



Weisung für die Benutzung von Informatikmitteln in der Verwaltung des Kantons Basel-Stadt

Weisung der Informatik-Konferenz Basel-Stadt
22. Oktober 2003
(mit Änderungen vom 15. September 2004, 7. März 2013 und 23. Juni 2016)

Inhaltsverzeichnis

1. Grundsatz.....	4
1.1 Ziele	4
1.2 Geltungsbereich	4
1.3 Verantwortungsbereich	4
2. Hardware.....	5
2.1 Beschaffungen, Installationen und Veränderungen	5
2.2 Mobile Geräte / Externe Arbeit / Externe Geräte	5
2.3 Anschluss ans DANEBS	5
3. Software	5
3.1 Beschaffungen, Installationen und Veränderungen	5
4. Datenbestände.....	6
4.1 Datensammlungen	6
4.2 Datensicherung	6
4.3 Aufbewahrung und Entsorgung	6
5. Passwörter	6
6. Computerviren.....	7
7. 7. Internet	7
7.1 Nutzung	7
7.2 Berechtigung	7
7.3 Verbotene Inhalte und Dienste	7
8. E-Mail.....	8
9. Private Nutzung von Informatik-Ressourcen.....	8
10. Überwachung und Folgen bei Widerhandlungen	8
10.1 Kontrollen	8
10.2 Widerhandlungen	9
11. Weitere Bestimmungen	9
11.1 Informationen zur Informatiksicherheit.....	9
12. Schlussbestimmung	9

Zusammenfassung für die eilige Leserin, den eiligen Leser¹

Die 10 goldenen Informatik-Sicherheitsregeln

1. Ich beschaffe, installiere oder verändere niemals Hard- / Software ohne Genehmigung.
2. Ich schütze meine Arbeitsstation vor unberechtigttem Zugriff auf Daten.
3. Ich sperre beim Verlassen des Arbeitsplatzes die Arbeitsstation (Ctrl+Alt+Del).
4. Ich gebe meine Passwörter nicht weiter, sie sind persönlich.
5. Ich gehe vorsichtig mit dem Versenden und Empfangen von E-Mails um.
6. Ich lade, installiere und verwende² keine Software aus dem Internet auf die Arbeitsstation.
7. Ich konsumiere und speichere keine Daten mit widerrechtlichem, beleidigendem oder herabwürdigendem Inhalt.
8. Ich melde Störungen und Sicherheitsrisiken unverzüglich den Informatikverantwortlichen.
9. Ich lasse nicht mehr benötigte Datenträger (CD, Diskette, etc.) physisch zerstören.
10. Ich informiere mich regelmässig unter <http://intranet.bs.ch/infrastruktur/informatik.html>.

¹ Eingefügt durch Beschluss vom 15. September 2004

² Eingefügt durch Beschluss vom 7. März 2013

Weisung für die Benutzung von Informatikmitteln in der Verwaltung des Kantons Basel-Stadt

22. Oktober 2003

Die Informatik-Konferenz erlässt gestützt auf § 11 der Verordnung zur Informatiksicherheit vom 9. April 2002³, sowie das Gesetz über den Schutz von Personendaten vom 18. März 1992⁴, das Urheberrechtsgesetz vom 9. Oktober 1992⁵ sowie das Personalgesetz vom 17. November 1999⁶ folgende Weisung:

1. Grundsatz

Die Weisung gilt für alle Benutzerinnen und Benutzer von Geräten der elektronischen Datenverarbeitung in der Verwaltung des Kantons Basel-Stadt. Sie beschreibt den Umgang mit den vorhandenen Informatikmitteln und nennt die dabei zu beachtenden Sorgfaltspflichten.

Unter den Informatikverantwortlichen wird die vom Departement respektive von den Dienststellen oder Organisationseinheiten bezeichneten Personen verstanden.

Unter Linie wird die Organisationsstruktur eines Departements verstanden. Dazu gehören insbesondere Dienststellen, Ressorts, Hauptabteilungen, Abteilungen, Organisationseinheiten, etc.

