Nr. 26b

Verordnung über die Informatiksicherheit und über die Nutzung von Informatikmitteln (Informatiksicherheitsverordnung)

vom 22. November 2016 (Stand 1. September 2021)

Der Regierungsrat des Kantons Luzern,

gestützt auf die §§ 2 Absatz 2, 19 Absatz 3, 20 Absätze 2 und 4 des Informatikgesetzes vom 7. März 2005[1], § 7 Absatz 2 des Kantonalen Datenschutzgesetzes vom 2. Juli 1990[2] sowie § 81 des Personalgesetzes vom 26. Juni 2001[3],
auf Antrag des Finanzdepartementes, *

beschliesst:

1 Allgemeine Bestimmungen

§ 1 *Gegenstand und Zweck*

[1] Die Verordnung bestimmt das Verfahren, die Zuständigkeiten und Verantwortlichkeiten sowie den Vollzug zur Gewährleistung der Sicherheit von Informationen, die mit Informatikmitteln bearbeitet werden.

[2] Sie bezweckt die Regelung des sicheren und wirtschaftlichen Einsatzes von Informatikmitteln zur Erfüllung von gesetzlichen Aufgaben sowie die Wahrung der Persönlichkeitsrechte der Anwenderinnen und Anwender.

---

1 SRL Nr. 26
2 SRL Nr. 38
3 SRL Nr. 51
* Siehe Tabellen mit Änderungsinformationen am Schluss des Erlasses.

§ 2 *Geltungsbereich*

[1] Diese Verordnung gilt für die kantonale Verwaltung (einschliesslich kantonaler Schulen) und für die Gerichte. Soweit die Sicherheit, die Funktionsfähigkeit, die Vertraulichkeit und die Verfügbarkeit der Informatikmittel betroffen sind, unterstehen ihr auch die Behördenmitglieder. Ausgenommen sind die Ausgleichskasse Luzern, die IV-Stelle Luzern, die Arbeitslosenkasse, die Gebäudeversicherung Luzern, die Luzerner Pensionskasse, die Lustat Statistik Luzern, der Verkehrsverbund Luzern, die kantonalen Spitäler (Luzerner Kantonsspital, Luzerner Psychiatrie), die Pädagogische Hochschule Luzern, die Universität und die Hochschule Luzern. *

[2] Sie gilt jedoch auch für die gemäss Absatz 1 ausgenommenen sowie für weitere Stellen, Körperschaften, Organe und Anwenderinnen und Anwender, soweit diese Informatikmittel des Kantons Luzern benutzen.

[3] Soweit diese Verordnung nichts anderes bestimmt, gelten für die Lernenden der kantonalen Schulen sinngemäss dieselben Vorschriften wie für die übrigen Anwenderinnen und Anwender. Falls Lernenden kantonale Geräte mit erweiterten Benutzerrechten zur Verfügung gestellt werden, gelten für diese Geräte die Bestimmungen für nichtkantonale Geräte. *

[4] Soweit die in den Absätzen 1–3 genannten Stellen, Körperschaften, Organe und Anwenderinnen und Anwender zur Bearbeitung von Informationen des Kantons Luzern nichtkantonale Geräte nutzen, finden für diese Geräte die §§ 4, 7, 8 Absätze 1 und 2, 9–16, 18, 20, 24 Absatz 3 und 26 keine Anwendung. *

§ 3 *Begriffe*

[1] Informationen im Sinn dieser Verordnung sind Sach- und Personendaten.

[2] Der Begriff der Informatikmittel richtet sich nach dem Informatikgesetz vom 7. März 2005[4]. Informatikmittel sind Geräte, Einrichtungen und Dienste, wie insbesondere Computersysteme, Computerprogramme, Kommunikationsdienste, die der elektronischen Erfassung, Verarbeitung, Speicherung, Übermittlung, Auswertung, Archivierung oder Vernichtung von Informationen dienen. *

[3] Die Begriffe der Personendaten und der Organe richten sich nach dem Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990[5]. *

[4] Anonym bedeutet, dass keine Rückschlüsse auf eine einzelne Person möglich sind.

[5] Protokolldaten sind sämtliche zum Zweck der Überwachung und Kontrolle nach dieser Verordnung notwendigen Daten.

[6] Der Begriff der Leistungserbringer richtet sich nach der Informatikverordnung vom 17. Juni 2016[6].

---

4 SRL Nr. 26
5 SRL Nr. 38
6 SRL Nr. 26a

§ 4 *Zuständigkeit*

[1] Inhaber einer Datensammlung und Betreiber einer zentralen Datenbank sind verpflichtet, Informatikmittel gegen Verlust und unerwünschte Einwirkungen zu sichern und Informationen, insbesondere 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 und Inventarisierung der Informationen und Informatikmittel nach den Schutzzielen,
c. die Erstellung eines Massnahmenplans zur Erreichung der Schutzziele und die Umsetzung der Sicherheitsanforderungen,
d. die Sensibilisierung der Anwenderinnen und Anwender hinsichtlich der Informatiksicherheit,
e. die Kontrolle der Informatiksicherheit.

