IIIIII KANTON solothurn

Regierungsratsbeschluss

vom 1. Juli 2003

Nr. 2003/1296

Weisung über die Benutzung der Informatiksysteme und -anwendungen in der kantonalen Verwaltung

---

1. Ausgangslage

Im Oktober 1990 erliess der Regierungsrat die Weisung über den Einsatz von Personal Computern und Terminals in der kantonalen Verwaltung (BGS 122.213.2) sowie Benutzer-Richtlinien für Personal Computer und Terminals (BGS 122.213.21). In den vergangenen mehr als zehn Jahren seit Inkrafttreten der erwähnten Erlasse hat sich der Informatikbereich stark gewandelt. Insbesondere die neuen netzbasierten Anwendungen ermöglichen heute die Kommunikation mittels E-Mail sowie den Zugriff auf das Internet. Derzeit bestehen rund 1500 Arbeitsplätze, welche über Internet-/Intranet-Anschlüsse verfügen. Bis ins Jahr 2004 sollen diese auf 2200 erhöht werden. Diese neuen Technologien haben sich grundsätzlich als sehr wertvolle Arbeitsinstrumente erwiesen, welche sich sowohl auf die Produktivität wie auch auf die Qualität der zu erbringenden Dienstleistungen positiv auswirkten. Sie können aber bei unsachgemässer oder missbräuchlicher Nutzung auch Schaden anrichten. So können unerlaubte Manipulationen bestehende Informatiksysteme lahm legen, Datenverluste verursachen oder den Datenverkehr beeinträchtigen. Auch die private Nutzung des Internets oder des E-Mails während der Arbeitszeit richtet finanziellen Schaden an. Softwarepiraterie oder Zugriffe auf illegale Internetseiten können zudem auch rechtliche Konsequenzen haben. Die Weisung für die Benutzung der Informatiksysteme und -anwendungen regelt deshalb den Umgang und die Nutzung mit den zur Verfügung stehenden Informatikmitteln und den neuen Technologien. Sie stellt eine Präventivmassnahme dar, um Missbräuche möglichst einzuschränken und die Sicherheit der Systeme und Anwendungen zu erhöhen.

Die Nutzungsvorschriften werden Bestandteil des Gesamtarbeitsvertrages sein, weshalb der vorliegenden Weisung voraussichtlich nur Übergangscharakter zukommt.

2. Zu den einzelnen Bestimmungen

§ 1 Geltungsbereich

Der Geltungsbereich der Weisung ist breit definiert, um möglichst alle Anwender zu erfassen. Nebst den Mitarbeitenden der Zentralverwaltung und der Gerichte gilt die Weisung auch für das Personal der Anstalten und der Spitäler.

§ 2 Zweck

Die Weisung legt einerseits fest, wie die Informatikmittel genutzt werden dürfen (Nutzungsvorschriften). Andererseits regelt sie auch die Voraussetzungen für die Kontrolle der Einhaltung der Vorschriften (Überwachungsvorschriften). Diese Präventiv- und Kontrollmassnahmen sollen die einwand-

freie Nutzung der Informatiksysteme und die Sicherheit der Daten und Anwendungen sicherstellen sowie technische Störungen verhindern. Sie bezweckt zudem auch, unerlaubtes Surfen im Internet oder den unzulässigen Umgang mit E-Mails zu verhindern.

§ 3 Informatiksysteme und -anwendungen

Die Bestimmung verdeutlicht, dass die Begriffe „Informatiksysteme und -anwendungen" sämtliche zur Verfügung stehende Informatikinfrastruktur einschliesslich der Programme zur Datenbearbeitung oder auch netzbasierte Anwendungen wie Internet oder E-Mail umfassen.

§ 4 Informatikdienstleister

Mit dem Begriff „Informatikdienstleister" werden alle Fachstellen erfasst, welche Informatikdienstleistungen für kantonale Dienststellen erbringen. In der Zentralverwaltung ist in der Regel das Amt für Informatik und Organisation zuständige Fachstelle. Bei den Anstalten sind jedoch auch Dritte mit diesen Aufgaben beauftragt und für die Spitäler ist die Informatikabteilung Spitäler (IAS) zuständig. Weil im Spitalbereich die Vorschriften über den Datenschutz und die Datensicherheit, die Sicherheitsvorkehrungen wie auch die Nutzung der Maildienste sowie des Internets weitergehenden Präzisierungen bedürfen, ist die IAS befugt, ergänzende Vorschriften in ihrem Zuständigkeitsgebiet zu erlassen.

