Stadtrat Volker Stein
Dezernent Infrastruktur

Frankfurt am Main, 20. Juni 2013

Regelungen zur Nutzung von Internet-Diensten sowie zur Nutzung von Geräten und Programmen

Mit sofortiger Wirkung werden folgende, für alle Mitarbeiter/-innen einschließlich der Auszubildenden und Praktikanten/-innen aller Ämter, Referate und Eigenbetriebe der Stadt Frankfurt am Main mit Ausnahme des Eigenbetriebs Städtische Kliniken Frankfurt am Main-Höchst geltenden Regelungen getroffen:

1 Nutzung von Internet-Diensten

Ziel der dienstlichen Nutzung von Internet-Diensten ist die Verbesserung der Informationsbeschaffung und der Kommunikation. Das Internet besteht aus Netzwerken unterschiedlicher Angebote. Die in diesem Dokument getroffenen Regelungen gelten prinzipiell für alle Internet-Dienste.

Unter »Internet-Diensten« sind z.B. zu verstehen:

- World Wide Web (Anzeige von Informationsseiten)
- E-Mail (Elektronische Post)
- FTP (Datentransfer, Download)
- Newsgroups (Elektronische Pinnwände), Foren
- Kommunikationsdienste
- Netzwerkspeicher
- Soziale Netzwerke

Grundvoraussetzung für die Nutzung von Internet-Diensten ist ein PC-Arbeitsplatz gemäß den vom Arbeitskreis Strategie und Controlling IuK veröffentlichten Normen und Standards. Bei Nutzung von Internet-Diensten sind zwingend auf dem PC-Arbeitsplatz Vorkehrungen zum Schutz vor Computerviren und Hackerangriffen zu treffen.

1.1 World Wide Web

1.1.1 Freischaltung des Internet-Zugangs

Für den bedarfsgerechten Zugang zu außerhalb des Intranets der Stadt Frankfurt am Main gelegenen Internet-Angeboten ist eine Freischaltung des betroffenen Arbeitsplatzes notwendig. Je nach technischem Anschlussmodell ist diese Freischaltung beim Amt für Informations- und Kommunikationstechnik oder der zuständigen IT-Betreuungsstelle zu beantragen.

Voraussetzung für die Internet-Freischaltung ist das Vorliegen des dienstlichen Interesses. Hierüber entscheidet die jeweilige Amts- und Betriebsleitung.

1.1.2 Nutzungsregeln

Bei der Nutzung des Internet-Zugangs sind die rechtlichen Bestimmungen des Datenschutz-, Straf- und Urheberrechts unbedingt zu beachten, d. h. eine Rechtsnormen verletzende oder missbräuchliche Nutzung ist ebenso wie eine Nutzung für private geschäftliche oder gewerbliche Zwecke sowie zur Erzielung von privaten Einnahmen untersagt.

Eine Rechtsnormen verletzende oder missbräuchliche Nutzung des Internet-Zugangs liegt insbesondere dann vor, wenn Beschäftigte sich Zugang verschaffen zu extremistischen, rassistischen, pornografischen, verfassungsfeindlichen und kriminellen Zwecken dienenden und nach geltendem deutschen Recht verbotenen Inhalten, ohne dass eine dienstliche Notwendigkeit besteht. Schwere Computerdelikte liegen insbesondere in folgenden Fällen vor:

a) Unberechtigter Zugang zu geschützten Daten.
b) Diebstahl, Manipulation und Zerstörung fremder Daten.

c) Einbruchsversuche in Informationsverarbeitungssysteme (z.B. zum Ausspähen von Passwörtern).
d) Unberechtigte Nutzung von Informationsverarbeitungssystemen (Zugriff auf Informationen und Ressourcen ohne Einwilligung des Eigentümers).
e) Computermanipulation und Computersabotage.
f) Verletzung von Urheberrechten.
g) Erstellung von Raubkopien, unberechtigte Nutzung von Software.
h) Verbreitung und Speicherung von extremistischen, verfassungsfeindlichen, rassistischen, pornografischen und kriminellen Inhalten.
i) Unberechtigte Weitergabe von Daten aus dem Aufgabenbereich der Stadtverwaltung wie z.B. Personal- oder Geschäftsdaten. Dazu gehört auch die Verwendung dieser schützenswerten Daten in Gänze oder in Teilen innerhalb von so genannten „sozialen Netzwerken".

1.1.3 **Downloads** / **Herunterladen von Daten**

Das Herunterladen von Daten aus dem Internet oder von stadtinternen Serversystemen darf ausschließlich zu dienstlichen Zwecken erfolgen.