1.1 Ziele

Die vorliegende Weisung dient der Gewährleistung der Informatiksicherheit, des Datenschutzes und der Förderung des verantwortungsbewussten Umganges mit Informatikeinrichtungen (Vertraulichkeit, Verfügbarkeit, Datenintegrität).

1.2 Geltungsbereich

Diese Weisung gilt für alle Mitarbeiterinnen und Mitarbeiter des Kantons Basel-Stadt, einschliesslich Aushilfs- und Temporärpersonal. Sie umfasst alle für Verwaltungszwecke eingesetzten Informatikmittel, unabhängig vom Standort. Die Linie kann für einzelne Bereiche ergänzende Regelungen treffen.

1.3 Verantwortungsbereich

Für die Einhaltung dieser Weisung sind die Dienststellen resp. Ressorts zuständig.

³ SG 153.320.

⁴ SG 153.260.

⁵ SR 231.1.

⁶ 162.100.

2. Hardware

2.1 Beschaffungen, Installationen und Veränderungen

Die Beschaffung darf nur in Absprache mit den Informatikverantwortlichen erfolgen. Änderungen an der Hardware sind nicht gestattet. Dies gilt für alle Aus- und Umbauten der Geräte sowie für den Anschluss zusätzlicher Geräte. Bei einem Arbeitsplatzwechsel dürfen Geräte nur in Absprache mit der Linie und den Informatikverantwortlichen verschoben werden.

2.2 Mobile Geräte / Externe Arbeit / Externe Geräte

Als mobile Geräte gelten insbesondere Notebook, Palmtop, PDA, Handy, digitale Kamera, USB-Flashsticks, etc. Unter „externer Arbeit“ versteht man das Verrichten von Tätigkeiten ausserhalb der Dienststellen mit dienststelleneigener Infrastruktur. Unter „externe Geräte“ versteht man Geräte, welche nicht im Besitze der Dienststelle sind.

Die Benutzerinnen und Benutzer mobiler oder externer Geräte sind unter Beachtung der Weisungen der vorgesetzten Stelle für die Datensicherheit, Datenschutz, Diebstahlschutz und Datensicherung selbst verantwortlich.

Die Linie legt fest, welche Daten auf mobilen Geräten bearbeitet werden dürfen.

2.3 Anschluss ans DANEBS

Nicht im Besitz der Verwaltung stehende Geräte dürfen nur im Auftrag der Linie und in Absprache mit den Informatikverantwortlichen ans Datennetz Basel-Stadt (DANEBS) angeschlossen werden.

3. Software

3.1 Beschaffungen, Installationen und Veränderungen

Die Beschaffung darf nur in Absprache mit der Linie und den Informatikverantwortlichen erfolgen. Die Installation oder strukturelle Veränderung von Programmen darf nur in Absprache mit den Informatikverantwortlichen erfolgen.

Jegliche Eigenentwicklung inklusive Bereitstellung von Office-Makros ist ohne Auftrag der Linie nicht erlaubt.

4. Datenbestände

4.1 Datensammlungen

Das Anlegen von Datensammlungen mit personenbezogenen Daten richtet sich in jedem Falle nach dem Datenschutzgesetz Basel-Stadt. Für andere Datensammlungen gelten die linieninternen Weisungen.

Wer feststellt, dass jemand Zugang zu Datenbeständen hat, für welche er oder sie keine Berechtigung hat, muss dies unverzüglich der Linie oder den Informatikverantwortlichen melden. Wer ohne Berechtigung Zugang zu Datenbeständen hat, darf diesen Zugang nicht benutzen, muss diese Daten geheim halten und darf sie nicht verwenden.

4.2 Datensicherung

Alle Informationen und Daten, gleich ob in elektronischer Form oder Papierform vorhanden, sind vor unberechtigtem Zugriff zu schützen.