§ 5 Verantwortung der Anwender

Die Bestimmung legt den Grundsatz der Eigenverantwortung fest. Jeder Informatikanwender ist nicht nur für den recht- und zweckmässigen sowie wirtschaftlichen Einsatz der an seinem Arbeitsplatz vorhandenen Informatikmittel verantwortlich, sondern auch für einen genügenden Wissensstand, um diese Mittel optimal zu nützen. Es ist Aufgabe des Arbeitgebers, die erforderliche Ausbildungs- und Weiterbildungsangebote bereit zu stellen. Recht und Pflicht der Arbeitnehmer ist es hingegen, von diesen Angeboten Gebrauch zu machen, um ihre Kenntnisse der EDV-Anwendungen à-jour zu halten oder vertiefen zu können. In der Verantwortung der Anwender liegt im weitern, dass die von ihnen bearbeiteten Daten vor Verlust, Manipulation oder unzulässiger Einsichtnahme durch Dritte geschützt sind.

§ 6 Nutzung zu dienstlichen Zwecken

Die Informatikmittel sind grundsätzlich für die Erledigung dienstlicher Aufgaben zu benützen. Ausserhalb der Arbeitszeit sollen die Systeme und Anwendungen aber auch zu privaten Zwecken benützt werden dürfen. Auch die gelegentliche private Nutzung der Informatikmittel während der Arbeitszeit soll erlaubt sein, wenn dies in zeitlich geringem Umfang erfolgt und dadurch die Arbeitsproduktivität nicht eingeschränkt wird. Ein striktes Verbot der privaten Nutzung wäre unrealistisch, da ansonsten beispielsweise bereits die Eingabe eines privaten Termins auf der Arbeitsstation als Dienstpflichtverletzung betrachtet werden müsste.

Die Nutzungsvorschrift gilt auch für die Benützung des E-Mails und des Internets. Auch diese Dienste dürfen mit der gebotenen Zurückhaltung bzw. in zeitlich engen Grenzen für private Zwecke verwendet werden. Diese Regelung erlaubt den gelegentlichen Versand eines privaten E-Mails oder den Abruf einiger weniger Informationen aus dem Internet, lässt hingegen keine Surftouren zu. Diese Regelung vertraut darauf, dass die Mitarbeitenden mit den ihnen zur Verfügung gestellten Arbeitsinstrumenten grundsätzlich vernünftig umgehen. Ein striktes Verbot wäre im Vergleich zur Nutzung anderer Informations- oder Kommunikationsmittel (Presseerzeugnisse, Telefonie, etc.) unverhältnismässig. Die Nutzungsvorschriften gelten selbstverständlich auch bei der Nutzung des Internets zu privaten Zwecken.

§ 7 Datenschutz und Datensicherheit

Die Vorschriften des Datenschutzes und der Datensicherheit müssen durch die Anwender beachtet werden. Während der Datenschutz den Schutz der Persönlichkeit bezweckt, bezieht sich die Datensicherheit auf den Schutz der Information, d.h. auf die Gewährleistung ihrer Vertraulichkeit, Verfügbarkeit und Unversehrbarkeit. Datensicherheit umfasst alle technischen und organisatorischen Massnahmen, die vom Inhaber der Datensammlung getroffen werden müssen, um den Anforderungen des Datenschutzgesetzes zu genügen.

Damit Daten vor unbefugten Zugriffen geschützt sind, sind die nötigen Sicherheitsvorkehrungen zu treffen. Personal Computer dürfen nur in überwachten oder abschliessbaren Räumen installiert werden. Tragbare Computer (Laptops) sind in analoger Weise zu schützen. Werden Daten gespeichert, sind diese vor unberechtigten Zugriffen – in der Regel durch Benutzung eines Passwortes - zu schützen. Nicht erforderlich ist hingegen, dass Dateien immer mit Passwort schreib- und lesegeschützt werden müssen, weil die Mitarbeitenden von ihren jeweiligen Arbeitsplätzen häufig Zugriff auf fremde Dateien haben. Meist werden die Dateiablagen so eingerichtet und benutzt, dass die Mitarbeitenden einer Organisationseinheit gemeinsamen Zugriff darauf haben. Werden die Daten auf diese Weise einem grösseren Benutzerkreis zugänglich gemacht, handelt es sich nicht um einen unbefugten Zugriff. Die Vorschriften zum Datenschutz und zur Datensicherheit stellen hingegen Vorkehrungen gegen **Unbefugte** dar.