Insbesondere ist es untersagt, Programme und Mediendateien (Video- und Audio-Dateien) zu nichtdienstlichen Zwecken herunter zu laden oder dauerhaft zu übertragen (Streaming).

Die dienstliche Nutzung von Streaming-Quellen, auch bekannt als Web-Radio bzw. Internet-TV u.ä., ist zeitlich auf das erforderliche Maß zu beschränken.

Es dürfen ausschließlich Daten aus seriösen Quellen – z.B. Originalhersteller von Hard- und Software, öffentliche Institutionen –, nicht aber von unbekannten Anbietern heruntergeladen werden.

Ausführbare Dateien dürfen nur zu dienstlichen Zwecken und ausschließlich durch die jeweils zuständige Systemadministration installiert werden.

Die jeweiligen Urheberrechte, Lizenzrechte und die geltenden gesetzlichen Bestimmungen sind zu beachten.

1.1.4 **Uploads** / **Hochladen von Daten**

Das Hochladen oder Ablegen von dienstlichen Daten von lokalen städtischen Systemen auf externe Speichersysteme oder andere technische Angebote im Internet ist grundsätzlich untersagt.

Dienstliche Vorgänge, die die Praxis von sogenannten Uploads (z.B. auf externe Web-Server oder externe Shareport Pointal Server) notwendig machen, sind von den Amts- und Betriebsleitungen mit dem Amt für Informations- und Kommunikationstechnik und dem Referat Datenschutz und IT-Sicherheit zu regeln.

1.1.5 **Passwörter**

Für die Anmeldung an Internet-Diensten ist aus Sicherheitsgründen jeweils ein separates Kennwort zu verwenden, dass nicht im stadtinternen Gebrauch benutzt wird.

1.1.6 **Abmelden nach Aufgabenerfüllung**

Wird ein IT-System von mehreren Benutzern verwendet, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jeder über eine eigene Kennung verfügt. Ist es einem Dritten möglich, an einem IT-System oder in einer Internet-Anwendung unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich.

Daher sind alle Benutzer verpflichtet, sich nach Aufgabenerfüllung von der Anwendung und dem IT-System (Computer) abzumelden.

1.1.7 **Arbeitspausen**

Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen.

1.1.8 **Operative IT-Sicherheit**

Auf die für die technische Aufrechterhaltung der IT-Sicherheitsstruktur getroffenen Regelungen des Amtes 16 im Dokument „Nutzung von Internetdiensten“ wird verwiesen.

1.2 E-Mail

Grundsätzlich sollte jede/r Mitarbeiter/-in einschließlich der Auszubildenden und Praktikanten/-innen aller Ämter, Referate und Eigenbetriebe der Stadt Frankfurt am Main mit Ausnahme des Eigenbetriebs Städtische Kliniken Frankfurt am Main-Höchst mit Zugang zu einem IT-Arbeitsplatz über eine eigene E-Mail-Adresse verfügen.

Kenntnisnahme und Bearbeitung der eingehenden E-Mails sind sicherzustellen.

1.2.1 **Einrichtung von E-Mail-Postfächern**

Postfächer können für Ämter und Betriebe, Organisationsbereiche (Abteilungen, Sachgebiete, Fachbereiche, Infostellen) und Personen eingerichtet werden.

Regel:

<Vorname>.<Nachname>@stadt-frankfurt.de

<Bereich>.<Organisationskennzeichnung>@stadt-frankfurt.de

1.2.2 **Benutzerbezogene E-Mail-Adressen**

Um einen geregelten E-Mail-Verkehr zu gewährleisten, darf stadtweit keine E-Mail-Adresse doppelt vergeben werden. Bei mehrfach vorkommenden Namen ist dieser um die Ämterbezeichnung sowie ggf. Ziffern zu ergänzen, z.B.:

karl.mustermann@stadt-frankfurt.de
karl.mustermann.amt40@stadt-frankfurt.de
karl.mustermann2.amt40@stadt-frankfurt.de

Personen, die in einer besonderen Vertrauensfunktion tätig sind (z.B. Frauenbeauftragte, Schwerbehindertenvertreter, Personalräte), wird zur Wahrnehmung dieser Funktion eine zusätzliche, funktionsbezogene E-Mail-Adresse eingerichtet:

karl.mustermann.pr@stadt-frankfurt.de	(Personalrat)
karl.mustermann.sb@stadt-frankfurt.de	(Schwerbehindertenvertreter)
karola.musterfrau.fb@stadt-frankfurt.de	(Frauenbeauftragte)

1.2.3 **Organisationsbezogene E-Mail-Adressen**

Die Ämter und Betriebe sind gehalten, ein Amtspostfach einzurichten und diese Adresse im Geschäftsverkehr zu verwenden.

z.B.:

info.amt40@stadt-frankfurt.de

Die Einrichtung weiterer Funktionspostfächer obliegt den Ämtern und Betrieben; es wird empfohlen, selbsterklärende Namen zu verwenden.

