Vorlage an den Landrat des Kantons Basel-Landschaft - Übersicht

---

Titel:	**Postulat der PUK Informatik "Datenschutz und Datensicherheit"**
Datum:	11. März 2008
Nummer:	2008-057
Bemerkungen:	**Verlauf dieses Geschäfts**

Links:

- Übersicht Geschäfte des Landrats
- Hinweise und Erklärungen zu den Geschäften des Landrats
- Landrat / Parlament des Kantons Basel-Landschaft
- Homepage des Kantons Basel-Landschaft

2008/057

Kanton Basel-Landschaft **Regierungsrat**

Vorlage an den Landrat

betr. Postulat der PUK Informatik „Datenschutz und Datensicherheit“

Vom 11. März 2008

1. EINLEITUNG

Der Landrat überwies am 14. Oktober 2004 das Postulat der Parlamentarischen Untersuchungskommission Informatik „Datenschutz und Datensicherheit“, Geschäftsnummer 2004/195, an den Regierungsrat. Es hat folgenden Wortlaut:

«Die Regierung wird beauftragt, ein Datenschutz- und Datensicherheitskonzept für Informatikprojekte zu erarbeiten, mit einer rechtlichen Grundlage den Persönlichkeits- und Datenschutz und die Datensicherheit für alle Informatikanwendungen zu klären und zu garantieren, den frühzeitigen Beizug von Datenschutzfachleuten bei allen Informatikprojekten sicherzustellen und einen Leitfaden für Projektleiter/innen und Anwender/innen auszuarbeiten.»

2. GRUNDLAGEN

Informationen zählen zu den wertvollsten Gütern der Verwaltung - diese gilt es zu schützen. Mit der zunehmenden Durchdringung der Verwaltung mit Informations-Technologie (IT) gewinnt die Informationssicherheit ständig an Bedeutung. In Anbetracht der heutigen Möglichkeiten für Informationszugriffe und der immer weitergehenden Vernetzung ist es wichtig, eine Übersicht über die vorhandenen Risiken der Informationssicherheit zu haben und diese dann systematisch anzugehen. Weil sich die Sicherheitsrisiken in einer lebendigen IT-Landschaft laufend verändern, muss die Risikoentwicklung auch entsprechend überwacht werden. Die Verwaltung stellt damit sicher, dass inakzeptable Risiken vermieden werden und dass die Informationssicherheit im erforderlichen Umfang gewährleistet werden kann, wie er sich aus der verfassungsrechtlichen Verantwortung und sinngemäss aus den anerkannten Regeln für das kaufmännische Gewerbe ergibt.

Die geregelte Umsetzung der Datensicherheit ist in zahlreichen öffentlichen Verwaltungen Standard. Die Ausarbeitung der vorliegenden Lösung basiert deshalb zum einen auf praxiserprobten Regelungen von Kantonen und des Bundes, zum andern aber auf den aktuellen Fassungen der internationalen Normen zum Management der Informationssicherheit, der ISO 27000-Familie.

3. DIE VERORDNUNG ÜBER DIE INFORATIONSSICHERHEIT

a) Einleitung

Im Sinne eines Leitbildes zur Informationssicherheit hat der Regierungsrat mit RRB Nr. … vom … die «Verordnung über die Informationssicherheit» in Kraft gesetzt[1].

Die Verordnung über die Informationssicherheit (VIS) regelt Ziele und Grundsätze der Informations- und Informatiksicherheit sowie die zugehörige Organisation und Verantwortung. Die Fachgruppe für Informatik (FGI) ist beauftragt, weiterführende Regelungen auszuarbeiten. Basierend auf dieser VIS wurden einzelne Aspekte konkretisiert und als „Anforderungen an die Informationssicherheit“ zusammengestellt. Die VIS orientiert sich inhaltlich an den Normen ISO 27001 und ISO 17799. ISO 17799 wird in Zukunft in die Norm ISO 27002 übergehen. Um auch zukünftige Entwicklungen in der Normenwelt zu antizipieren, ist deshalb wo immer möglich, von der Normen-Familie ISO 27000 die Rede. Das bedeutet aber auch, dass sich nicht nur die Bedrohungs- und Risiko-Situation, sondern auch das „Bekämpfungs-Hilfsmittel“ in Form der internationalen Normen ständig verändern.
Allein diese Tatsache zeigt, dass es sich bei Informationssicherheit um ein "bewegliches Ziel", ein so genanntes „Moving Target“ handelt, das sich folglich nur mit Dauereinsatz verfolgen lässt. Isolierte Einzelinitiativen bringen hier nur sehr bedingten Erfolg.

