Verordnung über die Informationssicherheit (VIS)

Vom 11. März 2008

GS 36.0543

Der Regierungsrat des Kantons Basel-Landschaft und die Geschäftsleitung des Kantonsgerichts, gestützt auf § 14 Absatz 2 des Datenschutzgesetzes vom 7. März 1991[1], beschliessen:

A. Allgemeine Bestimmungen

§ 1 Zweck und Zielsetzung

[1] Diese Verordnung regelt den Schutz der Informatik-Systeme des Kantons vor Systemausfällen und den Schutz der mit solchen Systemen bearbeiteten Informationen vor Verlust sowie unbefugter Kenntnisnahme und Veränderung.

[2] Oberstes Ziel ist die Kenntnis der aktuellen Risiken der Informationssicherheit und deren systematische und verhältnismässige Behandlung zu angemessenen Kosten.

[3] Erkannte Risiken werden verwaltungsweit einheitlich bewertet und durch angemessene Massnahmen auf ein akzeptables Restrisiko beschränkt.

[4] Ein existenzbedrohendes Risiko muss auf ein wirtschaftlich akzeptables Mass beschränkt werden. Erscheint dies aus technischen oder finanziellen Gründen nicht möglich, ist das Vorhaben abzulehnen oder abzubrechen.

[5] Über die Zulässigkeit eines Restrisikos und dessen anzustrebende Deckung entscheiden die finanzkompetenten Stellen.

[6] Risiken werden von den verantwortlichen Linienstellen getragen.

[7] Die vorhandenen Risiken sind mindestens alle 3 Jahre gesamthaft zu evaluieren und gegebenenfalls in eine entsprechende Verbesserungsplanung einzubringen.

§ 2 Geltungsbereich und Abgrenzung

[1] Diese Verordnung gilt für die Direktionen und ihre Dienststellen (inklusive kantonale Spitäler), die Landeskanzlei, das Kantonsgericht und die kantonalen Schulen.

1 GS 30.625, SGS 162

[2] Sie gilt für sämtliche Informatik-Systeme und darauf bearbeitete Informationen.

[3] Soweit keine anderen Regeln bestehen, gilt sie auch für nicht mittels Informatik bearbeitete Informationen.

[4] Bei der Zusammenarbeit mit Organisationen und Personen ausserhalb des Geltungsbereichs dieser Verordnung sind die hier festgelegten Grundsätze soweit wie möglich vertraglich zu vereinbaren.

§ 3 Ergänzende Regelungen

[1] Die Direktionen, die Landeskanzlei, das Kantonsgericht und die kantonalen Schulen können in ihrem Kompetenzbereich strengere Sicherheitsanforderungen festlegen.

[2] Die Fachgruppe Informatik (FGI) kann einzelne Aspekte dieser Verordnung konkretisieren und entsprechende ergänzende Weisungen zur Informationssicherheit erlassen, insbesondere zur Regelung von anzuwendenden Verfahren, generell gültigen Mindestanforderungen und zum Umgang mit vernetzungsbedingten Sicherheitsrisiken.

[3] Die FGI kann einzelnen dieser Verordnung unterstellten Institutionen einen erhöhten Freiheitsgrad zugestehen, solange

a. dadurch keine erhöhte Bedrohung der restlichen Institutionen entsteht;
b. ein eigenes Informationssicherheits-Managementsystem branchenüblicher Qualität betrieben und jährlich die vorhandenen Risiken der Informationssicherheit und die Verbesserungsplanung rapportiert werden;
c. mindestens alle drei Jahre die Angemessenheit des Managements der Informationssicherheit und der vorhandenen Risiken durch eine unabhängige Stelle zuhanden des oder der zentralen Informationssicherheitsbeauftragten nachgewiesen wird.

[4] Der zugestandene erhöhte Freiheitsgrad kann widerrufen werden, wenn die Voraussetzungen nicht mehr erfüllt sind.

B. Begriffe und Schnittstellen der Informationssicherheit

§ 4 Leistungserbringer und Leistungsbezüger

[1] Die Betreibenden der Informatik-Systeme sind die Leistungserbringenden.

[2] Die Benutzenden der Informatik-Systeme sind die Leistungsbeziehenden.

§ 5 Informationen

[1] Informationen im Sinne dieser Verordnung sind Daten jeglicher Art, die für Leistungsbeziehende oder -erbringende von Bedeutung sind.

[2] Informationen werden entsprechend ihrem Schutzbedarf anhand eines Rasters klassifiziert.

[3] Die Kriterien für die Klassifizierung sind Vertraulichkeit, Integrität und Verfügbarkeit der Informationen. Sie werden verwaltungsweit einheitlich festgelegt.

§ 6 Informatiksicherheit

Informatiksicherheit dient dem Schutz der elektronisch bearbeiteten Informationen.