1.2.4 **Versand zentraler E-Mails**

Im globalen Adressbuch steht ein Ordner „Zentrale E-Mail“ für die Ämter und Betriebe zur Verfügung. In diesem Ordner werden die von den Ämtern und Betrieben gemeldeten Funktions-E-Mail-Adressen hinterlegt. Somit kann eine zentrale E-Mail an alle Dezernate, Ämter und Betriebe versendet werden.

Der Versand von zentralen E-Mails ist ausschließlich von der gemeldeten E-Mail-Adresse möglich.

1.2.5 **Versand zentraler E-Mails an ausgewählte Empfänger**

Für E-Mail-Verteiler an externe Empfänger kann das Angebot des Amtes 16 genutzt werden.

1.2.6 **Adressierungsart**

Jede Nachricht ist mit einem aussagefähigen Betreff zu versehen. Bei der Adressierung der Empfänger stehen folgende Möglichkeiten zur Verfügung:

- »An«: Mit dieser Adressierungsart wird der Hauptempfänger der Mitteilung angewählt.
- »CC« (Carbon Copy): Diese Adressierungsart ist zu nutzen, wenn die Mitteilung einem oder mehreren Empfängern zur Mitkenntnis zugestellt werden soll.
- »BCC« (Blind Carbon Copy): Diese Adressierungsart ist grundsätzlich untersagt.

Zur Adressierung innerhalb der Stadtverwaltung steht das globale Adressbuch bereit. Darüber hinaus gehende E-Mail-Adressen von Geschäftspartnern oder anderen Ansprechpartnern können in einem privaten oder teambezogenen Outlook-Adressbuch gespeichert werden.

Über die jeweils zuständige Systemadministration ist es möglich, stadtweit anlassgerechte Verteilerlisten zur Verfügung zu stellen. Derartige Listen können auch von den Anwenderinnen und Anwendern selbst in Outlook-Adressbüchern angelegt und verwaltet werden.

Adressat einer E-Mail können somit sowohl einzelne Personen (oder Organisationseinheiten) als auch Personengruppen sein. Bei der Verwendung von Personengruppen ist darauf zu achten, dass der Empfängerkreis nicht unnötig groß bemessen ist.

Die Notwendigkeit und Aktualität von Verteilerlisten ist vom Eigentümer regelmäßig zu überprüfen. Sollte eine Verteilerliste nicht mehr benötig werden, ist diese zu löschen.

1.2.7 **Absenderangabe**

Jede E-Mail muss die nachfolgende Absenderangabe enthalten:

Stadt Frankfurt am Main
- Der Magistrat – oder – Die Oberbürgermeisterin -
(Amt)
(Organisationseinheit)
(Name d. Ansprechpartnerin/Ansprechpartners)
(Straße)
(Postleitzahl) Frankfurt am Main

(Telefon)
(Fax)
(E-Mail-Adresse d. Ansprechpartnerin/Ansprechpartners)
(Internet: www.frankfurt.de oder amtspezifische URL, z.B. www.ordnungsamt.stadt-frankfurt.de)

Es wird empfohlen, bei Nachrichten keinen weiteren Text (Disclaimer o.ä.) anzuhängen.

1.2.8 **E-Mail-Inhalte**

Die Anrede der E-Mail sollte dem Betreff angemessen Rechnung tragen. Insbesondere im formellen Schriftverkehr sind vertrauliche Anreden, die Verwendung von Emoticons (z.B. Symbole

für gut/schlecht oder freundlich/böse) und das Mischen von privaten und geschäftlichen Angelegenheiten unbedingt zu unterlassen. Im Übrigen wird auf die Regelungen der AGA I, Ziffer 4.7.6 (Briefstil) verwiesen. Antwort-E-Mails und weitergeleitete E-Mails sollten auf wichtige Textpassagen gekürzt werden.

Der Versand von Programmen ist – außer für die zuständigen Systemadministrationen – ausnahmslos untersagt.
Der Versand vertraulicher Unternehmensdaten und vertraulicher personenbezogener Daten innerhalb der Stadtverwaltung ist auf das dienstlich erforderliche Maß zu beschränken. Auf die korrekte Adressierung ist hierbei besondere Sorgfalt zu legen.

Im E-Mail-Verkehr mit externen Stellen dürfen grundsätzlich keine

- lizenzierte Programme,
- vertrauliche Unternehmensdaten und
- vertrauliche personenbezogene Daten

ganz oder in Teilen, gepackt übermittelt werden. Dies gilt nicht, wenn diese Übermittlung aus dienstlichen Gründen zwingend erforderlich ist. Auf das Verschlüsseln von Daten ist zu verzichten.