Aus Sicherheitsgründen ist ebenfalls vorzusehen, dass Daten auf dem Netzwerklaufwerk gespeichert werden. Disketten, CD oder DVD sind nicht geschützte Datenträger, weshalb sie möglichst nicht zum Einsatz gelangen sollten. Ist deren Einsatz unumgänglich, muss eine sichere Aufbewahrung sichergestellt sein.

§ 8 Sicherheitsvorkehrungen

Die Anwender haben bei der Nutzung der Informatikmittel die nötigen Sicherheitsvorkehrungen zu treffen. Solche Sicherheitsvorkehrungen, welche als bekannt vorausgesetzt werden dürfen, sind beispielsweise die Überprüfung der zugestellten Dateien oder Anhänge auf Viren durch Speicherung auf Netzwerklaufwerken. Eine Mitverantwortung tragen ebenfalls die Informatikdienstleister, welche die erforderlichen Sicherheitsprogramme zur Verfügung stellen.

Der Zugang zu den Informatiksystemen muss durch geeignete Massnahmen gesichert sein. In der Regel erfolgt dies durch die Benutzung von Benutzerlogins und von Passwörtern. Diese dürfen nicht an leicht zugänglichen Stellen aufgeschrieben werden. Wird der Arbeitsplatz für längere Zeit verlassen, ist die Arbeitsstation zu sperren oder das Büro zu schliessen.

§ 9 Technische Schutzmassnahmen durch den Arbeitgeber

Der Arbeitgeber ist wie der Anwender verpflichtet, die nötigen technischen Sicherheitsvorkehrungen zu treffen, um Risiken insbesondere im Zusammenhang mit der Internet- und E-Mail-Nutzung zu reduzieren. Er trägt eine wesentliche Mitverantwortung für die Sicherheit von Daten und Anwendungen. Das heisst im besonderen, dass er für einen technischen Schutz sorgen muss, damit beispielsweise keine Viren eingeschleppt oder keine Speicherüberlastungen verursacht werden. Konkrete Massnahmen dafür sind zum Beispiel der Einsatz von Firewalls, Antivirusprogrammen oder die Beschränkung der Speicherkapazität.

Firewalls dienen zum einen dem Schutz eigener Daten vor externen Zugriffen und filtern zum andern den Datenverkehr im Zusammenhang mit der Nutzung des Internets. Die Firewall kann mit soge-

nannten Sperrlisten erweitert werden, welche den Zugriff auf bestimmte Internetseiten verunmöglicht. In begründeten Fällen kann es aus dienstlichen Gründen unerlässlich sein, Zugang zu gesperrten Seiten zu ermöglichen. Absatz 2 sieht für diese Fälle eine Ausnahmeregelung vor.

§ 10 Nutzung der Informatiksysteme und –anwendungen im allgemeinen

Die Bestimmung regelt allgemein, in welchem Rahmen die Informatiksysteme und –anwendungen genutzt werden dürfen und welche Vorgänge im besonderen untersagt sind. Für die Nutzung des E-Mails sowie des Internets finden sich zusätzliche Vorschriften in den nachfolgenden Bestimmungen (§§ 11 und 12).

Absatz 1 fordert, dass die Systeme und Anwendungen ausschliesslich so zu nutzen sind, dass nicht gegen geltendes Recht verstossen wird. Die Computertechnik ermöglicht eine Vielzahl von Verstössen gegen bestehendes Recht. Im Vordergrund stehen strafrechtliche Tatbestände, aber auch Verstösse gegen wettbewerbs- oder urheberrechtliche Vorschriften oder Datenschutzbestimmungen. In Absatz 2 werden die im speziellen untersagten Nutzungsmöglichkeiten aufgeführt. Dazu gehören auch solche Vorgänge, welche unter Umständen nicht gesetzeswidrig, aber aus sicherheitstechnischen Gründen verboten sind.