[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 und informiert darüber,
e. ist Ansprechpartnerin für die Organe in Fragen der Informatiksicherheit.

§ 5 *Persönliche Verantwortung*

[1] Alle Anwenderinnen und Anwender sind für die Verwendung ihrer Informatikmittel im Rahmen der geltenden Rechtsordnung und dieser Verordnung persönlich verantwortlich.

[2] Insbesondere sind sie dafür verantwortlich, dass an ihrem Arbeitsplatz und in ihrem Zuständigkeitsbereich die entsprechenden Vorgaben zur Gewährleistung von Datenschutz und Informationssicherheit befolgt werden.

§ 6 *Schulungs- und Informationspflicht, Sensibilisierung*

[1] Die Departemente, die Staatskanzlei und die Gerichte sowie die gemäss § 2 Absatz 1 ausgenommenen und die weiteren Organe, Stellen und Körperschaften, soweit diese Informatikmittel des Kantons Luzern benutzen, sorgen dafür, dass die Anwenderinnen und Anwender über den richtigen Umgang mit den Informatikmitteln geschult und regelmässig informiert werden.

[2] Sie sind befugt, für ihren Zuständigkeitsbereich Weisungen über die Nutzung der Informatikmittel zu erlassen. Diese Weisungen sind dem oder der kantonalen Beauftragten für Informationssicherheit bekannt zu machen.

[3] Um die Risiken durch menschlichen Irrtum, Diebstahl, Betrug oder Missbrauch von Informationen und Informatikmitteln zu verringern, sensibilisieren sie die Anwenderinnen und Anwender 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.

§ 7 *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: Informationen sind nur den berechtigten Personen zugänglich,
c. Integrität: Informationen und Informatikmittel sind vor unberechtigten Änderungen geschützt. Die Informationen sind vollständig und richtig,
d. Nachvollziehbarkeit: Eine Ereigniskette (z.B. hinsichtlich der Bearbeitung oder des Zugriffs auf Informationen) 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.

§ 8 *Klassifizierung*

[1] Die Informationen und Informatikmittel sind nach folgenden Kriterien zu klassifizieren:

a. Verfügbarkeit: während der Bürozeiten, während erweiterter Bürozeiten, während 7×24 Stunden; jeweils unter Angabe der zulässigen Ausfalldauer,
b. Vertraulichkeit: öffentlich, intern, vertraulich 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. Darin können Behandlungsregeln aufgenommen werden, welche von den Anwenderinnen und Anwendern im Umgang mit klassifizierten Informationen zu beachten sind.

[3] Vertrauliche und geheime Informationen, namentlich besonders schützenswerte Personendaten und Persönlichkeitsprofile, dürfen nur verschlüsselt übertragen und auf Endgeräten gespeichert werden. Der oder die Beauftragte für den Datenschutz kann für die Speicherung von Personendaten und Persönlichkeitsprofilen auf Endgeräten Ausnahmen bewilligen. *

§ 9 *Projekte*

[1] In allen Projekten für neue Anwendungen und Systeme, mit denen vertrauliche oder geheime Informationen bearbeitet werden, ist ein Informationssicherheits- und Datenschutzkonzept zu erstellen. Die Dienststelle Informatik überwacht die Umsetzung der in den Projekten vereinbarten technischen Sicherheitsanforderungen.

[2] Die Dienststelle Informatik plant die kantonalen Informatiksicherheitsprojekte. Sie unterstützt die Organe bei der Projektierung und Einrichtung einer sicheren Informatik.

§ 10 *Massnahmenplan*

[1] Der Massnahmenplan dient der Erreichung der Schutzziele und der Einhaltung der Sicherheitsanforderungen im Zuständigkeitsbereich der Organe. Die einzelnen Massnahmen richten sich nach den Sicherheitsanforderungen im zweiten 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. Schutzziel und Geltungsbereich (bezüglich Informatikmitteln und Klassifizierung),
b. Inhalt,
c. Kosten,
d. Verantwortlichkeit,
e. Umsetzungsschritte und Termine,
f. Restrisiko,
g. Dokumentation (Nachweis der Umsetzung und Wirksamkeit der Massnahme).