1.2.9 **Verbindlichkeit von E-Mails, interne Weiterleitung, Speicherung, Rechtscharakter**

Die bestehenden Regelungen zur Behandlung von Postein- und -ausgängen – insbesondere im Hinblick auf die Unterrichtung von Vorgesetzten – (z.B. gemäß AGA I und amtsinterner Regelungen) sind, soweit systembedingt übertragbar, grundsätzlich auf E-Mails entsprechend anzuwenden.

Auch mit einer einfachen oder fortgeschrittenen elektronischen Signatur[1] unterzeichnete E-Mails sind rechtsgültig; außer, es ist gesetzlich die Schriftform gefordert oder eine elektronische Signatur ausdrücklich ausgeschlossen. Nicht jeder Verwaltungsakt oder Vertrag bedarf der Schriftform, daher ist die qualifizierte elektronische Signatur ein Ausnahmeerfordernis. Allerdings ist die Beweiskraft von nicht mit einer solchen Signatur unterzeichneten E-Mails im Streitfall nur gering. E-Mails und deren Anlagen ohne qualifizierte elektronische Signatur sind keine Originale, sondern (nicht fälschungssicher unterschriebene) elektronische Dokumente, die u.a. nachträglich ohne Hinterlassen von Spuren verändert werden können. Es kann nicht ausgeschlossen werden, dass E-Mails unbefugt und unbemerkt mitgelesen und verwendet werden. Ferner könnte sich der Absender einer E-Mail als ein anderer ausgeben.

Eingehende E-Mails sind als verbindliche Willenserklärung anzusehen und entsprechend zu behandeln. Bei begründeten Zweifeln über die Authentizität der Absenderangabe ist eine kurzfristige Verifizierung mit geeigneten Maßnahmen notwendig.

Eine Weiterleitung von Kettenbriefen ist, auch wenn der Anlass plausibel geschildert ist, stets nicht statthaft.

Für die Archivierung von E-Mails gilt die städtische Aktenordnung analog. Eingehende Dokumente sind – soweit die Archivierung erforderlich ist – in den jeweiligen fachbezogenen Datei-

---

[1] EINFACHE ELEKTRONISCHE SIGNATUR

Z.B. Schriftzug „Im Auftrag, Müller“ oder Abbildung der gescannten Unterschrift.

FORTGESCHRITTENE ELEKTRONISCHE SIGNATUR

Signatur mit Hilfe eines einmaligen Signaturschlüssels, der ein Software- oder auf einer PKI-Chipkarte befindlicher Hardwareschlüssel sein kann. Die Authentizität der Signatur wird von einer nicht gesetzlich autorisierten Stelle (z.B. VeriSign, Verwaltungs-PKI, andere externe Zertifizierungsstellen, interne Zertifizierungsstellen) bestätigt.

QUALIFIZIERTE ELEKTRONISCHE SIGNATUR

Signatur mit Hilfe eines einmaligen Signaturschlüssels, der auf einer PKI-Chipkarte sicher verwahrt sein muss. PKI-Karte, Chipkartenterminal und Signatursoftware müssen zertifiziert sein. Die Authentizität der Signatur wird von einem von der Bundesnetzagentur autorisierten Trustcenter bestätigt.

ordnern abzulegen (Näheres regeln die Ämter und Betriebe), zusätzlich ist eine Papierablage erforderlich, wenn die Nachricht erhebliche Auswirkungen auf Rechte und Pflichten der Stadt Frankfurt am Main – z.B. in Bezug auf ein bestehendes Vertragsverhältnis – besitzt.

Soweit eine elektronische Archivierung mittels spezieller Archivierungsprogramme erfolgt, sind die datenschutzrechtlichen Regelungen (z.B. § 6 HDSG - Verfahrensverzeichnis) zu prüfen.

1.2.10 **Abwesenheitsassistent**

Bei vorhersehbarer Abwesenheit (z.B. Urlaub, Fortbildung, Dienstreisen) ist der Abwesenheitsassistent zu aktivieren und auf eine alternative Kontaktstelle – die jeweilige Vertretung bei Abwesenheiten – zu verweisen. Da dies im Falle von unvorhersehbaren Abwesenheiten nicht möglich ist, sind amtsinterne Festlegungen zu treffen.

1.2.11 **Sicherheitsaspekte**

Eingehende E-Mails, deren Absender oder Inhalt zweifelhaft erscheinen und insbesondere zum Aktivieren von Programmen und sonstigen Eingaben auffordern, sind unverzüglich ohne weitere Behandlung zu löschen. Im Zweifelsfall ist die zuständige Systemadministration zu verständigen.