Datenablagen auf der lokalen Festplatte des PCs (Laufwerke C:\ oder weitere) sind zu vermeiden, da im Gegensatz zu den Netzlaufwerken keine automatische Sicherung erfolgt. Bei einem Gerätedefekt oder einem Austausch können diese Daten unwiederbringbar verloren gehen.

4.3 Aufbewahrung und Entsorgung

Magnetische und digitale Datenträger sind wie Papierdokumente wenn immer möglich unter Verschluss aufzubewahren. Dabei haben die Aufbewahrungsorte den Sicherheitsanforderungen (Schutz vor Einbruch, Feuer, Wasser, etc.) zu genügen. Die Dauer der Aufbewahrung richtet sich nach den gesetzlichen Vorschriften und Weisungen der Linie.

Vor Weitergabe beziehungsweise Entsorgung sind Datenträger in Absprache mit den Informatikverantwortlichen physisch zu zerstören oder mit Hilfe eines entsprechenden Tools unwiderruflich zu löschen.

5. Passwörter

Nach der Erstautorisierung ist unverzüglich das Passwort zu ändern. Passwörter müssen regelmässig geändert werden.

Passwörter sind persönlich, vertraulich und dürfen nicht bekannt gegeben werden.

Wenn der Betrieb besondere Anforderungen stellt, kann die Dienststellenleitung anordnen, dass ein Passwort hinterlegt werden muss oder von mehr als einer Person verwendet werden kann. Die Anordnung muss schriftlich erfolgen und die Anforderungen an die Sicherheit der jeweiligen Anwendung berücksichtigen.

Passwort-Notizen (falls vorhanden) sind unter Verschluss zu halten.

Es dürfen keine Passwörter verwendet werden, die einfach zu erraten sind, wenn man die Inhaberin oder den Inhaber kennt, wie zum Beispiel Namen, Adressen, Telefonnummern, Namen der Kinder oder von Haustieren usw.

Folgende Passwortregeln gelten ab dem 30.06 2016

Das Passwort muss mindestens aus **8** Zeichen bestehen und die Elemente der folgenden 4 Kategorien enthalten:

- Grossbuchstaben (z.B. ABC)
- Kleinbuchstaben (z.B. abc)
- Sonderzeichen (z.B. \$=?)
- Zahlen z.B. (z.B. 123)

Ein Passwort, welches die Kriterien erfüllt, könnte beispielsweise wie folgt aussehen:

@pEtr12r!

Der PC und mobile Geräte müssen mit einem Passwort geschützten Bildschirmschoner ausgerüstet sein. Dieser darf nicht deaktiviert werden.

Beim kurzfristigen Verlassen des Arbeitsplatzes muss der Bildschirm gesperrt werden. (CTRL+ALT+DEL). Beim längerfristigem Verlassen muss der PC ausgeschaltet werden.

6. Computerviren

Jeder PC ist mit einem aktuellen Virenschutzprogramm auszustatten. Dieses darf nicht deaktiviert werden. Um die automatische Virenschutzaktualisierung zu gewährleisten, muss der PC mindestens einmal innerhalb 24 Stunden ausgeschaltet werden.

Bei einem Virenereignis ist der Informatikverantwortliche umgehend zu informieren.

7. Internet

7.1 Nutzung

Das Internet ist für dienstliche Zwecke in Erfüllung der übertragenen Aufgaben zu verwenden.

Die private Nutzung des Internets darf nicht mit der Pflicht zur Erfüllung übertragenen Aufgaben in Konflikt geraten oder die Sicherheit der Informatikmittel beeinträchtigen.

7.2 Berechtigung

Eine Bewilligung für den Internetzugriff erteilt die Linie. Die Zugriffe auf die einzelnen Seiten im Internet werden zentral protokolliert.

7.3 Verbotene Inhalte und Dienste

Der Zugriff und das Auf- und Herunterladen oder die Weiterleitung von Material mit widerrechtlichem, beleidigendem oder herabwürdigendem Inhalt ist verboten (Erotik, Pornographie, Gewaltdarstellungen, extremistische oder rassistische Inhalte, etc.).