§ 11 *Überprüfung Schutzziele, Klassifizierung, Sicherheitsmassnahmen*

[1] Die Organe überprüfen in ihrem Zuständigkeitsbereich mindestens jährlich die Schutzziele und die Klassifizierung der Informationen und Informatikmittel sowie die Einhaltung der Sicherheitsanforderungen und die Angemessenheit der Sicherheitsmassnahmen. Sie erstatten den Organisations- und Informatikbeauftragten und dem oder der kantonalen Beauftragten für Informationssicherheit darüber Bericht und passen den Massnahmenplan wenn nötig an. Die Prüfung ist umgehend vorzunehmen, wenn die Aufgaben, die Organisation oder die eingesetzten Informatikmittel eines Organs ändern. Die Organe können die Schutzziele und die Klassifizierung sowie die getroffenen Massnahmen in ihrem Zuständigkeitsbereich zusätzlich durch eine qualifizierte unabhängige externe Stelle prüfen lassen.

[2] Sicherheitsmassnahmen und Notfallkonzepte für Informationen und Informatikmittel mit der Klassifizierung «geheim» oder «Verfügbarkeit während 7x24 Stunden» sind jährlich durch die Organe oder eine unabhängige externe Stelle zu überprüfen.

[3] Der oder die Beauftragte für den Datenschutz überprüft periodisch die Sicherheit, die Massnahmen und deren Umsetzung bei personenbezogenen Daten. *****

[4] Die in der vorliegenden Verordnung enthaltenen Regelungen zur Klassifizierung und zur Behandlung klassifizierter Informationen und Informatikmittel gelten nur insofern, als sie den übergeordneten bundes- und kantonalrechtlichen Vorgaben zur Vertraulichkeit von Informationen und Informatikmitteln nicht widersprechen.

2 Sicherheitsanforderungen

§ 12 *Schutz der Infrastruktur und der Informationen*

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

§ 13 *Zugriffsschutz und Zutrittskontrollen*

[1] Der Zugriff auf Informationen und Informatikmittel sowie die Vergabe und Mutation von Berechtigungen sind durch die Organe in einem Zugriffskonzept zu regeln.

[2] Sicherheitsbereiche müssen durch angemessene Zutrittskontrollen geschützt sein, damit sichergestellt ist, dass nur autorisierten Personen Zutritt gewährt wird.

[3] Benutzerpasswörter für die Informatikmittel müssen den Anwenderinnen und Anwendern (Angestellten, Auftragnehmern und Drittbenutzern) durch die Organe in einem geregelten und kontrollierbaren Verfahren zugeteilt werden. Die Anwenderinnen und Anwender müssen dabei auf ihre Verantwortung für die Aufrechterhaltung effektiver Zugriffskontrollen, insbesondere in Bezug auf die Nutzung des Passworts gemäss der entsprechenden Weisung zur Passwort-Policy, und auf die Sicherheit der Benutzergeräte hingewiesen werden.

[4] Privilegierte Zugriffsrechte sowie Zugriffsrechte auf vertraulich und geheim klassifizierte Informationen und Informatikmittel dürfen nur zurückhaltend vergeben werden. Solche Zugriffe müssen protokolliert und die Zugriffsrechte periodisch überprüft werden.

[5] Im Rahmen der einzelnen Funktionen eines Systems oder einer Anwendung sind die jeweiligen Anforderungen an die Überprüfung der Identität des Benutzers oder der Benutzerin beziehungsweise des Systems direkt zu formulieren und entsprechend in den Systemen und Anwendungen abzubilden.

[6] Zur Authentifizierung des Benutzers oder der Benutzerin ist grundsätzlich das zentrale Benutzerregister zu verwenden.

§ 14 *Entzug Zutritts- und Zugriffsrechte*

[1] Zutritts- und Zugriffsrechte von Anwenderinnen und Anwendern, Auftragnehmern oder Drittbenutzern müssen von den zuständigen Organen sofort entzogen werden, wenn deren Anstellung, deren Auftrag oder eine entsprechende Nutzungsvereinbarung beendet ist. Ändern Anstellung, Auftrag oder Nutzungsvereinbarung, sind die Zutritts- und Zugriffsrechte umgehend anzupassen.

§ 15 *Management der elektronischen Datenkommunikation*

[1] Informationen der kantonalen Organe sind grundsätzlich über das Datenkommunikationsnetz des Kantons Luzern (LUnet) auszutauschen.

[2] Anschlüsse an verwaltungsinterne oder -externe Informatikmittel, Netzwerke und Anwendungen bedürfen einer Bewilligung der betroffenen Organe. Mit einem externen Partner sind die seitens der Dienststelle Informatik vorgeschriebenen Sicherheitsmassnahmen schriftlich zu vereinbaren. Die Einhaltung der Sicherheitsanforderungen und die Angemessenheit der Sicherheitsmassnahmen ist durch die betroffenen Organe regelmässig risikobasiert zu überprüfen.

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

[4] Die Dienststelle Informatik ist für die Sicherung der Netzübergänge zuständig.