Sollten Nachrichten Dritter mit Virenwarnungen eingehen, sind diese zur Prüfung an die jeweils zuständige Systemadministration weiterzuleiten. Diese erteilt auch Auskunft bei Unklarheiten zu Handlungsanweisungen in von dort ergangenen Virenwarnungen.

1.2.12 **Namenskonventionen**

Grundsätzliche zu beachtende Regelungen für sämtliche Namenskonventionen, für den Einsatz eines stadtweiten Verzeichnisdienstes, sind durch das Amtes 16 im Dokument „Namenskonventionen (Basisinfrastruktur, Active Directory und Exchange 2003) veröffentlicht.

1.2.13 **E-Mail-Sicherheit**

Auf die für die technische Aufrechterhaltung der IT-Sicherheitsstruktur getroffenen Regelungen des Amtes 16 im Dokument „E-Mail Verkehr der Stadt Frankfurt“ wird verwiesen.

1.3 Nutzungsregelungen Echtzeitkommunikationsprogramme

Bei der Nutzung von Echtzeitkommunikationsprogrammen (z.B. Messenger bzw. Chat-Programme), die im Internet angeboten werden, sind der Austausch von Dateien sowie die Freigabe des eigenen Bildschirminhaltes ins Internet grundsätzlich nicht gestattet.

1.4 Protokollierungen/Auswertung der Protokolle

Der Zugriff auf Internetdienste wird durch die beteiligten Datenverarbeitungssysteme standardmäßig protokolliert, um Auswertungen nach Netzwerkbelastungs- und Abrechnungsgesichtspunkten zu ermöglichen.

Die Protokollierung wird nicht zur individuellen Leistungs- und Verhaltenskontrolle eingesetzt.

Die Protokollierungen sind spätestens nach drei Monaten zu löschen.

1.4.1 **Personenbezogene Einzelauswertung**

Eine personenbezogene Einzelauswertung von Protokollen ist nur dann zulässig, wenn ein konkreter Anlass dieses rechtfertigt und die Angelegenheit mit dem Beschäftigten nicht anderweitig geklärt werden kann. Anlässe, die zu einer personenbezogenen Auswertung von Protokollen führen können, sind in 1.1.2 aufgeführt.

Es muss auf jeden Fall ein Anfangsverdacht bestehen, dass durch die Nutzung von Internet-Diensten gegen dienst- bzw. arbeitsrechtliche Pflichten oder Weisungen verstoßen wird.

Der oder die Beschäftigte ist zuvor zu unterrichten und zu den aufgetretenen »Auffälligkeiten« zu hören. Es soll zunächst versucht werden, den Verdacht auch ohne eine Auswertung auszuräumen. Die Auswertung ist als »letzte Möglichkeit« anzusehen, wenn eine andere Klärung nicht möglich ist.

Von einer vorherigen Unterrichtung d. Beschäftigten ist allerdings abzusehen, wenn dadurch die Aufklärung erschwert oder verhindert wird bzw. wenn der Verdacht auf strafbare Handlungen (AGA I, Abschnitt 2.3.1) dies nicht sinnvoll erscheinen lässt.

Die personenbezogene Auswertung ist durch die Amts-/Betriebsleitung bzw. dessen Vertretung schriftlich zu verfügen. In besonderen Fällen kann es ggf. erforderlich sein, außer dem Internetprotokoll auch das Systemprotokoll des entsprechenden PC-Netzwerks (Server) und im Bedarfsfall auch die »Übersichten über Anwesenheiten« aus der Automatisierten Zeiterfassung (AZE) bzw. Arbeitszeitkarten heranzuziehen. Die Rechte nach dem HGLG und HPVG sind zu wahren. Für den Fall der Erstellung personenbezogener Einzelauswertungen ist die Personalvertretung vorab zu informieren und auf Verlangen hinzuzuziehen. Nach jeder Auswertung erfolgt eine schriftliche Dokumentation durch die Auswertenden nebst Unterschrift.

2 Fernzugriff auf das städtische Datennetz

2.1 Zugriff auf das städtische E-Mail – Exchange –System (z.B. OWA - Outlook–Web–Access)

Die Einrichtung eines Zugriffs auf das städtische E-Mail – Exchange-System von externen Geräten (z.B. bei anderen städtischen Ämtern oder vom privaten Rechner), um E-Mails, Kontakte, Notizen oder Termine bearbeiten zu können, ist ausschließlich im dienstlichen Interesse gerechtfertigt. Dieser web-basierende Zugriff auf Outlook (OWA-Zugriff) kann durch die jeweils zuständige Administration eines Amtes/Betriebes direkt eingerichtet werden.
Vor Einrichtung eines solchen Zugriffs ist durch die Daten verarbeitende Stelle eine Abwägung zwischen dienstlichem Erfordernis und dem Schutz personenbezogener Daten oder sonstiger Vertrauensstellungen vorzunehmen. Die Amts- oder Betriebsleitung entscheidet schriftlich über die Zulassung eines solchen Zugriffs.