§ 7 Physische Sicherheit der IT-Infrastruktur (Anlagenschutz)

Die für den Betrieb der Informatik-Infrastruktur notwendigen physischen Einrichtungen sind zu schützen.

§ 8 Service Level Agreements

[1] Leistungsbeziehende und Leistungserbringende legen alle Anforderungen an die Dienstleistung, insbesondere auch die Anforderungen zur Gewährleistung der Informationssicherheit in einem schriftlichen Service Level Agreement fest.

[2] Die Sicherheitsmassnahmen sind schriftlich festzulegen.

C. Grundsätze der Informationssicherheit

§ 9 Sicherheitsbewusstsein

Das Sicherheitsbewusstsein der Mitarbeitenden ist regelmässig zu schulen und eine Sicherheitskultur zu pflegen.

§ 10 Konzeptioneller Rahmen

Anzustreben ist ein Management der Informationssicherheit nach den Normen der ISO 27000 Familie.

§ 11 Wirtschaftlichkeit und Angemessenheit

Die Schutzmassnahmen müssen immer in einem angemessenen wirtschaftlichen Verhältnis zum möglichen Schaden stehen.

§ 12 Projekte und Systemanpassungen

[1] Im Rahmen von Projekten und Systemanpassungen hat die verantwortliche Stelle frühzeitig die Anforderungen an die Informationssicherheit festzulegen und zu berücksichtigen. Es gelten die Richtlinien gemäss der Projektführungsmethodik HERMES.

[2] Ein Projekt gilt frühestens dann als abgeschlossen, wenn die Informationssicherheit auch während des Betriebs und bei späteren Anpassungsarbeiten in genügendem Umfang gewährleistet ist.

[3] Für die Betriebsfreigabe muss eine Risikobeurteilung durch eine neutrale Fachperson und eine Bestätigung der Übernahme der Restrisiken durch den Leistungsbezüger vorliegen.

§ 13 Richtlinien zur Nutzung der Informatik

Richtlinien und Weisungen zur Nutzung der Informatik sind durch die FGI weiterzuentwickeln und regelmässig auf Einhaltung zu kontrollieren.

§ 14 Kostenmanagement

Die Kosten für die Informatiksicherheit sind Teil der Projekt- und Betriebskosten und dementsprechend zu budgetieren.

§ 15 Sicherheitsmassnahmen und ihre schriftliche Dokumentation

[1] Sicherheitsmassnahmen sind organisatorischer, technischer oder physischer Natur.

[2] Sie sind systematisch und in einem konzeptionellen Rahmen zu vollziehen sowie schriftlich zu dokumentieren.

[3] Für alle Anwendungen, Projekte und Datensammlungen wird eine zentrale Liste mit sicherheitsrelevanten Informationen geführt. Der oder die Informatiksicherheitsbeauftragte der Direktion (DIT-SiBe) hat Einsicht in das Portfolio oder führt es selber.

§ 16 Datenschutzfreundliche Technologien

[1] Bei der Beschaffung von Informatikmitteln zur Verwaltung von Personendaten ist die Datenschutzfreundlichkeit der Technologien angemessen zu berücksichtigen.

[2] Bevor Informatikmittel zu diesem Zweck beschafft werden, ist die zuständige Datenschutzbehörde anzuhören.

§ 17 Benutzerfreundlichkeit

Bei der Evaluation von Sicherheitslösungen wird auch deren Benutzerfreundlichkeit bewertet.

§ 18 Zugangsbeschränkungen

Benutzerprofile haben den Zugang auf diejenigen Informationen zu beschränken, welche für die Aufgabenerfüllung notwendig sind.

§ 19 Notfallkonzept

[1] Leistungsbeziehende und Leistungserbringende erstellen je eigene Notfallkonzepte und stimmen diese aufeinander ab.

[2] Die Notfallkonzepte regeln das Vorgehen bei einem Ausfall von Informatik-Systemen, der länger als die definierten Verfügbarkeitsanforderungen dauert.

D. Organisation und Verantwortung

§ 20 Grundsatz

Alle Mitarbeitende sind im Rahmen ihrer Tätigkeiten für die Wahrung der Sicherheit verantwortlich.

§ 21 Informationssicherheitsbeauftragte auf Stufe Kanton

[1] Die Informatikplanung und -koordination (IPK) übernimmt die Aufgaben des/der zentralen Informationssicherheitsbeauftragten (KIT-SIBE).