§ 16 *Datenaustausch*

[1] Der Austausch von Informationen zwischen sämtlichen Kommunikationseinrichtungen hat nach den von der Dienststelle Informatik festgelegten Verfahren und Methoden zu erfolgen.

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

[3] Die Kommunikationsteilnehmerinnen und -teilnehmer sind selbst dafür verantwortlich, dass bei der Kommunikation über LUnet die jeweiligen Vertraulichkeitsanforderungen eingehalten werden.

§ 17 *Speicherung und Ablage der Informationen*

[1] Informationen und elektronische Datenträger sind so aufzubewahren, dass sie für Unberechtigte nicht einsehbar sind. Anwenderinnen und Anwender müssen Informationen gemäss den geltenden Weisungen geordnet und zentral auf den dafür vorgesehenen und geeigneten Anwendungen und Systemen speichern und ablegen, damit sie verfügbar bleiben und regelmässig gesichert werden.

[2] Die Dienststelle Informatik ist in alle Vorhaben, die eine temporäre oder dauerhafte Speicherung von Informationen des Kantons Luzern auf Systemen von Dritten einschliessen, frühzeitig einzubeziehen.

§ 18 *Datensicherung, Sicherstellung des Geschäftsbetriebs*

[1] Der Leistungserbringer stellt sicher, dass Informationen und Software in regelmässigen Abständen gesichert werden.

[2] Der Leistungserbringer ist verantwortlich dafür, dass die Funktionsfähigkeit der Datensicherungskopien regelmässig getestet wird. Bei der elektronischen Archivierung stellt er die Verlässlichkeit und die Authentizität der Informationen mit angemessenen organisatorischen und technischen Vorkehrungen sicher.

[3] Die Organe sind dafür verantwortlich, dass Pläne entwickelt und umgesetzt werden, um Störungen und Ausfällen von kritischen Geschäftsprozessen im erforderlichen Umfang zu begegnen und die Verfügbarkeit der Informatikmittel in Zusammenarbeit mit dem Leistungserbringer sicherzustellen.

§ 19 *Entsorgung von Datenträgern*

[1] Defekte oder zu entsorgende Datenträger sind
a. entweder der Dienststelle Informatik zu übergeben; diese stellt sicher, dass alle Informationen und lizenzierte Software irreversibel vernichtet und die Datenträger sicher und umweltgerecht entsorgt werden, oder
b. gemäss den Vorgaben der Dienstelle Informatik zu vernichten.

§ 20 *Schutz vor Schadsoftware*

[1] Die Leistungserbringer betreiben Infrastrukturen, mit denen das Eindringen und die Verbreitung von Schadsoftware erkannt und soweit möglich verhindert werden.

3 Nutzung und Missbrauch von Informatikmitteln

§ 21 *Grundsätze für die Nutzung*

[1] Für die Bearbeitung von Informationen des Kantons Luzern dürfen grundsätzlich nur kantonale Informatikmittel verwendet werden. Kantonale Schulen sind von dieser Regelung nicht betroffen.

[2] Bei der Verwendung kantonaler Informatikmittel ist zu beachten:
a. Es dürfen nur kantonale Informatikmittel eingesetzt werden, die von den zuständigen Organen zugelassen werden.
b. Die Informatikmittel dürfen grundsätzlich nur zur Erfüllung dienstlicher Aufgaben benutzt werden.

c. Die Verwendung kantonaler Informatikmittel zu privaten Zwecken darf den Dienstbetrieb nicht erschweren oder einschränken und die Sicherheit nicht gefährden.
d. Aus der privaten Nutzung kantonaler Informatikmittel kann kein Rechtsanspruch auf die Verfügbarkeit der Infrastruktur des Kantons Luzern und der privaten Informationen abgeleitet werden.
e. Benutzernamen und Passwörter sind persönlich und nicht übertragbar. Die Passwörter sind geheim zu halten.

[3] Die Verwendung nichtkantonaler Geräte ist von dem oder der zuständigen Organisations- und Informatikbeauftragten zu bewilligen. Dabei gilt:
a. Die Dienststelle Informatik legt die mit kantonalen Informatikmitteln und nichtkantonalen Geräten nutzbaren Informatikservices in einer Weisung fest.
b. Die Weisung ist periodisch dem neuesten Stand der Technik anzupassen und bedarf der Genehmigung des Gremiums der Organisationsverantwortlichen (OVG).
c. Die Dienststelle Informatik lehnt die Verantwortung für allfällige auf der Infrastruktur des Kantons Luzern abgelegte nichtkantonale Informationen ab.
d. Benutzernamen und Passwörter sind persönlich und nicht übertragbar. Die Passwörter sind geheim zu halten.