§ 11 Nutzung der Maildienste

Für den Versand und Empfang von E-Mails ist der Anwender selber verantwortlich. Er hat dafür besorgt zu sein, dass beispielsweise keine vertraulichen Informationen per E-Mail an Unberechtigte versandt werden. Besonders schützenswerte Personendaten oder besonders vertrauliche Informationen sollen nicht an externe Mailadressaten versandt werden, sofern sie nicht durch besondere Massnahmen geschützt werden können. Unzulässig ist die Verwendung einer fremden Arbeitsstation zum Versand von E-Mails, sofern die berechtigte Person dafür nicht ihr Einverständnis erteilt hat. Missbräuche sollen dadurch unterbunden werden.

Absatz 3 führt die technischen Sicherheitsvorkehrungen auf, welche bei der Nutzung von E-Mails zu beachten sind. Anhänge zu Mails, welche von Adressaten ausserhalb des kantonalen Netzes zugestellt werden, müssen auf Virenbefall geprüft werden. Untersagt ist auch das Öffnen oder Speichern von unbekannten Dateitypen oder solchen mit speziellen Endungen (wie EXE, COM,BAS, VBS, AVI, MP2, MPEG, etc.).

Web-basierende-E-Maildienste ermöglichen es, private Mailboxen abzurufen. Diese Möglichkeit birgt allerdings die Gefahr, dass der Virenschutz umgangen werden kann. Der Zugang zu solchen Briefkästen soll deshalb aus Sicherheitsgründen nur mit Bewilligung des Amtes für Informatik und Organisation erlaubt sein, welche in der Lage ist zu prüfen, ob solche Diensteanbieter die nötigen Sicherheitsvorkehrungen garantieren können.

§ 12 Internet-Nutzung

Anschlüsse an das Internet oder Intranet sollen grundsätzlich gewährt werden. In der Regel wird ein sogenannter reduzierter Internet-Zugang ermöglicht, bei welchem der Datenverkehr gefiltert wird. Der Zugang zu Seiten, welche auf einer Sperrliste sind, ist damit nicht möglich. Dienstliche Gründe können es erforderlich machen, dass ein uneingeschränkter Zugang ermöglicht wird. Entsprechende Bewilligungen erteilt der oder die Vorgesetzte einer Dienststelle.

Auf kostenpflichtige Seiten soll nur zugegriffen werden, wenn dies aus dienstlichen Gründen erforderlich ist. Zulässig ist damit das Abrufen von Fachzeitschriften oder fachspezifischer Maildienste, welche

kostenpflichtige Seiten zur Verfügung stellen. Auf Seiten mit gesetzes- oder sittenwidrigen Inhalten (Seiten mit pornographischem oder rassistischem Inhalt etc.) darf hingegen nur in speziellen Ausnahmefällen (z.B. polizeiliche Ermittlungen) und wenn eine ausdrückliche Bewilligung des oder der Vorgesetzen vorliegt, zugegriffen werden.

Viele Internet-Seiten enthalten Multimedia-Effekte, welche nur funktionieren, wenn spezielle Programmteile installiert werden. Gleichzeitig werden solche Programmteile unentgeltlich zur Installation angeboten. Solche Programme wie auch anderweitig erworbene Software dürfen jedoch ohne Bewilligung der Informatikdienstleister auf den zentralen Rechnern aus Geschwindigkeits- und Sicherheitsgründen nicht installiert werden. Spielprogramme oder ähnliches darf ebenfalls nicht benutzt werden, da sie enorme Speicherkapazitäten beanspruchen können und damit die Systeme beeinträchtigen. Untersagt ist ebenso die sogenannte Softwarepiraterie, indem von lizenzpflichtiger Software Kopien angefertigt werden.

Absatz 5 soll verhindern, dass Anwender ihren Internetzugang beispielsweise nicht als privaten Internetshop betreiben oder private Börsengeschäfte via Internet abwickeln.

§ 13 Kontrolle der Einhaltung der Nutzungsvorschriften

Die Bestimmung legt fest, mit welchen Kontrollen die Anwender rechnen müssen. Technisch lassen sich Kontrollen wie folgt durchführen: Bei der Nutzung netzbasierter Anwendungen hinterlässt der Anwender Spuren in Form von Randdaten. Diese Spuren geben Auskunft darüber, wer zu welcher Zeit welche Zugriffe (abgerufene URL) oder Manipulationen (Ein- Ausloggen, Applikationsabruf etc.) getätigt hat. Diese Spuren werden als Protokollierungen aufgezeichnet. Surfprogramme erstellen auch temporäre Dateien der Inhalte (Cache) und permanente Spuren-Dateien (Cookies) über besuchte Internet-Seiten. Diese Aufzeichnungen ermöglichen die Überwachung der Einhaltung der Vorschriften.

