Verordnung zur Informatiksicherheit (ISV)

Vom 9. April 2002 (Stand 1. Januar 2012)

Der Regierungsrat des Kantons Basel-Stadt

erlässt, gestützt auf § 8 Abs. 4 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 [1)] sowie § 4 des Gesetzes betreffend die Organisation des Regierungsrates und der Verwaltung des Kantons Basel-Stadt (Organisationsgesetz) vom 22. April 1976 [2)], folgende Verordnung: [3)]

I. Abschnitt: Zweck, Definitionen und Sicherheitsziele

§ 1 *Zweck und Geltungsbereich*

[1] Diese Verordnung regelt die Aufgaben, Kompetenzen und Verantwortlichkeiten zur Wahrung der Informatiksicherheit bei den Informatiksystemen, für welche der Kanton verantwortlich ist.

§ 2 *Definitionen*

[1] Informatiksicherheit umfasst den Schutz sämtlicher elektronisch verarbeiteter Informationen – unabhängig vom Informationsträger – bei Eingabe, Verarbeitung, Speicherung, Ausgabe und Transport sowie den Schutz aller technischen und organisatorischen Methoden und Hilfsmittel, welche dazu eingesetzt werden.

§ 3

[1] Informatiksysteme im Sinne dieser Verordnung bestehen aus folgenden Komponenten:

1. Daten: elektronisch gespeicherte Information im weitesten Sinn (z.B. Daten aus der Buchhaltung, Adressen, Textdokumente, Bilder, Grafiken, e-Mails).
2. Datenbestände: bestehen aus physisch oder sachlogisch zusammenhängenden Daten, welche für den wiederholten Gebrauch oder aus rechtlichen Gründen abgelegt bzw. gespeichert sind. Ein Datenbestand ist nicht an ein bestimmtes Speichermedium oder einen bestimmten Speicherort gebunden.
3. Anwendungen: dienen der Erfüllung bestimmter Aufgaben und bestehen aus manuellen und programmierten Abläufen und Verfahren.
4. Technologien: sind die Plattform für die Anwendungen (z.B. Hardware, Betriebssysteme, Software, Datenbank-Systeme, Netzwerke, Palm Computing, Telefonie über Internet).
5. Anlagen: dienen dem Betrieb und der Unterbringung von Informatiksystemen (z.B. Gebäude, Rechenzentren, Ausweich-Rechenzentren, Backup-Auslagerungsort, Backup-Transport).

§ 4 *Sicherheitsziele*

[1] Die folgenden Sicherheitsziele sind für die in § 3 genannten Komponenten von Informatiksystemen umzusetzen:

1. Verfügbarkeit: Die Daten, resp. die Datenbestände müssen am richtigen Ort zur richtigen Zeit zur Verfügung stehen. Zusätzlich muss die Betriebsbereitschaft und die Funktionalität bzw. Kontinuität der Anwendungen, Technologien und Anlagen sichergestellt werden.

1) SG 153.260.
2) SG 153.100.
3) Ingress in der Fassung von § 31 Ziff. 2 der Informations- und Datenschutzverordnung (IDV) vom 9. 8. 2011 (wirksam seit 1. 1. 2012).

2. Vertraulichkeit: Komponenten von Informatiksystemen dürfen nur einem definierten Personenkreis bekannt werden. Es ist insbesondere darauf zu achten, dass Informationen oder Anwendungen nicht von Personen zur Kenntnis genommen werden, die dazu nicht befugt sind.
3. Richtigkeit und Integrität: Alle erforderlichen Komponenten von Informatiksystemen sind vollständig, unverfälscht und korrekt zu erhalten.
4. Nachvollziehbarkeit: Die für die Daten zuständige Person kann festlegen, für welche Daten die Verarbeitungsschritte mittels einer Prüfspur nachvollziehbar und deren Urheber identifizierbar sein müssen. Verarbeitungsschritte können sowohl organisatorische wie EDV-technische Arbeiten umfassen.