[4] Bei der Verwendung nichtkantonaler Geräte ist zu beachten:
a. Für nichtkantonale Geräte erlässt die Dienststelle Informatik Weisungen.
b. Die Dienststelle Informatik legt die Anforderungen an zugreifende Geräte in einer Weisung fest, entscheidet über die zugelassenen Geräte und überprüft die Einhaltung der technischen Anforderungen.
c. Den Anwenderinnen und Anwendern ist zur Kenntnis zu bringen, dass Informationen und Software auf ihren Geräten aus Sicherheitsgründen gelöscht werden können.
d. Anwenderinnen und Anwender stellen sicher, dass ihr nichtkantonales Gerät kein Risiko für die Sicherheit und die Unversehrtheit der Infrastruktur des Kantons Luzern darstellt.
e. Die Verwendung nichtkantonaler Geräte darf den Dienstbetrieb nicht erschweren oder einschränken.

§ 22 *Mobile Datenträger und Informatikmittel sowie mobiles Arbeiten*

[1] Für den sicheren Umgang mit mobilen Datenträgern und Informatikmitteln sind von der Dienststelle Informatik spezielle Weisungen zu erlassen. Insbesondere müssen die Weisungen vorsehen, dass Informationen vor unberechtigten Zugriffen zu schützen sind, und festlegen, welche Informationen auf mobilen Datenträgern und Informatikmitteln gespeichert werden dürfen.

[2] Nutzen Anwenderinnen und Anwender einen mobilen Arbeitsplatz, haben sie sich an die geltenden Weisungen und Sicherheitsvorgaben zu halten. Wenn sie hoheitliche Aufgaben erfüllen, hat dies unter Ausschluss der Öffentlichkeit an den von den Organen dafür vorgeschriebenen Arbeitsorten zu erfolgen.

§ 23 *Feststellung von Vorkommnissen und Schwachstellen*

[1] Alle Anwenderinnen und Anwender von Informatikmitteln des Kantons Luzern sind verpflichtet, beobachtete oder vermutete Vorkommnisse oder Schwachstellen, welche eine Gefährdung darstellen für

a. die technische Sicherheit, die Funktionsfähigkeit und die Verfügbarkeit von Informatikmitteln,
b. die Schutzziele gemäss § 7 dieser Verordnung oder
c. den wirtschaftlichen Einsatz von Informatikmitteln,

den zuständigen Organisations- und Informatikbeauftragten ohne Verzug zu melden. Diese entscheiden über das weitere Vorgehen.

[2] Vorkommnisse oder Schwachstellen im Zusammenhang mit Personendaten sind von den zuständigen Organisations- und Informatikbeauftragten dem oder der Beauftragten für den Datenschutz zu melden. *

[3] Die zuständigen Organisations- und Informatikbeauftragten müssen ein Verfahren vorsehen, das eine schnelle, planmässige und wirksame Reaktion auf sicherheitsrelevante Vorkommnisse ermöglicht. Für Informationen und Informatikmittel mit Verfügbarkeit während 7x24 Stunden ist ein spezielles Notfallkonzept zu erstellen.

§ 24 *Nutzung von E-Mail und Internet*

[1] Mit E-Mail dürfen keine vertraulichen und geheimen Informationen und namentlich keine besonders schützenswerte Personendaten unverschlüsselt übermittelt werden.

[2] Vorbehalten bleibt das Versenden von vertraulichen und geheimen Informationen namentlich von besonders schützenswerten Personendaten ohne Verschlüsselung, soweit die Dateneigner der vertraulichen Informationen und bei Personendaten die betroffenen Personen ausdrücklich damit einverstanden sind.

[3] Die private Nutzung von Internet und E-Mail ist in beschränktem Umfang zulässig. Sie ist auf ein Minimum zu beschränken und soll in der Regel ausserhalb der Arbeitszeiten stattfinden.

§ 25 *Missbrauch der Informatikmittel*

[1] Missbräuchlich ist jede Verwendung der Informatikmittel, die

a. gegen diese Verordnung verstösst,
b. gegen andere Bestimmungen der Rechtsordnung verstösst,
c. Rechte Dritter verletzt.