Aus Gründen des Persönlichkeitsschutzes ist eine stetige, personenbezogene Überwachung als Präventivmassnahme jedoch nicht zulässig. Gestattet sind stichprobenartige, anonyme Kontrollen der Protokollierungen, um zu überprüfen, ob die Nutzungsregelungen eingehalten wurden. Erst wenn aufgrund der anonymen Kontrolle ein konkreter Missbrauch aufgedeckt wird, dürfen personenbezogene Auswertungen unter folgenden Bedingungen vorgenommen werden: Hat der Missbrauch eine technische Störung zur Folge, darf eine personenbezogene Auswertung sofort vorgenommen werden und die Resultate sind an die vorgesetzte Stelle zur Prüfung von Sanktionen weiterzuleiten. Wird eine missbräuchliche Nutzung durch die dafür zuständige Stelle (Informatikdienstleister) festgestellt, ohne dass es zu technischen Störungen kommt, sind die gemachten Feststellungen dem oder der Vorgesetzen einer Dienststelle zu melden. Er oder sie orientiert in der Folge die Mitarbeitenden über die festgestellten Missbräuche und kündigt ihnen gleichzeitig an, dass eine personenbezogene Überwachung vorgenommen wird, falls weitere Missbräuche festgestellt würden. Unter denselben Voraussetzungen (vorgängige Orientierung der Mitarbeitenden) kann auch der oder die Vorgesetzte einer Dienststelle eine personenbezogene Auswertung verlangen, wenn ein konkreter Verdacht auf missbräuchliche Nutzung vorliegt. Muss eine Warnung wegen festgestellter Missbräuche ausgesprochen werden, können während einer gewissen Zeitspanne (z.B. während 6 Monaten) anonymisierte Kontrollen durchgeführt und im Falle eines weiteren Missbrauchs sofort personenbezogen ausgewertet werden.

Wenn im Rahmen einer anonymen Kontrolle der konkrete Verdacht geschöpft wird, dass eine Straftat begangen wurde, so können die entsprechenden Beweise (Protokollierungen, Backups) gesichert

werden. Der Informatikdienstleister meldet die Feststellungen dem oder der Vorgesetzten einer Dienststelle. Wenn der Missbrauch zugleich eine technische Störung hervorgerufen hat, ist die fehlbare Person sofort zu identifizieren und gegen sie Anzeige zu erstatten. Ansonsten ist Anzeige gegen Unbekannt zu erstatten und die Auswertungen werden von der Strafjustizbehörde vorgenommen.

Werden durch die Nutzung von Informatikmitteln Dienstpflichten verletzt, ist ebenfalls eine sofortige Identifikation zulässig. Besteht beispielsweise der Verdacht, dass Mitarbeitende durch E-Mails belästigt werden, kann die Identität der fehlbaren Person sofort festgestellt werden. Solche Missbräuche beeinträchtigen unter Umständen die Leistungsbereitschaft der Mitarbeitenden und wirken sich negativ auf das Arbeitsklima aus, was eine sofortige personenbezogene Auswertung von Aufzeichnungen rechtfertigt.

Die Informatikdienstleister haben im übrigen beispielsweise mit einer internen Weisung sicher zu stellen, dass nur ein sehr beschränkter Kreis von Mitarbeitenden Einsicht in die Protokollierungen hat. Diese Massnahme stellt eine zusätzliche Gewähr dar, dass die Auswertung der Protokollierungen weisungsgemäss erfolgt und die Persönlichkeitsrechte der Mitarbeitenden respektiert werden.

Die Informatikdienstleister sollen Rechenschaft über ihre Kontrolltätigkeit ablegen. Vorgesehen wird, dass dies gegenüber dem oder der Beauftragten für Information und Datenschutz erfolgen soll. Er oder sie ist aufgrund der nach dem Informations- und Datenschutzgesetz übertragenen Aufgaben (InfoDG; BGS 114.1) die am besten geeignete Stelle, die Kontrolltätigkeit zu prüfen.