Die „Anforderungen an die Informationssicherheit“ wurden am 18.12.2006 resp. 19.3.2007 von der FGI verabschiedet. Die auf diese Anforderungen antwortende VIS dokumentiert die obersten Grundsätze zum Umgang mit Risiken der Informations- und Informatiksicherheit und zur Risikotransparenz im Besonderen. Damit sind die wesentlichen Grundlagen der Informationssicherheit, wie es ihrer Bedeutung entspricht, durch den Regierungsrat abgestützt und somit stark verankert. Zusätzlich ist die Verordnung an öffentlicher Stelle publiziert und adressatengerecht von allen Betroffenen und Beteiligten (d.h. sowohl von verwaltungsinternen Stellen und Personen als auch von externen Dienstleistern) jederzeit einsehbar. Zudem wird dadurch vermieden, dass die grundlegenden Anforderungen zur Informationssicherheit auf verschiedene Dokumente verteilt werden.

---

[1] In der Privatwirtschaft wird dies „Leitbild Informationssicherheit“, „Information Security Policy“ oder Informations-

Die Verordnung über die Informationssicherheit regelt auch die Sicherheit in Bereichen, die bisher durch die Datenschutzverordnung erfasst waren. Deshalb hat der Regierungsrat Anpassungen an der Datenschutzverordnung vorgenommen.

b) Grundlagen

Als Rechtsgrundlage für die Verordnung über die Informationssicherheit dient das Datenschutzgesetz. Massnahmen zur Gewährleistung der Nachvollziehbarkeit von Informationsbearbeitungen und der Verfügbarkeit von Informationen sind auch auf Grund der allgemein anerkannten kaufmännischen Grundsätze erforderlich, denen ja auch die Verwaltung sinngemäss unterliegt. Als bereits bestehende Grundlage unterstützt die Projektmanagement-Methode HERMES die Abwicklung von Informatik-Projekten als Leitfaden für Projektleitenden. Informationssicherheit und Datenschutz (ISDS) sind Bestandteil dieser Methode. Die Projektleitenden werden zu diesen Themen hinreichend in Kenntnis gesetzt, so dass sich ein zusätzlicher Leitfaden für diese erübrigt. HERMES definiert auch den Zeitpunkt, wann diese Themen bearbeitet werden müssen.

c) Übersicht über die «Verordnung über die Informationssicherheit»

A. Allgemeine Bestimmungen (§§ 1 - 3)

Die Zweckbestimmung nennt die mit der Informationssicherheit verfolgten Ziele. Es gilt zu verhindern, dass Systemausfälle die behördliche Arbeit unangemessen erschweren oder verhindern. Zudem ist sicherzustellen, dass die mit IT-Systemen bearbeiteten Informationen ausschliesslich den befugten Stellen in der nötigen Qualität – also unverfälscht – zur Verfügung stehen. Dazu werden gemeinsame, grundlegende Sicherheitsanforderungen an die Informationssicherheit definiert.

Die VIS gilt für die Direktionen und ihre Dienststellen (inklusive kantonale Spitäler), die Landeskanzlei, das Kantonsgericht und die kantonalen Schulen. Da der Kanton mit externen Stellen zusammenarbeitet (insbesondere Privatunternehmen, die mit den IT-Abteilungen kooperieren und Gemeinden, die am Kantonsnetz angeschlossen sind), müssen auch diese demselben Sicherheitsstandard unterworfen werden.

Für einen angemessenen Schutz ist es von zentraler Bedeutung, dass die Risiken der Informationssicherheit rechtzeitig erfasst und bewertet werden. In einer mindestens alle 3 Jahre vorzunehmenden Gesamtevaluation sind gegebenenfalls weitere Verbesserungen zu planen. Das verbleibende Restrisiko muss von einer entsprechend finanzkompetenten Linienstelle aktiv übernommen werden. Der FGI wird die Aufgabe übertragen, die Anforderungen an die Informationssicherheit zu konkretisieren. Unter bestimmten Voraussetzungen kann die FGI einzelnen der VIS

Sicherheitspolitik genannt.

unterstellten Institutionen einen erhöhten Freiheitsgrad zugestehen, was diese aber nicht vom regelmässigen Nachweis der Angemessenheit ihrer Sicherheitsmassnahmen entbindet.