[2] Missbräuchlich sind insbesondere folgende absichtliche Handlungen:

a. Einrichten, Anschliessen oder Installation von Informatikmitteln entgegen den Bestimmungen dieser Verordnung,
b. Einloggen mit einem fremden Benutzerpasswort,
c. Nutzung von Informatikservices entgegen den geltenden Weisungen,

d. Manipulation von Informatikmitteln des Kantons, insbesondere Änderungen an vorgegebenen Konfigurationseinstellungen,
e. Ausnutzen von Fehlkonfigurationen,
f. Vorkehrungen zur Störung des Betriebs von Computern oder Netzwerken,
g. Erstellen, Speichern, Ausführen und Verbreiten von Fernsteuerungs-, Spionage- und Virenprogrammen (z.B. Viren, trojanische Pferde, Würmer oder Scripte),
h. Versenden von E-Mails in Täuschungs- oder Belästigungsabsicht und private Massenversendungen,
i. Zugreifen auf Informationen mit rassistischem, sexistischem, pornografischem oder gewaltverherrlichendem Inhalt sowie deren Erfassung, Verarbeitung, Speicherung und Übermittlung, soweit die Handlungen nicht im Rahmen eines dienstlichen Auftrags erfolgen,
j. widerrechtliches Kopieren von Informationen oder Software jeglicher Art,
k. widerrechtliches Bereitstellen, Verbreiten und Verwenden von urheberrechtlich geschützten Werken jeglicher Art (insbes. Filme, Musik und Fotos).

[3] Zur Gewährleistung der Sicherheit der Informatikmittel ist es dem oder der kantonalen Beauftragten für Informationssicherheit erlaubt, anerkannte Werkzeuge und Methoden für die Schwachstellenanalyse einzusetzen. Er oder sie kann eine externe Stelle mit dieser Analyse beauftragen. Der Leiter oder die Leiterin der Dienststelle Informatik ist vorgängig über die beabsichtigte Überprüfung zu informieren.

§ 26 *Notfallzugriff auf Informationen und E-Mails*

[1] Kann in einem dienstlichen Notfall vom betroffenen Anwender oder von der betroffenen Anwenderin nicht vorgängig die Zustimmung eingeholt werden, so kann bei den Organisations- und Informatikbeauftragten, beim Leiter oder bei der Leiterin der Dienststelle Informatik, bei deren Stellvertretung oder bei dem oder der kantonalen Beauftragten für Informationssicherheit Antrag gestellt werden, damit unter Aufsicht des oder der kantonalen Beauftragten für Informationssicherheit oder deren Stellvertretung auf das Postfach oder auf Dateien des persönlichen Laufwerks des Anwenders oder der Anwenderin zugegriffen werden kann, um dringend benötigte dienstliche Informationen zu beschaffen. Auf privat gekennzeichnete Unterordner, offensichtlich private oder als solche gekennzeichnete E-Mails oder Dateien darf nicht zugegriffen werden. Der betroffene Anwender oder die betroffene Anwenderin ist vom Leiter oder von der Leiterin der Dienststelle Informatik über den Vorgang schriftlich zu informieren.

4 Überwachung und Kontrollen

§ 27 *Zweck von Überwachung und Kontrolle*

[1] Die Massnahmen und Tätigkeiten zur Überwachung und Kontrolle der Informatikmittel dienen in erster Linie der Überprüfung und der Gewährleistung
a. der technischen Sicherheit,

b. der Funktionsfähigkeit,
c. der Verfügbarkeit der Informatikmittel.

[2] Überwachungs- und Kontrollmassnahmen dienen zudem
a. der Überprüfung und der Gewährleistung der Schutzziele gemäss § 7 dieser Verordnung,
b. der Prävention des Missbrauchs von Informatikmitteln,
c. dem personenbezogenen Nachweis des Missbrauchs von Informatikmitteln,
d. der Sicherstellung des wirtschaftlichen Einsatzes von Informatikmitteln.

§ 28 *Zuständigkeit für die Überwachung und Kontrolle*

[1] Die Organe und die Dienststelle Informatik haben die Informatikmittel in ihrem Zuständigkeitsbereich zu überwachen und zu kontrollieren.

[2] Die zuständigen Organe können die Ausführung von Aufgaben im Bereich der Überwachung und Kontrolle an andere Organe oder unabhängige Dritte delegieren. Der Leiter oder die Leiterin der Dienststelle Informatik und der oder die Beauftragte für den Datenschutz sind durch die Organe vor der Delegation rechtzeitig zu orientieren. *****

§ 29 *Überwachungs- und Kontrollmassnahmen*

[1] Informatikmittel werden, soweit wirtschaftlich und technisch sinnvoll, mit geeigneten technischen und organisatorischen Massnahmen vor unerwünschten Einwirkungen, technischen Störungen und missbräuchlicher Nutzung geschützt. Die Wirksamkeit der technischen Massnahmen wird mit Systemüberwachungssoftware und mittels Auswertung von Protokolldaten gewährleistet.

[2] E-Mails inklusive Attachments und als privat gekennzeichnete Informationen dürfen ohne vorgängige Zustimmung der betroffenen Personen nicht gelesen werden.

[3] Unzulässig sind die Erstellung und die Auswertung von Protokolldaten mit dem einzigen Zweck, personenbezogene Nutzungsprofile von Informatikmitteln zu erhalten. Ausgenommen sind Auswertungen, wenn Störungen festgestellt werden, welche die technische Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel ernsthaft gefährden, sowie Auswertungen bei begründetem Verdacht auf Missbrauch der Informatikmittel oder bei strafrechtlichen Vorfällen.