§ 14 Massnahmen bei Missbrauch

Die missbräuchliche Nutzung der Informatiksysteme und –anwendungen stellt eine Dienstpflichtverletzung dar, die sanktioniert werden kann. Bei Verdacht auf strafrechtliche Handlungen kann Strafanzeige erstattet werden. Die Zugriffsberechtigung auf die Systeme kann entzogen werden.

§ 15 Informationspflicht

Hohen Stellenwert kommt der Information der Mitarbeitenden über die Nutzungs- und Überwachungsvorschriften gemäss der vorliegenden Weisung zu. Die Anwender müssen über ihre Rechte und Pflichten bei der Nutzung der Informatiksysteme und –anwendungen im Bild sein, damit sie ihr Verhalten danach richten können. Die Abgabe der Weisung an jeden Mitarbeitenden schafft Transparenz und Rechtssicherheit zwischen Arbeitnehmer und Arbeitgeber. Dem oder der Vorgesetzten einer Dienststelle obliegt diese Informationspflicht.

§§ 16 und 17

Keine Bemerkungen.

Weisung über die Benutzung der Informatiksysteme und -an-wendungen in der kantonalen Verwaltung

RRB Nr. 2003/1296

Der Regierungsrat des Kantons Solothurn
gestützt auf § 54 Gesetz über das Staatspersonal vom 27. September 1992[1])

beschliesst:

§ 1. Geltungsbereich

Die Weisung gilt für das Personal der kantonalen Verwaltung, der Gerichte, der kantonalen Schulen, der kantonalen Anstalten sowie für das Personal der im Kanton gelegenen und von ihm massgeblich subventionierten Spitäler (im folgenden Anwender genannt).

§ 2. Zweck

[1] Diese Weisung regelt die Nutzung der Informatiksysteme und -anwendungen durch die Anwender am Arbeitsplatz.
[2] Sie bezweckt, die sachgerechte Nutzung der Informatiksysteme und –anwendungen sicherzustellen sowie Missbräuche zu verhindern und regelt die Voraussetzungen für die Überwachung der Nutzungsvorschriften.

§ 3. Informatiksysteme und -anwendungen

[1] Informatiksysteme umfassen sämtliche Geräte und Einrichtungen sowie die dazugehörende Infrastruktur und Software, die zur elektronischen Bearbeitung von Daten eingesetzt werden.
[2] Informatikanwendungen umfassen Programme, welche die Nutzung von Informatiksystemen für die Erfüllung oder Unterstützung bestimmter Aufgaben ermöglichen einschliesslich netzbasierter Anwendungen wie Internet und elektronische Maildienste (E-Mail oder elektronische Post).

§ 4. Informatikdienstleister

[1] Informatikdienstleister sind jene Fachstellen, welche für die kantonale Verwaltung, die Gerichte, die kantonalen Schulen, die kantonalen Anstalten sowie für die Spitäler Informatiksysteme betreuen.
[2] Die Informatikabteilung der Spitäler (IAS) ist befugt, in ihrem Zuständigkeitsbereich Ergänzungen zur vorliegenden Weisung zu erlassen.

§ 5. Verantwortung der Anwender

Der Anwender ist verantwortlich für

a) den recht- und zweckmässigen sowie wirtschaftlichen Einsatz und die sorgfältige Behandlung der zur Verfügung gestellten Informatiksysteme und -anwendungen;
b) die Nutzung der Schulungs- und Weiterbildungsangebote im Informatik-Bereich;
c) die von ihm bearbeiteten Daten;
d) die Einhaltung der Nutzungsvorschriften nach dieser Weisung.

[1]) BGS 126.1

§ 6. Nutzung zu dienstlichen und privaten Zwecken

[1] Die zur Verfügung gestellten Informatiksysteme und -anwendungen einschliesslich der Maildienste und des Internets sind zur Erfüllung von dienstlichen Aufgaben zu benutzen.

[2] Die Nutzung zu privaten Zwecken ist zulässig,

a) während der Arbeitszeit, sofern dies gelegentlich und in zeitlich geringem Umfang erfolgt und betriebliche Interessen nicht beeinträchtigt werden oder

b) ausserhalb der Arbeitszeit.