II. Abschnitt: Aufgaben, Kompetenzen und Verantwortlichkeiten

§ 5 *Organisation in der Dienststelle, im Amt*

[1] Die Aufgaben, Kompetenzen und Verantwortlichkeiten für die Umsetzung der Sicherheitsziele werden wie folgt festgelegt:

1. Dienststellenleitung: Sie trägt die Verantwortung für die Informatiksicherheit im Amt oder in der Dienststelle und bezeichnet und überwacht die amtsinternen Aufgaben- und Verantwortungsträger.
2. Benutzerinnen und Benutzer: Sie setzen die zur Verfügung gestellten Hilfsmittel der Informatik nur im Rahmen ihrer Kompetenzen und für dienstliche Zwecke ein. Sie unternehmen geeignete Schritte, um erkannten Gefahren zu begegnen und Probleme einer Lösung zuzuführen.
3. Anwenderorganisation: Der erforderliche Schutzbedarf für die Anwendung ist festzuhalten und die Einhaltung der definierten Schutzmassnahmen ist regelmässig zu kontrollieren.
4. Projektentwicklung: Die Sicherheitsaspekte sind bereits in der Projektrealisierung zu planen und in die Lösung zu integrieren.

§ 6 *Betreiberinnen und Betreiber*

[1] Betreiberinnen und Betreiber von Informatik-Diensten und treuhänderische Verwalter von Informationen oder von Verfahren zu deren Verarbeitung sind verantwortlich für:

1. die Einhaltung der mit den für die Daten und Anwendungen zuständigen Personen vereinbarten Anforderungen bezüglich Informatiksicherheit;
2. die Meldung festgestellter Sicherheitsrisiken und ungewöhnlicher Ereignisse an die beauftragende und die betroffene Dienststelle.

§ 7 *Datenzugriff*

[1] Um unberechtigte Zugriffe zu verhindern, muss jeglicher Zugriff auf Daten kontrolliert werden. Die entsprechenden technischen und organisatorischen Massnahmen müssen geschäftlichen Bedürfnissen und rechtlichen Anforderungen genügen.

[2] Voraussetzung zum Ergreifen von Massnahmen für die Zugriffskontrolle ist die durchgeführte Beurteilung der Datenbestände von den für die Daten zuständigen Personen bezüglich Vertraulichkeit.

§ 8 *Datenaustausch zwischen Informatiksystemen*

[1] Beim Transport von Daten zwischen Informatiksystemen unterschiedlicher Verantwortungsbereiche muss die Empfangsstelle über ihre Verpflichtungen informiert werden. Die Pflicht bezüglich der Daten geht von der sendenden zur empfangenden Stelle über. Die Übergabe der Verantwortung muss schriftlich festgehalten werden.

§ 9

[1] Der Datentransport über Netze ausserhalb des kantonseigenen Datennetzes DANEBS ist nur über gesicherte, von der Betreiberin oder vom Betreiber des DANEBS bereitgestellte Netzübergänge zulässig.

III. Abschnitt: Umsetzung und Kontrolle

§ 10

[1] Die Umsetzung der Informatiksicherheit obliegt den in den Dienststellen und Ämtern verantwortlichen Personen und den Betreiberinnen und Betreibern.

§ 11

[1] Die Informatik-Konferenz erlässt die ausführenden Bestimmungen zur Umsetzung der verschiedenen Sicherheitsziele. [4)]

§ 12

[1] Die Departemente sorgen für die Einhaltung der Vorgaben der Informatiksicherheit. Die Finanzkontrolle und der Datenschutz können in die jährlich zu erstellenden Prüfberichte Einsicht nehmen.

IV. Abschnitt: Schlussbestimmungen

§ 13

[1] Die in Abschnitt 2 genannten Aufgaben sind für bestehende Informatiksysteme innert einem Jahr zu erfüllen. Für neue Projekte gelten die Bestimmungen sofort.

Diese Verordnung ist zu publizieren; sie wird sofort wirksam. [5)] Auf den gleichen Zeitpunkt wird das Datenschutzreglement für Informatik vom 22. Dezember 1987 aufgehoben.

4) § 11: Die Bestimmungen (Richtlinien über die Informatik in der Verwaltung des Kantons Basel-Stadt vom 12. 7. 2005, Weisungen der Informatik-Konferenz Basel-Stadt für die Benutzung von Informatikmitteln in der Verwaltung des Kantons Basel-Stadt vom 22. 10. 2003 und Weisung zur Nutzung von E-Mails und zur Handhabung elektronischer Kalender in der Verwaltung des Kantons Basel-Stadt vom 1. 11. 2007) können bei der Fachstelle für Informatik und Organisation eingesehen werden.

5) Wirksam seit 28. 4. 2002.