[4] Technische Überwachungs- und Kontrollinstrumente sowie Filtersperren sind zulässig.

[5] Gesicherte und archivierte Protokolldaten dürfen nur im Rahmen der gesetzlichen Vorgaben verwendet werden.

[6] Protokolldaten dürfen nur anonymisiert an Dritte übergeben werden. Ist es für die Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit oder der Verfügbarkeit der Informatikmittel zwingend, kann ausnahmsweise auf die Anonymisierung verzichtet werden. Vor der Übergabe von Protokolldaten an Dritte muss mit diesen eine Geheimhaltungsvereinbarung abgeschlossen werden.

§ 30 *Anonyme Auswertungen von Protokolldaten*

[1] Die Organisations- und Informatikverantwortlichen, der Leiter oder die Leiterin der Dienststelle Informatik, deren Stellvertretung und der oder die kantonale Beauftragte für Informationssicherheit können einzelne anonyme Auswertungen zur Überprüfung der Zweckerfüllung der Überwachungs- und Kontrollmassnahmen anordnen. Die eingesetzten Systemverantwortlichen sind für die Durchführung der angeordneten anonymen Auswertungen und für Auswertungen im Rahmen ihres dienstlichen Auftrages verantwortlich. Die Auswertungen können von der Dienststelle Informatik oder von Dritten manuell oder maschinell mittels spezieller Software durchgeführt werden.

[2] Anonyme Auswertungen zur Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit oder der Verfügbarkeit der Informatikmittel sind uneingeschränkt erlaubt.

§ 31 *Personenbezogene Auswertungen von Protokolldaten*

[1] Die zuständigen Departementssekretärinnen und -sekretäre, der Staatsschreiber oder die Staatsschreiberin, der Präsident oder die Präsidentin des Kantonsgerichtes, der Leiter oder die Leiterin der Dienststelle Informatik und der oder die kantonale Beauftragte für Informationssicherheit können ausnahmsweise einzelne personenbezogene Auswertungen zur Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit oder der Verfügbarkeit der Informatikmittel anordnen, wenn eine ernsthafte Gefährdung besteht und personenbezogene Auswertungen zur Störungsbehebung unumgänglich sind.

[2] Bei begründetem Verdacht auf Missbrauch von Informatikmitteln können die Departementssekretärinnen und -sekretäre, der Staatsschreiber oder die Staatsschreiberin und der Präsident oder die Präsidentin des Kantonsgerichtes ausnahmsweise einzelne personenbezogene Auswertungen anordnen, welche sich auch auf den Inhalt von E-Mails und auf Internetzugriffe beziehen. Über personenbezogene Auswertungen, welche sich auf den Inhalt von E-Mails und auf Internetzugriffe beziehen, müssen betroffene Personen sowie der oder die Beauftragte für den Datenschutz vorgängig schriftlich informiert werden. *****

[3] Der Leiter oder die Leiterin der Dienststelle Informatik ist für die Durchführung von personenbezogenen Auswertungen zuständig. Die Auswertungen können manuell oder mittels spezieller Software durchgeführt werden.

[4] Dem oder der Beauftragten für den Datenschutz und den betroffenen Personen ist nachträglich über die durchgeführten Auswertungen Bericht zu erstatten. Den betroffenen Personen sind die sie betreffenden Auswertungsresultate mitzuteilen, ausser wenn eine solche Auswertung im Rahmen eines Ermittlungs- oder Strafverfahrens erfolgt ist und die Strafprozessordnung darauf Anwendung findet. *****

§ 32 *Aufbewahrung von Protokolldaten*

[1] Protokolldaten werden mindestens sechs Monate und längstens zwei Jahre beziehungsweise spätestens bis zum Abschluss eines Straf-, Zivil- oder Verwaltungsverfahrens aufbewahrt.

[2] Personenbezogene Protokolle und Protokolldaten werden sechs Monate beziehungsweise spätestens bis zum Abschluss eines Straf-, Zivil- oder Verwaltungsverfahrens aufbewahrt und danach irreversibel vernichtet.

[3] Nach Ablauf der Aufbewahrungsfrist werden die Protokolldaten gelöscht. Archiv-, Backup- und Sicherungsdaten bleiben davon unberührt.

[4] Archiv-, Backup- und Sicherungsdaten dürfen nur innerhalb der Fristen gemäss den Absätzen 1 und 2 zum Zweck der Kontrolle und zur Überwachung des Nutzerverhaltens verwendet werden.