§ 7. Datenschutz und Datensicherheit

[1] Jeder Anwender hat die Vorschriften des Informations- und Datenschutzgesetzes[1]) zu beachten sowie die erforderlichen Vorkehren gegen Diebstahl und Missbrauch von Daten sowie Hard- und Software zu treffen.

[2] Daten dürfen nur dann gespeichert werden, wenn sie durch spezielle Massnahmen wie Abschliessen der Arbeitsstation, Passwortbenutzung oder ähnliches vor unberechtigten Zugriffen geschützt werden.

[3] Daten sind auf den Netzwerklaufwerken abzulegen. Die Verwendung von Disketten oder ähnlichen Datenträgern ist möglichst zu vermeiden. Solche Datenträger sind unter Verschluss aufzubewahren.

§ 8. Sicherheitsvorkehrungen

[1] Die Anwender haben die nötigen Sicherheitsvorkehrungen zu treffen, um die Informatiksysteme und -anwendungen vor äusseren Einwirkungen wie Virenbefall oder Speicherüberlastungen zu schützen.

[2] Die Arbeitsstation ist durch die Benutzung eines Passwortes vor unberechtigten Zugriffen zu schützen. Wird der Arbeitsplatz für längere Zeit verlassen, ist die Arbeitsstation zu sperren oder das Büro zu schliessen.

§ 9. Technische Schutzmassnahmen durch den Arbeitgeber

[1] Die Informatiksysteme werden durch geeignete technische Vorkehrungen wie Firewalls oder Antivirusprogramme geschützt, um die Sicherheit von Daten und Anwendungen zu garantieren oder den Betrieb vor Systemüberlastungen zu schützen.

[2] Die Sicherheitsvorkehrungen können auf Antrag der zuständigen Dienststelle aufgehoben werden, sofern dies aus dienstlichen Gründen erforderlich ist.

§ 10. Nutzung der Informatiksysteme und -anwendungen im allgemeinen

[1] Die Informatiksysteme und -anwendungen sind ausschliesslich im Rahmen der geltenden Gesetze und Vorschriften zu benützen.

[2] Den Anwendern ist es insbesondere untersagt,

a) die Informatikinfrastruktur zur Begehung oder zur Unterstützung strafbarer Handlungen zu nutzen;

b) auf die System- und Netzwerksicherheit zuzugreifen oder zu versuchen, die Sicherheitsvorkehrungen zu durchbrechen;

c) ohne Zustimmung des zuständigen Informatikdienstleisters Programme auf den Personal Computern oder auf den zentralen Rechnern zu installieren oder an bestehenden Programmen Änderungen vorzunehmen;

d) Spielprogamme oder ähnliche Angebote zu benutzen;

e) Kopien von lizenzpflichtiger Software anzufertigen oder weiter zu geben;

[1]) BGS 114.1.

f) Unberechtigten Dritten Daten zugänglich zu machen.

§ 11. Nutzung der Maildienste (elektronische Post)

[1] Die Anwender von Maildiensten sind für den Inhalt ihrer Mitteilungen verantwortlich, welche von ihrem Anschluss übermittelt werden.

[2] Besonders schützenswerte Personendaten oder besonders vertrauliche Informationen dürfen nicht an Mailadressaten ausserhalb des kantonalen Netzwerkes versendet werden, sofern keine Verschlüsselung oder Authentifizierung erfolgt.

[3] Die Verwendung eines fremden Mailservers als Verteilstation für die Verbreitung von elektronischen Mitteilungen ist ohne vorgängige Genehmigung durch die berechtigte Person nicht zulässig.

[4] Mailanhänge, welche von Absendern ausserhalb der Verwaltung zugestellt werden, sind vor deren Öffnung durch Speicherung auf die Netzwerklaufwerke auf Viren zu überprüfen.

[5] Zugriffe auf private Internet Mailboxen sind nur mit Bewilligung des Amtes für Informatik und Organisation zulässig.

§ 12 Internet-Nutzung

[1] Die Bewilligung zur Nutzung des Internets umfasst in der Regel den reduzierten Internet-Zugang.

[2] Der oder die Vorgesetzte einer Dienststelle kann einen uneingeschränkten Internet-Zugang bewilligen, wenn dienstliche Gründe es erfordern.

