Verordnung über die Informatiksicherheit

vom 24. Februar 2004 (Stand 1. März 2004)

Die Regierung des Kantons St.Gallen

erlässt

in Ausführung von Art. 95 des Staatsverwaltungsgesetzes vom 16. Juni 1994[1]

als Verordnung:[2]

I. Allgemeine Bestimmungen (1.)

Art. 1 Geltungsbereich

[1] Diese Verordnung gilt für die Staatsverwaltung nach Art. 1 des Staatsverwaltungsgesetzes vom 16. Juni 1994[3], ausgenommen die selbständigen öffentlich-rechtlichen Anstalten.

[2] Sie wird auf Gerichte und andere Justizbehörden sachgemäss angewendet, soweit diese nicht richterlich handeln.

Art. 2 Grundsatz

[1] Informatiksysteme werden durch angemessene organisatorische und technische Massnahmen vor äusseren Einwirkungen und unbefugten Zugriffen geschützt.

Art. 3 Begriffe

[1] Folgende Begriffe bedeuten:

a) Informatiksysteme: Geräte und Einrichtungen sowie die dazugehörende Infrastruktur, Betriebssoftware und die Informatikanwendungen, die zur elektronischen Bearbeitung von Daten eingesetzt werden, einschliesslich der bearbeiteten Daten.

1 sGS 140.1.
2 Im Amtsblatt veröffentlicht am 8. März 2004, ABl 2004, 609; in Vollzug ab 1. März 2004.
3 sGS 140.1.

b) Informatikanwendungen: Programme, welche die Nutzung von Informatiksystemen für die Erfüllung oder die Unterstützung bestimmter Aufgaben ermöglichen.
c) Daten: Alle digitalen Informationen, die mit Informatiksystemen bearbeitet werden.
d) Ereignis: Verletzung der Informatiksicherheit, die zu einem finanziellen Schaden oder einem Imageverlust führt oder eine massive Verminderung der Verfügbarkeit von betroffenen Informatiksystemen zur Folge hat.
e) Normalbetrieb: Betrieb der Informatiksysteme im Normalfall.
f) Notbetrieb: Betrieb der betroffenen Informatiksysteme nach dem Eintritt eines Ereignisses.

Art. 4 Verantwortlichkeiten

[1] Die Konferenz der Departementsinformatikverantwortlichen legt die Sicherheitsmassnahmen, abgestuft nach den Risiken, in einem Massnahmenkatalog fest. Die Sicherheitsmassnahmen dienen der Reduktion der Risiken.

[2] Die Ämter beurteilen die Risiken, legen die Sicherheitsstufen fest, ermitteln die zu treffenden Sicherheitsmassnahmen und sorgen für deren Umsetzung.

[3] Departemente und Dienst für Informatikplanung kontrollieren die Einstufung der Informatiksysteme und -anwendungen.

Art. 5 Unterstützung

[1] Departementsinformatikverantwortliche und Dienst für Informatikplanung beraten die Ämter bei der Risikobeurteilung, bei der Festlegung der Sicherheitsstufen, bei der Ermittlung der Sicherheitsmassnahmen sowie bei deren Umsetzung und Überprüfung.

II. Sicherheitsstufen und Sicherheitsmassnahmen (2.)

Art. 6 Risikobeurteilung

[1] Die Ämter legen für ihre Informatiksysteme und -anwendungen je einzeln die Gefährdung fest, indem sie die damit verwalteten Daten klassifizieren.

[2] Sie berücksichtigen die Risiken aufgrund unvorsichtigen oder böswilligen Verhaltens von Mitarbeitenden und Aussenstehenden, aufgrund technischer Mängel an Geräten und Gebäuden sowie aufgrund von Feuer und Elementarereignissen.

Art. 7 *Klassifizierung*
a) Vertraulichkeit

[1] Als «geheim» gelten Daten, wenn es sich um besonders schützenswerte Personendaten, um Persönlichkeitsprofile, um Daten, deren Missbrauch eine betroffene Person in gesellschaftlicher und wirtschaftlicher Hinsicht erheblich benachteiligen, oder um vertraglich geschützte Daten handelt.

[2] Als «vertraulich» gelten Daten, wenn es sich um Personendaten, um Daten, deren Missbrauch eine betroffene Person in gesellschaftlicher und wirtschaftlicher Hinsicht benachteiligen, um Daten von finanzieller Relevanz oder um Daten handelt, für die eine Archivierungspflicht besteht.

