diese Verordnung gilt für die kantonale Verwaltung (einschliesslich kantonaler Schulen) und für die Gerichte.

---

* G 2010 21
[1] SRL Nr. 26
[2] SRL Nr. 38

[2] Ausgenommen sind die Ausgleichskasse Luzern, die IV-Stelle Luzern, die Arbeitslosenkasse, die Gebäudeversicherung, die Luzerner Pensionskasse, die Lustat Statistik Luzern, der Verkehrsverbund Luzern, die kantonalen Spitäler (Luzerner Kantonsspital, Luzerner Psychiatrie), die im Rahmen eines Konkordats geführten Hochschulen und Fachhochschulen sowie die Universität.

[3] Sie gilt jedoch auch für die in Absatz 2 genannten sowie für weitere Stellen und Körperschaften, soweit diese Informatikmittel des Kantons Luzern benutzen.

II. Allgemeine Bestimmungen

§ 3 *Begriffe*

[1] Der Begriff «Informatikmittel» richtet sich nach dem Informatikgesetz vom 7. März 2005[3].

[2] Die Begriffe «Personendaten», «besonders schützenswerte Personendaten», «Inhaber einer Datensammlung», «Bearbeiten von Personendaten» sowie «Organ» richten sich nach dem Datenschutzgesetz vom 2. Juli 1990[4].

[3] Der Begriff «Informationen» richtet sich nach der Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz vom 10. Dezember 2002[5].

§ 4 *Zuständigkeit*

[1] Inhaber einer Datensammlung und Betreiber einer zentralen Datenbank sind verpflichtet, Informatikmittel gegen Verlust und unerwünschte Einwirkungen zu sichern und Personendaten vor unbefugtem Zugriff und unbefugter Bearbeitung zu schützen.

[2] Die Organe sind in ihrem Zuständigkeitsbereich verantwortlich für
a. die Bestimmung der Schutzziele für Informationen und Informatikmittel,
b. die Klassifizierung der Informationen und Informatikmittel nach den Schutzzielen,
c. die Erstellung eines Massnahmenplans zur Erreichung der Schutzziele und die Umsetzung der Sicherheitsanforderungen,
d. die Sensibilisierung ihrer Angestellten, Auftragnehmer und Drittbenutzer hinsichtlich der Informatiksicherheit,
e. die Kontrolle der Informatiksicherheit.

[3] SRL Nr. 26. Auf dieses Gesetz wird im Folgenden nicht mehr hingewiesen.
[4] SRL Nr. 38. Auf dieses Gesetz wird im Folgenden nicht mehr hingewiesen.
[5] SRL Nr. 26c (bis 28. Februar 2009 Nr. 38c). Auf diese Verordnung wird im Folgenden nicht mehr hingewiesen.

[3] Die Dienststelle Informatik
a. bewirtschaftet die Informatiksicherheitsprojekte,
b. unterstützt in Zusammenarbeit mit den Organisations- und Informatikbeauftragten die Organe bei der Einrichtung einer sicheren Informatik und der Umsetzung und Kontrolle der Sicherheitsmassnahmen,
c. überwacht die Einhaltung der technischen Sicherheitsanforderungen,
d. dokumentiert den Stand der Informatiksicherheit des Kantons Luzern,
e. ist Ansprechpartnerin für die Organe in Fragen der Informatiksicherheit.

§ 5 *Schutzziele*

[1] Für Informationen und Informatikmittel gelten folgende Schutzziele:
a. Verfügbarkeit: Informationen und Informatikmittel sind zugänglich und nutzbar. Massgeblich sind die zulässige Ausfalldauer im Einzelfall und die Anzahl zulässiger Ausfälle pro Kalenderjahr.
b. Vertraulichkeit: Daten sind nur den berechtigten Personen zugänglich.
c. Integrität: Anwendungen und Daten sind vor unberechtigten Änderungen geschützt. Die Daten sind vollständig und richtig.
d. Nachvollziehbarkeit: Eine Ereigniskette kann nachträglich nachvollzogen werden.