[3] Untersagt sind Zugriffe

a) auf kostenpflichtige Internetseiten, sofern nicht dienstliche Gründe dies erfordern oder

b) solche mit gesetzes- oder sittenwidrigen Inhalten. Ausnahmen bewilligt der oder die Vorgesetzte einer Dienststelle, wenn dienstliche Gründe dies erfordern.

[4] Im Internet abrufbare Programme oder Programmteile dürfen auf den Informatiksystemen ohne Einwilligung der Informatikdienstleister nicht installiert oder gespeichert werden.

[5] Die kommerzielle Nutzung von Internetdiensten zu privaten Zwecken ist untersagt.

§ 13. Kontrolle der Einhaltung der Nutzungsvorschriften

[1] Die Informatikdienstleister überwachen die Einhaltung der Nutzungsvorschriften stichprobenweise und anonym durch Auswertung der Protokollierungen.

[2] Liegt ein Missbrauch vor, welcher zu einer technischen Störung des Informatiksystems führt oder bei welchem ein begründeter Verdacht auf Begehung einer Straftat oder Verletzung von Dienstpflichten besteht, werten die Informatikdienstleister die Protokollierungen personenbezogen aus und leiten die Auswertung an den oder die Vorgesetzte der betreffenden Dienststelle weiter.

[3] Bei übrigen Verstössen gegen die Nutzungsvorschriften darf eine personenbezogene Auswertung der Protokollierungen erst vorgenommen werden, nachdem die Anwender der betreffenden Dienststelle über den festgestellten Missbrauch informiert und ihnen die personenbezogene Auswertung bei Wiederholung des Missbrauchs angekündigt wurde.

[4] Bei dringendem Verdacht auf missbräuchliche Nutzung der Informatiksysteme und –anwendungen kann der oder die Vorgesetzte einer Dienststelle eine personenbezogene Auswertung der Protokollierungen verlangen, sofern der oder die Anwender über den Missbrauchsverdacht informiert und die personenbezogene Auswertung angekündigt wurde.

[5] Die Informatikdienstleister bestimmen die mit der Überwachung beauftragten Personen und stellen sicher, dass Unbefugten keine Einsicht in die Protokollierungen gewährt wird. Sie erstatten dem oder der Beauftragten für Information und Datenschutz jährlich über Art, Umfang und Ergebnisse Bericht.

§ 14. Massnahmen bei Missbrauch

[1] Die missbräuchliche Nutzung der Informatiksysteme und -anwendungen stellt eine Verletzung der Dienstpflichten dar, welche nach dem Gesetz über das Staatspersonal[1]) und dem Verantwortlichkeitsgesetz[2]) sanktioniert werden können.

[2] Bei Verdacht auf strafrechtliche Handlungen wird Strafanzeige erstattet. Bei leichteren Vergehen kann auf Strafanzeige verzichtet werden.

[3] Bei wiederholten Verstössen gegen die Nutzungsvorschriften kann der Informatikdienstleister in Absprache mit der vorgesetzten Stelle dem betroffenen Anwender die Zugriffsberechtigung auf die Informatiksysteme entziehen.

§ 15. Informationspflicht

Der oder die Vorgesetzte einer Dienststelle stellt sicher, dass die Anwender die Nutzungsvorschriften, die Überwachungsmassnahmen sowie die möglichen Sanktionen bei Missbräuchen kennen.

§ 16. Aufhebung bisherigen Rechts

Mit Inkrafttreten dieser Weisung sind die Weisungen über den Einsatz von Personal Computern und Terminals in der kantonalen Verwaltung vom 16. Oktober 1990[3]) und die Benutzer-Richtlinien für Personal Computer und Terminals vom 16. Oktober 1990[4]) aufgehoben.

§ 17. Inkrafttreten

[1] Diese Weisung tritt am 1. Oktober 2003 in Kraft.

[2] Sie ist allen Mitarbeiterinnen und Mitarbeitern in geeigneter Form bekannt zu machen.

Yolanda Studer
Staatsschreiber – Stellvertreterin

Verteiler

Finanzdepartement (pa\aio\weisung\edv-weisung/Version4.doc)
Amt für Informatik und Organisation
Personalamt
Departemente
Staatskanzlei (SAN)
Vorgesetzte der Ämter und Dienststellen, je mit Schreiben
GS
BGS

[1]) BGS 126.1
[2]) BGS 124.21
[3] BGS 122.213.2
[4] BGS 122.213.21