B. Begriffe und Schnittstellen der Informationssicherheit (§§ 4 - 8)

In diesem Abschnitt werden die wichtigsten Begriffe und Schnittstellen definiert. Der Datenschutz und dessen Schnittstellen werden hier nicht erwähnt. Er ist in den entsprechenden Gesetzen und Verordnungen hinreichend definiert und gilt im Hinblick auf Informationssicherheit vor allem als ein Aspekt der Vertraulichkeit und teilweise der Integrität, im Sinne des Korrektheitsanspruches an die Personeninformation.

C. Grundsätze der Informationssicherheit (§§ 9 - 19)

Die wesentlichen Grundsätze der Informationssicherheit sind:

- Das Sicherheitsbewusstsein jedes Einzelnen.
- Die Orientierung an den Normen der Familie ISO 27000.
- Massnahmen müssen in einem angemessenen wirtschaftlichen Verhältnis zum möglichen Schaden stehen und enthalten auch Personal- und Organisationskosten.
- IT-Projekte sind erst abgeschlossen, wenn der Schutz in genügendem Umfang gewährleistet ist.
- Weisungen und Richtlinien zur elektronischen Bearbeitung von Informationen sind laufend weiterzuentwickeln.
- Die Kosten für IT-Sicherheit sind in den Projekten entsprechend zu budgetieren. Auch eine allfällige Erhöhung von Betriebskosten als Folge von Sicherheitsmassnahmen.
- Alle Sicherheitsmassnahmen sind zu dokumentieren.
- Die zuständigen Aufsichtstellen des Datenschutzes sind auch bei der Beschaffung von IT-Sicherheitslösungen anzuhören.
- Benutzende erhalten nur soviel Informationszugriff, wie sie zur Erfüllung ihrer Aufgaben benötigen («Need-to-Know»-Prinzip).
- Für den Betrieb der IT-Systeme sind Notfallkonzepte auszuarbeiten, die das Vorgehen bei übermässigen Störungen und Systemausfällen regeln.

D. Organisation und Verantwortung (§§ 20- 26)

In diesem Abschnitt werden die Aufgaben und Verantwortungen definiert: Als Grundsatz wird festgehalten, dass die Direktionen, respektive sinngemäss die Landeskanzlei, das Kantonsgericht und die kantonalen Schulen dafür verantwortlich sind, die in ihrer Zuständigkeit bearbeiteten Informationen angemessen zu schützen. Sie überprüfen auch, ob die Sicherheitsmassnahmen angemessen und umgesetzt sind. Auf der operativen Ebene regeln Projektvereinbarungen und

Service Level Agreements die Verantwortlichkeiten. Als allgemeiner Grundsatz wird zudem daran erinnert, dass alle Mitarbeitenden die Sicherheitsbestimmungen einhalten müssen. Geregelt wird auch die Koordination der Informationssicherheit auf Stufe Kanton und auf Stufe Direktion.

E. Einführung der Verordnung (§§ 27-28)

Die Umsetzung soll schrittweise nach Massgabe der vorhandenen Risiken erfolgen.
Die Verfahren und die Organisation zur Bestimmung von angemessenen Risiken und Schutzmassnahmen sind innert 24 Monaten nach Inkrafttreten umzusetzen.

4. ANPASSUNG VON GELTENDEM RECHT

Die Verordnung über die Informationssicherheit regelt die Sicherheit in Bereichen, die bisher durch die §§ 2-7 der Datenschutzverordnung erfasst waren. Daraus folgt, dass nun in der Datenschutzverordnung erstens der Vorrang der VIS-Regelungen festzuschreiben ist (neuer § 1a Datenschutzverordnung). Weil es der VIS nicht unterstellte Bereiche gibt, in denen die DSV Gültigkeit hat, dürfen die entsprechenden DSV Paragrafen nicht einfach aufgehoben werden.