[2] Die Organe und die Dienststelle Informatik sind befugt, für ihren Zuständigkeitsbereich die Schutzziele zu verfeinern und zusätzliche Weisungen zu erlassen.

§ 6 *Klassifizierung*

[1] Die Informationen und Informatikmittel sind nach folgenden Kriterien zu klassifizieren:
a. Verfügbarkeit: während der Bürozeiten, während erweiterter Bürozeiten und 7 × 24 Stunden,
b. Vertraulichkeit: öffentlich, intern und geheim,
c. Integrität: unkritisch (bezüglich Abweichungen und Fehler tolerierbar), mittel (Grad der Integrität erkennbar, Fehler behebbar) und hoch (Integrität zwingend sicherzustellen),
d. Nachvollziehbarkeit: keine Nachvollziehbarkeit, anonymisierte Nachvollziehbarkeit und personenbezogene Nachvollziehbarkeit.

[2] Die Organe und die Dienststelle Informatik sind befugt, für ihren Zuständigkeitsbereich die Klassifikation zu verfeinern und zusätzliche Weisungen zu erlassen.

§ 7 *Massnahmenplan*

[1] Der Massnahmenplan dient der Erreichung der Schutzziele im Zuständigkeitsbereich des Organs. Die einzelnen Massnahmen richten sich nach den Sicherheitsanforderungen im dritten Teil dieser Verordnung. Dabei sind der Grundsatz der Verhältnismässigkeit, der Stand der Technik und die verfügbaren Mittel zu berücksichtigen.

[2] Der Massnahmenplan enthält für jede Massnahme folgende Angaben:
a. Schutzziele und Klassifizierung,
b. Inhalt,
c. Kosten,
d. Verantwortlichkeiten,
e. Umsetzungsschritte und Termine,
f. Restrisiko,
g. Dokumentation.

§ 8 *Sensibilisierung*

Um die Risiken durch menschlichen Irrtum, Diebstahl, Betrug oder Missbrauch von Informationen und Informatikmittel zu verringern, sensibilisieren die Organe ihre Angestellten, Auftragnehmer und Drittbenutzer für die Informatiksicherheit. Sie stellen dabei sicher, dass diese ihre Verantwortlichkeiten in Bezug auf die Schutzziele verstehen und regelmässig über organisationseigene Regelungen und Verfahren zur Informatiksicherheit informiert werden.

III. Sicherheitsanforderungen

§ 9 *Schutz der Organisationsinfrastruktur und der zugehörigen Informationen*

Zur Verhinderung von Verlust, Beschädigung und Missbrauch von Informatikmitteln und zur Verhinderung eines Unterbruchs von Geschäftsaktivitäten müssen die Gebäude, Räume und Geräte vor Sicherheitsbedrohungen und umgebungsbedingten Gefahren geschützt werden.

§ 10 *Zugriffsschutz*

[1] Der Zugriff auf Informationen, Informatikmittel und Daten ist in einem Zugriffskonzept zu regeln.

[2] Zur Beschränkung des Zugriffs sind die Sicherheitseinrichtungen des zentralen System-Managements zu verwendet.

[3] Benutzerpasswörter für die Informatikmittel müssen den Angestellten, Auftragnehmern und Drittbenutzern in einem geregelten und kontrollierbaren Verfahren zugeteilt werden. Die Benutzerinnen und Benutzer müssen dabei auf ihre Verantwortung für die Aufrechterhaltung effektiver Zugangskontrollen, insbesondere in Bezug auf den Gebrauch des Passworts und die Sicherheit der Benutzergeräte, hingewiesen werden.

[4] Privilegierte Zugriffsrechte dürfen nur zurückhaltend vergeben werden. Sie müssen registriert und periodisch überprüft werden.