[2] Der/die KIT-SIBE

a. koordiniert alle kantonsinternen und kantonsübergreifenden Informationssicherheitsaspekte;
b. steht zur Überprüfung der Anforderungen und zur Aufsicht im Bereich der Informationssicherheit zur Verfügung, ist jedoch nicht für deren Durchsetzung verantwortlich;
c. stellt periodisch, mindestens aber alle 3 Jahre, einen Risikobericht und eine gesamtheitliche Massnahmenplanung zusammen;
d. koordiniert zwischen den Direktionen, der Landeskanzlei, dem Kantonsgericht und den kantonalen Schulen und stellt einheitliche Verfahren zum Umgang mit Informations- und Informatik-Sicherheit zur Verfügung.

§ 22 Informationssicherheitsbeauftragte auf Stufe Direktion

[1] Jede Direktion, die Landeskanzlei, das Kantonsgericht und die kantonalen Schulen bestimmen eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten (DIT-SIBE).

[2] Die oder der DIT-SIBE koordiniert direktionsweit im Rahmen seiner bzw. ihrer Aufgaben, Kompetenzen und Verantwortung, die Sicherheitsanliegen im Bereich Informationssicherheit mit Schwergewicht Informatik und stimmt diese mit dem oder der zentralen KIT-SIBE ab.

§ 23 Leistungsbeziehende und Leistungserbringende

[1] Die Leistungsbeziehenden legen in Abstimmung mit dem oder der DIT-SIBE die Sicherheitsanforderungen für Projekte, Anwendungen und Datensammlungen fest und organisieren unter Einbezug der Auftraggebenden und der Vertragspartner periodisch die Kontrollen der Umsetzung der Sicherheitsmassnahmen.

[2] Die Direktionen, die Landeskanzlei das Kantonsgericht und die kantonalen Schulen sind dafür verantwortlich, dass ihre Mitarbeitenden die zuständigen

Stellen/Organe und die Abläufe der Informationssicherheit in der Kantonsverwaltung stufengerecht kennen.

[3] Die Leistungserbringenden haben die von den Leistungsbeziehenden definierten Vorgaben einzuhalten.

[4] Die Verantwortlichen stellen sicher, dass die Sicherheitsmassnahmen beim Betrieb von Informations- und Kommunikationstechnik auf allen Systemen und für alle involvierten Personen umgesetzt werden.

[5] Die Verantwortlichkeiten auf der operativen Ebene werden in den Projektvereinbarungen und in den Service Level Agreements zwischen den Leistungsbezügern und den Leistungserbringern detailliert festgehalten.

[6] Der/die Leistungsbeziehende muss zuhanden des/der DIT-SIBE eine periodische Überprüfung der vorgenommenen Umsetzung der Informatiksicherheit und der vorhandenen Sicherheitsrisiken bei sich und beim Leistungserbringer vornehmen.

§ 24 Informationsschutz

Die Direktionen, die Landeskanzlei, das Kantonsgericht und die kantonalen Schulen sind dafür verantwortlich, die in ihrer Zuständigkeit bearbeiteten Informationen gemäss bestehenden Weisungen angemessen zu schützen.

§ 25 Mitarbeitende

[1] Die Mitarbeitenden sind für die Einhaltung von Sicherheitsbestimmungen in ihrem Arbeitsbereich verantwortlich.

[2] Als Verfassende von Informationen sind sie für deren Klassifizierung und Schutz besorgt.

§ 26 Kontinuierlichen Verbesserung

[1] Die Direktionen, die Landeskanzlei, das Kantonsgericht und die kantonalen Schulen überprüfen mindestens alle 3 Jahre, ob die Sicherheitsmassnahmen angemessen sind und ob sie umgesetzt werden.

[2] Die Ergebnisse werden zuhanden des/der KIT-SIBE und der Aufsichtsstelle Datenschutz rapportiert.

[3] Es besteht ein kontinuierliches Verbesserungsprogramm.

E. Einführung der Verordnung

§ 27 Einführung der Verordnung

[1] Diese Verordnung wird schrittweise nach Massgabe der jeweils vorhandenen Risiken umgesetzt.

[2] Innerhalb von 24 Monaten nach Inkrafttreten dieser Verordnung sind

a. die Organisation und die Verfahren zur Bestimmung von angemessenen Massnahmen und den vorhandenen Risiken umzusetzen;

b. Massnahmen mit sehr gutem Verhältnis von Kosten zu Nutzen zu treffen;

c. der erste Bericht zur Informationssicherheit zu erstellen;

d. die erste Fassung des kontinuierlichen Verbesserungsprogrammes zuhanden des Regierungsrates zu erstellen.

[3] Die übrigen Massnahmen sind so rasch als möglich umzusetzen.

[4] Der/die KIT-SIBE erarbeitet gemeinsam mit der FGI das kontinuierliche Verbesserungsprogramm.

§ 28 Inkrafttreten

Diese Verordnung tritt am 30. Juni 2008 in Kraft.

Liestal, 11. März 2008

Im Namen des Regierungsrates
die Präsidentin: Pegoraro
der Landschreiber: Mundschin