2.2 Einrichtung von externen Zugängen für Telearbeitsplätze oder für einen externen Zugriff auf Verfahren und Programme

Soweit zur dienstlichen Nutzung der externe Zugriff auf IT-Systeme, Verfahren oder Programme erforderlich ist (z.B. Telearbeitsplatz, Notfallplanung, Remote–Zugang), hat dies ausschließlich in Abstimmung mit dem Amt für Informations- und Kommunikationstechnik (über das dort eingerichtete Portal; siehe Anlage) zu erfolgen. Auch in diesen Fällen ist eine Abwägung, wie unter Ziffer 2.1 gefordert, vorzunehmen und zu dokumentieren.

Die Ausgestaltung eine Telearbeitsplatzes ist beteiligungspflichtig. Die Beteiligungsrechte nach dem Hessischen Gleichberechtigungsgesetz (HGlG) und dem Hessischen Personalvertretungsgesetz (HPVG) sind in diesem Fall zu beachten.

2.3 Zugriff mittels Teleservice

Soweit zur dienstlichen Nutzung ein Zugriff mittels Teleservice des Amtes für Informations- und Kommunikationstechnik eingerichtet werden soll, gelten die Regelungen dieser Richtlinie und die in Ziffer 8.4 und 8.8 der AGA II analog.

Andere Methoden, um auf IT-Systeme oder Verfahren innerhalb des Stadtnetzes zuzugreifen, sind mit dem Amt 16 abzustimmen.

3 Nutzung von Geräten und Programmen

3.1 Nutzung dienstlicher Geräte und Programme zu privaten Zwecken

Die private Nutzung von Computern, Programmen und Internet-Diensten ist grundsätzlich unter Beachtung folgender Regeln gestattet:

a) PC-Arbeitsplätze und Internet-Dienste werden zur Erfüllung dienstlicher Aufgaben bereitgestellt.
b) Die Betriebsbereitschaft der Geräte und Programme darf vom Anwender nicht beeinträchtigt werden.
c) Rechtsvorschriften (Datenschutzrecht, Strafrecht, Urheberrecht) sind zwingend einzuhalten.
d) Dienstliche Belange gehen stets vor; die Arbeit darf unter der privaten Nutzung nicht leiden. Die private Nutzung ist auf Pausen oder die Zeit vor dem Dienstbeginn bzw. nach dem Dienstende zu beschränken.
e) E-Mails haben niemals rein privaten Charakter, da die E-Mail-Adresse die Angabe »@stadt-frankfurt.de« enthält und daher vom Empfänger ggf. Ansprüche gegen die Stadt Frankfurt am Main geltend gemacht werden können. Private E-Mails dürfen keine dienstlichen Absenderangaben (Organisationseinheit, Anschrift) tragen und sind deutlich als »privat« zu kennzeichnen.

Die Amts- und Betriebsleitungen sind berechtigt, bei Zuwiderhandlung diese Gestattung im Einzelfall anlassbezogen einzuschränken oder zu untersagen.

Die private Nutzung von Internet-Diensten erfordert die vorherige Abgabe einer Erklärung nach dem Telekommunikationsgesetz (TKG), mit der d. Beschäftigte der anlassbezogenen Einsicht und Auswertung der Nutzungsprotokolle durch den Arbeitgeber zustimmt (siehe **Anlage** »Einwilligungserklärung gemäß § 93 des Telekommunikationsgesetztes«). Die private Nutzung von Internet-Diensten ist nicht gestattet, wenn diese Erklärung nicht abgegeben wird.

3.2 Nutzung privater Geräte und Programme für dienstliche Zwecke

Die Nutzung privater Geräte und Programme für dienstliche Zwecke ist grundsätzlich untersagt. Ausnahmen können von den jeweiligen Amts- und Betriebsleitungen in begründeten Fällen zugelassen werden und bedürfen der schriftlichen Genehmigung.

Für den Anschluss und Betrieb mobiler Datenverarbeitungs- und Speichergeräte wird auf die AGA II Ziffer 8.8 verwiesen.

3.2.1 Räume mit Schutzbedarf

Die Nutzung von privaten Computern/Notebooks etc. ist in Räumen die einem hohen Schutzbedarf unterliegen grundsätzlich nicht gestattet.