§ 11 *Beendigung oder Änderung der Anstellung*

[1] Die Rechte der Angestellten, Auftragnehmer oder Drittbenutzer auf Zugang zu Informationen und Informatikmitteln müssen sofort entzogen werden, wenn ihre Anstellung, ihr Auftrag oder eine entsprechende Nutzungsvereinbarung beendet ist. Ändern Anstellung, Auftrag oder Nutzungsvereinbarung, sind die Zugangsrechte umgehend anzupassen.

[2] Sicherheitsbereiche müssen durch angemessene Zutrittskontrollen geschützt sein, um sicherzustellen, dass nur autorisierten Personen Zutritt gewährt wird.

§ 12 *Management der elektronischen Datenkommunikation*

[1] Der ausgewiesene Datenkommunikationsbedarf der kantonalen Organe wird grundsätzlich über das Datenkommunikationsnetz des Kantons Luzern (LUnet) abgewickelt.

[2] Anschlüsse an verwaltungsinterne oder -externe Informationssysteme, Netzwerke und Anwendungen bedürfen einer Bewilligung der betroffenen Organe.

[3] Die Dienststelle Informatik ist verantwortlich für die Sicherheit des LUnet. Sie kann Einschränkungen in der Nutzung festlegen, um die allgemeine Verfügbarkeit sicherzustellen.

§ 13 *Datenaustausch*

[1] Der Austausch von Informationen zwischen sämtlichen Kommunikationseinrichtungen hat nach einem fest geregelten, sicheren Verfahren zu erfolgen.

[2] Es sind geeignete Schutzmassnahmen zu ergreifen, um unbefugten Zugriff, Missbrauch und Verfälschung der Informationen während des Datenaustausches zu verhindern. Der Schutz muss auch beim Austausch über Organisationsgrenzen hinweg gewährleistet sein.

§ 14 *Datensicherung, Sicherstellung des Geschäftsbetriebs*

[1] Informationen und Software müssen in regelmässigen Abständen mittels Datensicherung gesichert werden.

[2] Die Funktionsfähigkeit der Datensicherungskopien ist sicherzustellen.

[3] Es müssen Pläne entwickelt und umgesetzt werden, um bei Störungen den Betrieb aufrechtzuerhalten oder wieder herzustellen und um die Verfügbarkeit von Informatikmitteln nach Unterbrechungen oder Ausfällen von kritischen Geschäftsprozessen im erforderlichen Mass und im erforderlichen Zeitraum sicherzustellen.

§ 15 *Entsorgung von Datenträgern*

Bei der Entsorgung sämtlicher Datenträger ist sicherzustellen, dass vorher alle Informationen entfernt werden und lizenzierte Software irreversibel überschrieben ist.

§ 16 *Mobile Datenträger und Informatikmittel sowie Telearbeit*

[1] Für den sicheren Umgang mit mobilen Datenträgern und Informatikmitteln sind spezielle Weisungen zu erlassen. Insbesondere müssen die Weisungen vorsehen, dass Informationen vor unberechtigten Zugriffen zu schützen sind.

[2] Die Weisungen sind periodisch dem neusten Stand der Technik anzupassen.

[3] Bei Einrichtung und Nutzung eines Telearbeitsplatzes zu Hause muss die infrastrukturelle Sicherheit gewährleistet sein. Zum Schutz der Informationen vor unbefugtem Zugriff ist dabei insbesondere sicherzustellen, dass sichere Geräte und Telekommunikationsverbindung benutzt werden.

§ 17 *Schutz vor Schadsoftware*

Das Eindringen von Schadsoftware muss erkannt und soweit möglich verhindert werden. Es ist sicherzustellen, dass bei einem Schadensfall die Informationen und die Software wiederhergestellt werden können.

IV. Kontrolle

§ 18 *Meldung von Vorkommnissen und Schwachstellen*

[1] Angestellte, Auftragnehmer und Drittbenutzer von Informatikmitteln sind verpflichtet, alle beobachteten oder vermuteten sicherheitsrelevanten Vorkommnisse den zuständigen Organisations- und Informatikbeauftragten ohne Verzug zu melden. Sie informieren diese auch über neu entdeckte Schwachstellen der Informatiksicherheit.