5. FINANZIELLE AUSWIRKUNGEN

Die initiale Umsetzung der Organisation und der Verfahren zur Bestimmung von Risiken und Massnahmen soll mit dem bestehenden Stellenbestand und im Rahmen der aktuellen Budgetierung erfolgen. Gemäss Beschluss der FGI vom 18.12.2006 wird der für die Umsetzung der Verordnung notwendige Bedarf an zusätzlichen Ressourcen im Rahmen der IT Strategie der kantonalen Verwaltung diskutiert.
Verbesserungsmassnahmen und -projekte sind jeweils im Rahmen der kontinuierlichen Verbesserungsplanung einzubringen. Im gleichen Rahmen ist gegebenenfalls die Stellensituation zu überprüfen. Da es sich um jeweils aufeinander aufbauende Verbesserungszyklen handelt, ist es nicht möglich, zum jetzigen Zeitpunkt zuverlässige Kostenschätzungen für das Ziel „umgesetzte, angemessene Schutzmassnahmen“ abzugeben. Andererseits hat sich eine flächendeckende, einheitliche Umsetzung vordefinierter Massnahmen, was in einem gewissen Rahmen zu kalkulierbaren Kosten erfolgen kann, als wenig zielführend, respektive zu kostenintensiv für die damit erreichbaren Ziele erwiesen. Dies ist auch der Grund, warum die aktuellen Normen die Umsetzung von Sicherheit auf Basis eine qualitativ hochwertigen Managementsystems fordern, weil nur so, mit einem sogenannten risikoorientierten Ansatz, eine den sich ständig ändernden Bedingungen angemessene und kosteneffiziente Umsetzung erfolgen kann.

Die an IT-Projekten und am -Betrieb beteiligten Leistungsbeziehenden haben im Rahmen der Definition der Sicherheitsanforderungen und der Sicherheitskontrollen mit einem gewissen Mehraufwand zu rechnen. Dieser Mehraufwand verteilt sich auf eine Vielzahl von Dienststellen und Mitarbeitende in einem jeweils verhältnismässig kleinen Umfang. Eine qualifizierte Schätzung der finanziellen Auswirkungen ist aus diesen Gründen nicht möglich.

6. ANTRAG

Der Regierungsrat beantragt dem Landrat, das Postulat „Datenschutz und Datensicherheit“ der Parlamentarischen Untersuchungskommission Informatik abzuschreiben.

Liestal, 11. März 2008

IM NAMEN DES REGIERUNGSRATES

Die Präsidentin:

Pegoraro

der Landschreiber:

Mundschin

Beilage: Verordnung über die Informationssicherheit

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

Verordnung zum Datenschutzgesetz

Änderung vom 11. März 2008

GS 36.0550

Der Regierungsrat des Kantons Basellandschaft beschliesst:

I.
Die Verordnung vom 13. August 1991[1] zum Datenschutzgesetz wird wie folgt geändert:

§ 1a Vorrang der Verordnung über die Informationssicherheit
Die §§ 2-7 dieser Verordnung gelten für alle Datenbearbeitungen und für alle IT-Systeme, auf welche die Verordnung über die Informationssicherheit (VIS) nicht anwendbar ist oder für welche noch keine Sicherheitsmassnahmen im Sinne von § 1 der VIS festgelegt sind.

§ 3 Absätze 3 und 4
[3] IT-Systeme umfassen die Hardware (inklusive sämtliche Verbindungen zu anderen Systemen, die Betriebssysteme und die systemnahe Software) und die IT-Anwendungen, die für die Bearbeitung von Personendaten eingesetzt werden.
[4] IT-Anwendungen sind die Programme und die dazugehörigen Daten für die IT-unterstützte Erfüllung behördlicher Aufgaben.

§ 4 Zutritt zu den Räumen
Es dürfen nur berechtigte Personen freien Zutritt zu Räumlichkeiten haben, in denen sich Datenträger oder grössere Datensammlungen (Datenbanken etc.) befinden.

§ 5 Absatz 2
[2] IT-Anwendungen für die Bearbeitung von Personendaten sind so zu speichern und zu sichern, dass sie nötigenfalls rekonstruiert werden können.

1 GS 30.634, SGS 162.11

§ 6 Titel, Absätze 1 und 2
Zugriff auf IT-Systeme
[1] Es dürfen nur berechtigte Personen Zugriff auf das IT-System haben.
[2] Es ist durch technische Massnahmen dafür zu sorgen, dass der Zugang zum IT-System nur mit Hilfe von persönlichen Passworten möglich ist. Die persönlichen Passworte sind periodisch zu wechseln. Die Passworte sind geheim zu halten.

II.
Diese Änderung tritt am 30. Juni 2008 in Kraft.

Liestal, 11. März 2008

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