[3] Alle anderen Daten werden bezüglich Vertraulichkeit als nicht klassifiziert eingestuft.

Art. 8 *b) Verfügbarkeit*

[1] Die Anforderung «hohe Verfügbarkeit» wird an die Daten gestellt, deren Nichtverfügbarkeit Leben gefährdet oder deren Bedeutung für die Aufgabenerfüllung so gross ist, dass die Verfügbarkeit auf einem entsprechenden Informatiksystem innert eines Tages wiederhergestellt werden muss. An Daten, deren Wiederbeschaffung nicht möglich ist und deren Verlust einen grossen finanziellen Schaden oder einen Imageschaden in der Öffentlichkeit verursacht, wird dieselbe Anforderung an die Verfügbarkeit gestellt.

[2] Die Anforderung «mittlere Verfügbarkeit» wird an die Daten gestellt, deren Bedeutung für die Aufgabenerfüllung so gross ist, dass die Verfügbarkeit innert drei Tagen auf einem entsprechenden Informatiksystem wiederhergestellt werden muss. An Daten, deren Wiederbeschaffung möglich ist, deren Verlust aber einen mittleren finanziellen Schaden oder einen Imageschaden in der Verwaltung verursacht, wird dieselbe Anforderung an die Verfügbarkeit gestellt.

[3] Alle anderen Daten werden bezüglich Verfügbarkeit als nicht klassifiziert eingestuft.

Art. 9 *Sicherheitsstufen*

[1] Bei der Einstufung «geheim» bzw. «hohe Verfügbarkeit» wird ein hoher Schutz für die Informatiksysteme und -anwendungen gewährleistet.

[2] Bei der Einstufung «vertraulich» bzw. «mittlere Verfügbarkeit» wird ein mittlerer Schutz für die Informatiksysteme und -anwendungen gewährleistet.

[3] Werden die Daten als nicht klassifiziert eingestuft, wird ein Grundschutz für die Informatiksysteme und -anwendungen gewährleistet.

Art. 10 Massnahmenkatalog

[1] Ein Massnahmenkatalog legt nach der Klassifizierung der Daten die Informatik-Sicherheitsmassnahmen für die Informatiksysteme und -anwendungen fest bezüglich:
a) Verhinderung einer unbefugten Kenntnisnahme von Daten (Vertraulichkeit);
b) Verhinderung einer unbefugten Veränderung von Daten oder Zugriffsrechten (Integrität und Authentizität);
c) höchstzulässiger Dauer eines Ausfalls (Verfügbarkeit).

[2] Die Konferenz der Departementsinformatikverantwortlichen ist für Erstellung und Nachführung des Massnahmenkatalogs zuständig.

III. Organisation (3.)

Art. 11 Informatik-Sicherheitsorganisation der Ämter

[1] Die Ämter bestimmen eine Informatik-Sicherheitsorganisation.

[2] Die nach der Informatik-Sicherheitsorganisation zuständige Person:
a) trifft die erforderlichen Vorsorgemassnahmen;
b) stellt nach dem Eintritt eines Ereignisses die Geschäftsfortführung mit Hilfe der Informatiksysteme und deren Rückführung in den Normalbetrieb sicher.

Art. 12 Amtsübergreifende Koordination

[1] Der Departementsinformatikverantwortliche sorgt für die amtsübergreifende Koordination innerhalb des Departementes bzw. der Staatskanzlei.

Art. 13 Kantonaler Informatik-Sicherheitsbeauftragter

[1] Der Dienst für Informatikplanung sorgt für die departementsübergreifende Koordination. Er bestimmt hiefür einen kantonalen Informatik-Sicherheitsbeauftragten.

[2] Der kantonale Informatik-Sicherheits-Beauftragte ist sowohl im Normalbetrieb als auch im Notbetrieb im Einsatz.

Art. 14 Teilstab Informatik

[1] Der kantonale Führungsstab bestimmt einen Teilstab Informatik.

[2] Der Teilstab Informatik wird bei Grossereignissen, Notlagen und Katastrophen eingesetzt, wenn die Informatiksicherheit gefährdet ist.

IV. Umsetzung (4.)

Art. 15 Bestehende Informatiksysteme

[1] Die Ämter stufen bestehende Informatiksysteme und -anwendungen gemäss der Klassifizierung der Daten ein und sorgen für die Umsetzung der erforderlichen Sicherheitsmassnahmen.