[2] Sicherheitsrelevante Vorkommnisse im Zusammenhang mit Personendaten sind auch dem oder der kantonalen Datenschutzbeauftragten zu melden.

[3] Die Organe müssen ein Verfahren vorsehen, das eine schnelle, wirksame und planmässige Reaktion auf sicherheitsrelevante Vorkommnisse ermöglicht. Für Informationen und Informatikmittel mit der Klassifizierung Verfügbarkeit 7 × 24 Stunden ist ein spezielles Notfallkonzept zu erstellen.

§ 19 *Überprüfung*

[1] Die Organe überprüfen regelmässig die Schutzziele und die Klassifizierung der Informationen und Informatikmittel sowie die Einhaltung und die Angemessenheit der Sicherheitsmassnahmen. Sie erstatten dem oder der Organisations- und Informatikbeauftragten darüber Bericht und passen den Massnahmenplan wenn nötig an. Die Prüfung ist umgehend vorzunehmen, wenn Aufgaben, Organisation oder eingesetzte Informatikmittel eines Organs ändern. Der oder die Organisations- und Informatikbeauftragte kann die

Schutzziele und die Klassifizierung sowie die getroffenen Massnahmen zusätzlich durch eine qualifizierte unabhängige externe Stelle prüfen lassen.

[2] Sicherheitsmassnahmen und Notfallkonzepte für Informationen und Informatikmittel mit der Klassifizierung geheim oder Verfügbarkeit 7 × 24 Stunden sind regelmässig durch die Organisations- und Informatikbeauftragten oder eine unabhängige externe Stelle zu überprüfen.

[3] Der oder die kantonale Datenschutzbeauftragte überprüft periodisch die Sicherheit, die Massnahmen und deren Umsetzung bei personenbezogenen Daten.

§ 20 *Protokollierung*

[1] Es werden Protokolle erstellt, welche Benutzeraktivitäten, Systemfehler und sicherheitsrelevante Vorkommnisse festhalten. Dabei sind der Grundsatz der Verhältnismässigkeit, der Stand der Technik und die verfügbaren Mittel zu berücksichtigen. Die Protokolle sind regelmässig von unabhängigen Personen oder maschinell auszuwerten, um sicherheitsrelevante Vorkommnisse zu identifizieren.

[2] Die Auswertung erfolgt anonym. Ist eine personenbezogene Auswertung notwendig, richtet sich diese nach den Vorschriften in der Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz.

[3] Die Aufzeichnungen sind vor Verlust, Zerstörung und Fälschung zu schützen. Datenschutz, Integrität und Vertraulichkeit sind zu wahren.

[4] Die Protokolle sind während zweier Jahre aufzubewahren. Bei personenbezogenen Protokollen beträgt die Aufbewahrungsfrist sechs Monate.

V. Schlussbestimmungen

§ 21 *Aufhebung bisherigen Recht*

Die Verordnung über die Sicherheitsgrundsätze und das Bewilligungsverfahren im Bereich des elektronischen Datenaustausches vom 23. April 1996[6] wird aufgehoben.

§ 22 *Übergangsbestimmung*

Die Bestimmung der Schutzziele, die Klassifizierung von Informationen und Informatikmitteln und die Erstellung eines Massnahmenplans haben innerhalb von zwei Jahren nach Inkrafttreten dieser Verordnung zu erfolgen.

---

[6] G 1996 65 (SRL Nr. 39b)

§ 23 *Inkrafttreten*

Die Verordnung tritt am 1. März 2010 in Kraft. Sie ist zu veröffentlichen.

Luzern, 2. Februar 2010

Im Namen des Regierungsrates
Der Präsident: Anton Schwingruber
Der Staatsschreiber: Markus Hodel