Bei der Nutzung von privaten Handys, PDAs oder Smartphones darf der Schutz der dienstlichen Daten nicht beeinträchtigt werden. Die Amts- und Betriebsleitungen können die Nutzungserlaubnis im Einzelfall anlassbezogen einschränken oder untersagen.

4 Folgen des Verstoßes gegen diese Dienst- und Geschäftsanweisung

Bei Zuwiderhandlung gegen diese Dienst- und Geschäftsanweisung sind die Amts- und Betriebsleitungen berechtigt, vorübergehend oder dauerhaft die teilweise oder vollständige Nutzung von Geräten, Programmen und Internet-Diensten zu untersagen sowie dienst- und arbeitsrechtliche Konsequenzen zu ziehen.

Die Rechte nach dem HGlG und HPVG sind zu wahren.

Schwerwiegende Computerdelikte unter Verletzung gesetzlicher Vorschriften ziehen eine strafrechtliche Verfolgung nach sich.

Die hier getroffenen Regelungen sind allen betroffenen Bediensteten gegen Unterschrift zur Kenntnis zu geben.

Über diese Nutzungsregeln werden die Bediensteten regelmäßig (jährlich) informiert, auf eventuelle Änderungen ist hinzuweisen. Die Kenntnisnahme ist vom Beschäftigten zu bestätigen. Ein Vermerk ist zu den Sachakten zu nehmen.

Stein

Anlagen

Name, Vorname	Personalnummer

Einwilligungserklärung

(Stand: April 2013)

1. Nutzung von Internetdiensten

Ich bin damit einverstanden, dass auch bei einer privaten Nutzung des Internets ein Einzelnachweis der Nutzungsdaten erstellt wird. Diese Daten können keine Auskünfte über die Inhalte der genutzten Internetressourcen geben. Es wird hierbei die Zeit der Nutzung, die Internetadresse der genutzten Seiten sowie die übertragene Datenmenge protokolliert. Die im Einzelnachweis enthaltenen Nutzungsdaten können von meinem Dienstherrn/Arbeitgeber anlassbezogen überprüft werden, um festzustellen, ob die nachgenannten Bedingungen von mir eingehalten worden sind.

Mir ist bekannt, dass ich Internet-Dienste nur für private Zwecke nutzen darf, wenn dadurch dienstliche Interessen nicht beeinträchtigt werden. Eine Beeinträchtigung der dienstlichen Interessen liegt insbesondere dann vor, wenn ich durch die private Nutzung von Internet-Diensten die mir übertragenen Aufgaben vernachlässige, interne Daten auf Systemen außerhalb der Stadtverwaltung ablege bzw. unrechtmäßig per E-Mail versende, die Verfügbarkeit der dienstlichen informations- und kommunikationstechnischen Einrichtungen gefährde oder das Ansehen der Stadt schädige.

Mir ist ferner bekannt, dass ich staats- bzw. verfassungsfeindliche, antidemokratische, rassistische, pornografische, sexistische, gewaltverherrlichende oder (sonstige) strafrechtlich relevante Internetinformationen nicht bewusst abrufen, ausdrucken, speichern, verteilen oder anderweitig verwenden darf. Auch eine Nutzung von Internet-Diensten für eigene geschäftliche/gewerbliche Zwecke oder zur Erzielung von privaten Einnahmen ist unzulässig. Ich beachte bei meiner Internetnutzung die städtischen Regelungen (insbesondere AGA II, Abschnitt 8), die ich im Intranet der Stadtverwaltung einsehen kann.

Wenn begründete Zweifel an meiner korrekten Nutzung von Internet-Diensten oder der Beachtung der obigen Bedingungen auftreten, bin ich bereit, bei der Aufklärung mitzuwirken. Ich bin davon unterrichtet worden, dass die Auswertung meiner Internet-Nutzungs- und Abrechnungsdaten vorgenommen werden kann, wenn der hinreichende Verdacht entsteht, dass ich gegen die oben genannten Bedingungen für die private Nutzung verstoßen habe. In einem solchen Fall können auch Systemprotokolle des Servers und ggf. »Übersichten über Anwesenheiten« aus der automatisierten Zeiterfassung (AZE) bzw. Arbeitszeitkarten mit herangezogen werden soweit dies erforderlich ist. Mir ist bekannt, dass ein Verstoß gegen die vorstehenden Regelungen dienst- oder arbeitsrechtliche Konsequenzen haben kann.

Die Protokolle zur Erstellung der Einzelnachweise werden nach Ablauf von 30 Tagen nach Erstellung auf dem entsprechenden Serversystem (Proxyserver, E-Mail-Server) im Amt 16 gelöscht.