Art. 16 Einführung neuer Informatiksysteme

[1] Bei Neu- oder Ersatzbeschaffungen von Informatiksystemen und -anwendungen legen die Ämter die erforderlichen Informatik-Sicherheitsmassnahmen im Rahmen der Einführungsprojekte fest und setzen sie um.

Art. 17 Instruktion des Personals

[1] Die Ämter informieren die Mitarbeitenden über die Sicherheitsmassnahmen, die sie zu beachten haben.

[2] Sie sorgen für die Ausbildung.

V. Datenverarbeitung ausserhalb des Amtes (5.)

Art. 18 Zusammenarbeit mehrerer Ämter

[1] Wenn ein Amt Daten durch andere Ämter bearbeiten lässt oder sie mit diesen austauscht, werden die Sicherheitsstufen und -massnahmen sowie die Verantwortlichkeiten bei der Umsetzung gemeinsam festgelegt.

Art. 19 Zusammenarbeit mit Dritten

[1] Wenn ein Amt Daten durch Stellen, welche dieser Verordnung nicht unterstehen, bearbeiten lässt, wird im Zusammenarbeitsvertrag vereinbart, welche Massnahmen der Beauftragte zu treffen hat und wie ihre Einhaltung kontrolliert wird.

Art. 20 Datenaustausch über öffentliche Netze

[1] Der Datenaustausch über öffentliche Netze ist nur über gesicherte Zugangspunkte zulässig. Als öffentlich gelten alle Netze ausserhalb des Kommunikationsnetzes KOMSG des Kantons.

[2] Der Zugriff von öffentlichen Netzen auf das kantonsinterne Netz erfolgt über die vom Netzbetreiber bereitgestellten gesicherten Netzübergänge.

[3] Der Netzbetreiber kann Ausnahmen bewilligen.

Art. 21 Verwaltungsexterne Informatikarbeitsplätze

[1] Unter welchen Voraussetzungen die Bearbeitung von Daten ausserhalb der Räumlichkeiten des Amtes und die Verwendung von Daten auf privaten Geräten zulässig ist, wird in einer Dienstanweisung geregelt.

VI. Überprüfung der Informatik-Sicherheitsmassnahmen (6.)

Art. 22 Amtsinterne Überprüfung

[1] Die Ämter überprüfen periodisch Einhaltung und Angemessenheit der Informatik-Sicherheitsmassnahmen.

[2] Ändern Aufgaben, Organisation oder eingesetzte Informatiksysteme oder -anwendungen eines Amtes, überprüfen sie die Sicherheitsstufen und Schutzziele sowie die Angemessenheit der Informatik-Sicherheitsmassnahmen.

Art. 23 Kontrolle und Test

[1] Bei Informatiksystemen und -anwendungen mit der Einstufung «hohe Verfügbarkeit» bzw. «geheim» lassen die Ämter die Informatik-Sicherheitsmassnahmen periodisch durch unabhängige interne oder externe Stellen überprüfen.

[2] Der kantonale Informatik-Sicherheitsbeauftragte kann Prüfungen stichprobenweise veranlassen.

[3] Bei Informatiksystemen und -anwendungen mit der Einstufung «hohe Verfügbarkeit» wird ein Notfallkonzept erstellt und periodisch getestet.

Schlussbestimmungen (VII.)

Art. 24 Aufhebung bisherigen Rechts

[1] Die Verordnung über die Abteilung für Datenverarbeitung und Organisation vom 22. April 1975[4] wird aufgehoben.

Art. 25 Übergangsbestimmung

[1] Für die bestehenden Informatiksysteme und -anwendungen beurteilen die Ämter innerhalb von zwei Jahren nach Vollzugsbeginn dieser Verordnung die Risiken und legen die Sicherheitsstufen, die Informatik-Sicherheitsmassnahmen sowie den Zeitplan ihrer Umsetzung fest.

4 nGS 10–45 (sGS 141.7).

Art. 26 Vollzugsbeginn

[1] Dieser Erlass wird ab 1. März 2004 angewendet.

* Änderungstabelle - Nach Bestimmung

Bestimmung	Änderungstyp	nGS-Fundstelle	Erlassdatum	Vollzugsbeginn
Erlass	Grunderlass	39-29	24.02.2004	01.03.2004

* Änderungstabelle - Nach Erlassdatum

Erlassdatum	Vollzugsbeginn	Bestimmung	Änderungstyp	nGS-Fundstelle
24.02.2004	01.03.2004	Erlass	Grunderlass	39-29