5 Überprüfung des Vollzugs

§ 33 *Vollzug*

[1] Der Regierungsrat und der Präsident oder die Präsidentin des Kantonsgerichtes sind für die Überprüfung des Vollzugs dieser Verordnung mittels Auswertung von Protokolldaten zuständig.

[2] Die gemäss Absatz 1 zuständige Behörde kann durch den Leiter oder die Leiterin der Dienststelle Informatik unter den Voraussetzungen gemäss § 30 anonyme Plausibilitätskontrollen (Stichproben) über eine beschränkte vergangene oder zukünftige Benutzungsdauer durchführen lassen, um den Vollzug dieser Verordnung zu überprüfen.

[3] Besteht begründeter Verdacht auf Missbrauch von Informatikmitteln, kann die gemäss Absatz 1 zuständige Behörde unter den Voraussetzungen gemäss § 31 personenbezogene Auswertungen von Protokolldaten durchführen lassen.

§ 34 *Sanktionen*

[1] Bei Verstoss gegen die Rechtsordnung im Zusammenhang mit der Nutzung von Informatikmitteln und bei Verstoss gegen diese Verordnung können die personalrechtlich vorgesehenen Sanktionen ergriffen werden, soweit für die betroffenen Personen das Personalrecht des Kantons Luzern anwendbar ist.

[2] Gegen Lernende der kantonalen Schulen, welche im Zusammenhang mit der Nutzung von Informatikmitteln gegen die Rechtsordnung oder gegen diese Verordnung verstossen, können bildungsrechtlich vorgesehene Massnahmen ergriffen werden.

[3] Die Strafverfolgung und die Geltendmachung zivilrechtlicher Ansprüche bleiben vorbehalten.

§ 35 *Umsetzungsfristen*

[1] Die Umsetzung der §§ 15 Absatz 4, 20 und 32 Absatz 1 hat bis zum 31. Dezember 2018 zu erfolgen.

[2] Die Umsetzung der §§ 8 Absatz 3 und 24 Absatz 1 hat bis zum 31. Dezember 2022 zu erfolgen. *****

Änderungstabelle - nach Paragraf

Element	Beschlussdatum	Inkrafttreten	Änderung	Fundstelle G
Erlass	22.11.2016	01.01.2017	Erstfassung	G 2016-54
Ingress	23.08.2021	01.09.2021	geändert	G 2021-055
§ 2 Abs. 1	20.11.2018	01.01.2019	geändert	G 2018-072
§ 2 Abs. 3	02.03.2021	01.08.2021	geändert	G 2021-013
§ 2 Abs. 4	02.03.2021	01.08.2021	eingefügt	G 2021-013
§ 3 Abs. 2	02.03.2021	01.08.2021	geändert	G 2021-013
§ 3 Abs. 3	23.08.2021	01.09.2021	geändert	G 2021-055
§ 8 Abs. 3	23.08.2021	01.09.2021	geändert	G 2021-055
§ 11 Abs. 3	23.08.2021	01.09.2021	geändert	G 2021-055
§ 23 Abs. 2	23.08.2021	01.09.2021	geändert	G 2021-055
§ 28 Abs. 2	23.08.2021	01.09.2021	geändert	G 2021-055
§ 31 Abs. 2	23.08.2021	01.09.2021	geändert	G 2021-055
§ 31 Abs. 4	23.08.2021	01.09.2021	geändert	G 2021-055
§ 35 Abs. 2	10.12.2019	01.01.2020	geändert	G 2019-075

Änderungstabelle - nach Beschlussdatum

Beschlussdatum	Inkrafttreten	Element	Änderung	Fundstelle G
22.11.2016	01.01.2017	Erlass	Erstfassung	G 2016-54
20.11.2018	01.01.2019	§ 2 Abs. 1	geändert	G 2018-072
10.12.2019	01.01.2020	§ 35 Abs. 2	geändert	G 2019-075
02.03.2021	01.08.2021	§ 2 Abs. 3	geändert	G 2021-013
02.03.2021	01.08.2021	§ 2 Abs. 4	eingefügt	G 2021-013
02.03.2021	01.08.2021	§ 3 Abs. 2	geändert	G 2021-013
23.08.2021	01.09.2021	Ingress	geändert	G 2021-055
23.08.2021	01.09.2021	§ 3 Abs. 3	geändert	G 2021-055
23.08.2021	01.09.2021	§ 8 Abs. 3	geändert	G 2021-055
23.08.2021	01.09.2021	§ 11 Abs. 3	geändert	G 2021-055
23.08.2021	01.09.2021	§ 23 Abs. 2	geändert	G 2021-055
23.08.2021	01.09.2021	§ 28 Abs. 2	geändert	G 2021-055
23.08.2021	01.09.2021	§ 31 Abs. 2	geändert	G 2021-055
23.08.2021	01.09.2021	§ 31 Abs. 4	geändert	G 2021-055