Mir ist außerdem bekannt, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Dieser Widerruf ist zu protokollieren. Bei Widerruf wird die private Nutzung von Internet-Diensten untersagt.

Ich bin damit einverstanden, dass jeglicher Internetdatenverkehr mit Virenscannern auf Schadcode oder Angriffsmuster hin überprüft wird. Dies gilt auch für verschlüsselte Webseiten (also Seiten, die per „https“ aufgerufen werden, wie z.B. beim Online Banking oder bei der Übermittlung von Kreditkartendaten zum Zwecke des Einkaufs im Internet). Diese Verschlüsselungen werden beim Übergang aus dem Internet ins städtische Netzwerk durch ein „Blackbox-Verfahren“ aufgehoben, bei dem es technisch ausgeschlossen ist, dass Inhalte mitgelesen, bekannt gemacht oder weitergeleitet werden.

Die Entschlüsselung der Daten geschieht maschinell und allein zu dem Zweck, Schadcode oder Angriffsmuster festzustellen; eine weitergehende inhaltliche Kenntnisnahme und Bewertung der übertragenen Daten durch städtische Mitarbeiter oder Dritte findet nicht statt. Gefährden Inhalte die Sicherheit des städtischen IT-Verbundes, wird die Datenübertragung blockiert. Die übertragenen Daten bleiben im Übrigen unverändert. Mit der Entschlüsselung von https-Verbindungen zum Zwecke des Virenscannens erkläre ich mich ausdrücklich einverstanden.

Mir ist außerdem bekannt, dass ich auch diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Dieser Widerruf ist zu protokollieren. Bei Widerruf wird die private Nutzung von Internet-Diensten untersagt.

2. Postfachzugriff bei unvorhergesehener Abwesenheit oder bei Ausscheiden

a) Aktivieren des Abwesenheitsassistenten

Ich bin damit einverstanden, dass im Falle meiner unvorhergesehenen, längeren, insbesondere krankheitsbedingten Abwesenheit oder bei Ausscheiden ein/e berechtigte/r Systemadministrator/in in Abstimmung mit einem Vertreter/einer Vertreterin der Personalverwaltung oder des Fachbereiches, in dem ich tätig bin, den Abwesenheitsassistenten aktiviert.

b) Zugriff auf E-Mails aus zwingenden dienstlichen Gründen

Der Zugriff auf und die Öffnung einzelner E-Mails wird grundsätzlich nicht vorgenommen. Sollte sich allerdings aus zwingenden dienstlichen Gründen im Einzelfall die Notwendigkeit eines solchen Zugriffs ergeben (z.B. wegen Fristwahrung bei vergaberechtlichen Vorgängen), ist hierfür in Anwendung der DV 217 (siehe AGA II Ziffer 8.9 - § 6) in den Ämtern und Betrieben mit der zuständigen Personalvertretung ein Verfahren zu vereinbaren.

Mir ist bewusst, dass mein Arbeitgeber/Dienstherr technisch den Zugriff auf alle E-Mails in meinem Postfach hat. Dies betrifft auch meine privaten E-Mails. Es wird vermieden, deren Inhalt einzusehen. Dienstliche E-Mails werden in den vorgenannten Fällen im Vieraugenprinzip anhand der Betreffzeile herausgesucht und zur Bearbeitung an die zuständige Stelle geleitet. Über den Zugriff auf mein Postfach werde ich nach Rückkehr unaufgefordert umfassend informiert.

c) Zugriff auf E-Mail-Postfächer von Mitgliedern nachfolgender Gremien

Werden E-Mails von Mitgliedern einer Personalvertretung oder einer Schwerbehindertenvertretung aus den zuvor genannten Gründen benötigt, muss ein Mitglied der jeweiligen Vertretung beteiligt werden.

d) Zugriff auf E-Mail-Postfächer von Frauenbeauftragten

Soweit ein Zugriff auf das Postfach von Frauenbeauftragten erforderlich ist, wird wie unter Buchstabe c) dieser Erklärung verfahren.

e) Löschen des persönlichen E-Mail-Postfaches nach Beendigung des Dienst- oder Beschäftigungsverhältnisses

Mir ist bekannt, dass nach Beendigung meines Dienst- oder Beschäftigungsverhältnisses mein persönliches E-Mail-Postfach zeitnah gelöscht wird.

f) Schlussbestimmung

Diese Erklärung ersetzt alle bisher abgegebenen Einwilligungserklärungen zur E-Mail- und Internetnutzung und wird zu meiner Personalakte genommen.

Frankfurt am Main, Datum	siehe Empfangsbescheinigung Unterschrift