Es ist verboten, ohne ausdrückliche Bewilligung der Linie und ohne Absprache mit den Informatikverantwortlichen Software aus dem Internet herunterzuladen oder zu installieren (Gefahr von Viren, Verletzung von Urheberrechten).

8. E-Mail

Das automatische Umleiten von Mails auf eine externe Mailadresse ist aus sicherheits- und datenschutzrechtlichen Gründen untersagt.

Der Umgang mit E-Mail muss mit Vorsicht erfolgen. Die Vertraulichkeit ist beim Emailversand nicht gewährleistet (Vergleich: E-Mail gleich Postkarte). Diese kann nur durch geeignete Verschlüsselung erreicht werden.

Die Absendenden sind für die richtige Adressierung, Inhalte, insbesondere Anhänge, verantwortlich.

9. Private Nutzung von Informatik-Ressourcen

Die Linie kann die private Nutzung sowohl der Informatikmittel als auch des Internets in eigener Kompetenz erlauben, wenn die beanspruchten Ressourcen (Arbeitszeit, Netzwerkkapazität) hierbei vernachlässigbar sind. Die private Nutzung darf nicht mit der Pflicht zur Erfüllung übertragener Aufgaben in Konflikt geraten oder die Sicherheit der Informatikmittel beeinträchtigen.

Konfigurationsänderungen an der Hard- und Software für private Zwecke sind verboten.

Die kommerzielle Nutzung von Informatikmitteln zu privaten Zwecken ist nicht erlaubt.

Die Informatikverantwortlichen sind bei ihren Arbeiten nicht verpflichtet, zum Schutz privater Daten Massnahmen zu ergreifen oder zu unterlassen.

10. Überwachung und Folgen bei Widerhandlungen

10.1 Kontrollen

Bei Verdacht auf Missbrauch ist eine Einsicht in die Aufzeichnungsprotokolle der Internetnutzung ausschliesslich auf Anordnung der Linie möglich. Diese Überwachung hat die Grundsätze des Datenschutzes und des Schutzes der Privatsphäre im Rahmen der anwendbaren gesetzlichen Bestimmungen zu berücksichtigen. Die Einsicht in Mutationen von betrieblichen Datensammlungen ist jederzeit möglich.

Die betroffenen Mitarbeitenden sind über den Beginn und das Ende dieser Auswertung vorgängig zu informieren.

Bei Verdacht auf strafbare Handlungen bedarf es keiner vorgängigen Information der Mitarbeitenden.

10.2 Widerhandlungen

Widerhandlungen gegen die vorliegende Weisung werden mit personalrechtlichen Sanktionen geahndet und allenfalls strafrechtlich verfolgt (StGB Art. 197 ff, Art. 320).

Die Mitarbeitenden haben den Schaden (verlorene Arbeitszeit, Materialverbrauch, Kosten für Wiederherstellung, Reparaturen und Folgeschäden bei Ausfallzeit etc.), den sie dem Staat bei einem Verstoß gegen diese Weisungen grobfahrlässig oder vorsätzlich verursachen, zu ersetzen.

11. Weitere Bestimmungen⁷

11.1 Informationen zur Informatiksicherheit

Aktuelle Informationen sind im Intranet unter <http://informatik.intranet.bs.ch/verbindliche-vorgaben.html> verfügbar.

12. Schlussbestimmung

Die Weisung tritt sofort in Kraft. Sie ersetzt die Weisung des Zentralen Personaldienstes (ZPD) für die Einrichtung und Benutzung des Remote Access Service (RAS) vom Dezember 2001, die Weisung des ZPD für die Benutzung des Internet am Arbeitsplatz vom Dezember 2001 und die Benutzerrichtlinien der IK zur sicheren Verwendung von Internet/ Intranet vom 25. Oktober 2000.

Basel, 22. Oktober 2003

sig. Dr. Markus Grolimund
Vorsitzender der Informatik-Konferenz

sig. Georges Hatt
Sekretär der Informatik-Konferenz

⁷ 11.2. Gestrichen durch Beschluss vom 15. September 2004