Dienstanweisung Nr. 4/1-16,2

für den Einsatz und die Nutzung von stationärer und mobiler IT im Bezirksamt Harburg

(DA-Bez-IT)

vom 01.11.2008
in der Fassung vom 01. Januar 2019

Einleitung

Diese Dienstanweisung gilt für alle Beschäftigten im Bezirksamt Harburg. Sie regelt die Nutzung der Informationstechnik in Bezug auf die Informationssicherheit, die geltenden Bestimmungen des bundes- und landesrechtlichen Datenschutzes sowie die gesetzlichen und betrieblichen Anforderungen der Datensicherung.

Ziel dieser Dienstanweisung ist der bestimmungsgemäße Einsatz von und der Umgang mit der genutzten Informationstechnologie. Insbesondere stehen hierbei Sicherheitsbedürfnisse hinsichtlich der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen, datenschutzrechtliche Erfordernisse, die Einhaltung von getroffenen Rahmenvertragsvereinbarungen sowie gesetzliche und arbeitsrechtliche Absicherung der Beschäftigten im Vordergrund. Die wichtigsten zu beachtenden Regelungen sind im Anhang zu dieser Dienstanweisung als Linkliste aufgeführt.

1 Begriffsdefinition

1.1 Der Begriff Endgerät umfasst alle in der FHH eingesetzten technischen Geräte, die Daten verarbeiten können. Ausgenommen sind Multifunktionsgeräte, Drucker, Scanner, Faxgeräte, Kopierer, Labor- und Meßgeräte sowie Geräte, die ausschließlich für sprachliche Kommunikation genutzt werden (Telefonie).

1.2 Als mobiles Endgerät werden unter anderem folgende Geräte bezeichnet:

- Notebook
- Pentop
- Smartphone
- Tablet

1.3 Unter IT-Zubehör fallen Komponenten oder Geräte, die sich außerhalb einer Zentraleinheit eines Endgerätes befinden, z.B. Kameras, Kopfhörer und

- Externe Speichermedien (USB-Stick, externe Festplatten)

Die unter 1.1 bis 1.3 genannten technischen Geräte werden im Folgenden als IT-Geräte bezeichnet.

2 Organisation, Rollen, Verantwortlichkeiten

2.1 IT-Beauftragter

Der IT-Beauftragte ist der Dezernent für Steuerung und Service. Er koordiniert die Festsetzung von Prioritäten für IT-Vorhaben und wirkt bei Entscheidungen von grundsätzlicher Bedeutung im Bereich IT in übergeordneten Gremien mit. Er steuert und kontrolliert die Maßnahmen zur Einführung und zum Betrieb von IT-Technik im Bezirksamt.

2.2 N/ITB

Die für die übergreifenden IT-Angelegenheiten in den Bezirksämtern zuständige Dienststelle ist die Zentralstelle für IT-Angelegenheiten der Bezirksverwaltung. N/ITB ist unter anderem Auftraggeber gegenüber Dataport für die Softwareprodukte, regelt übergreifende Betriebsaufgaben und stellt den Informationssicherheitsbeauftragten der Bezirksverwaltung.

2.3 RS-IT

Die für IT-Angelegenheiten im Bezirksamt zuständige Organisationseinheit RS-IT im Dezernat für Steuerung und Service ist zuständig für die lokale IT-Infrastruktur und IT-Organisation. Hierzu gehören im Wesentlichen die Benutzer- und Betriebsmittelverwaltung sowie die Funktion des Auftraggebers gegenüber Dataport für IT-Infrastruktur und IT-Arbeitsplätze im Bezirksamt.

2.4 Anwender

Die Anwender sind die Endnutzer der IT-Geräte.

2.5 Dataport

Dataport ist der zentrale IT-Dienstleister der Freien und Hansestadt Hamburg und betreibt und betreut grundsätzlich die in der Bezirksverwaltung eingesetzte Hardware und Software.

2.6 Personalrat

Der Personalrat wird entsprechend der Vorgaben des Hamburgischen Personalvertretungsgesetzes (HmbPersVG) beim Einsatz von Hard- und Software eingebunden.

3 Beschaffung und Nutzung von IT-Geräten und Software

3.1 IT-Geräte und Software dürfen ausschließlich durch oder mit Zustimmung von RS-IT oder N/ITB beschafft werden.

3.2 Alle mit der Nutzung von IT-Geräten zusammenhängenden Tätigkeiten, wie z.B. Inbetriebnahme, Administration, Umzug, Reparatur, Öffnung, Veränderung, erfolgen grundsätzlich durch Dataport oder von Dataport beauftragte Subunternehmen. In Ausnahmefällen kann die Administration von IT-Geräten auch durch Mitarbeiter von RS-IT erfolgen.

3.3 RS-IT veranlasst die Einhaltung der einschlägigen Bestimmungen in den Bereichen Arbeitsschutz und Ergonomie im Zuge der Erstausstattung von Arbeitsplätzen mit IT-Technik. Eine regelmäßige Überprüfung der Arbeitsplätze ist durch die Fachkraft für Arbeitssicherheit durchzuführen. Anwender oder Personalrat haben die Möglichkeit, anlassbezogen um eine Überprüfung zu bitten.

3.4 Bei Störfällen an IT-Geräten und Software ist der User-Help-Desk von Dataport (UHD) durch den betroffenen Anwender zu kontaktieren.

3.5 Auf dienstlich zur Verfügung gestellten Endgeräten darf grundsätzlich nur dienstlich beschaffte Software installiert und genutzt werden. Ausnahmen müssen vom zuständigen IT-Verantwortlichen (RS-IT) genehmigt und revisionssicher dokumentiert werden (s. Endgeräte-RL, Teil B, Ziffer 7).

3.6 Die Nutzung von privaten IT-Geräten für dienstliche Zwecke, insbesondere die Verarbeitung dienstlicher Daten, ist grundsätzlich unzulässig mit Ausnahme von ZUVEX und dSmartdesk, welche einen gesicherten Zugriff auf interne Anwendungen aus dem Internet heraus ermöglichen. Der Zugriff erfolgt nur auf freigegebene Anwendungen und nicht auf das gesamte FHH Netz.

3.7 Die private Nutzung dienstlicher IT-Geräte ist bis auf generell geregelte Ausnahmen in anderen Vorschriften und Vereinbarungen grundsätzlich untersagt.

4 Allgemeine Sicherheitsmaßnahmen

4.1 Bei der Verarbeitung personenbezogener Daten sind die entsprechenden Bestimmungen des Hamburgischen Datenschutzgesetzes sowie ggf. fachbezogene Rechtsnormen zu beachten.

4.2 Bei Verlust oder Diebstahl von IT-Geräten ist unverzüglich RS-IT zu informieren.

4.3 Der Anwender hat durch geeignete Maßnahmen jederzeit sicher zu stellen, dass unbefugten Personen keine Einsicht in dienstliche Daten ermöglicht wird. Das Dienstzimmer ist auch dann abzuschließen, wenn der Arbeitsplatz nur kurze Zeit verlassen wird. Vor Verlassen des Arbeitsplatzes muss der Rechner durch Drücken der Windowstaste + L-Taste gesperrt werden, weil bei Nutzungsunterbrechung erst nach 15 Minuten der automatische Bildschirmschutz aktiviert wird. Eine Veränderung dieser Standardeinstellung des Bildschirmschutzes durch Anwender ist nicht möglich.

4.4 Arbeitsplatzrechner, Notebooks und Pentops sind nach letztmaligem Gebrauch täglich vollständig herunter zu fahren. Nur dadurch wird gewährleistet, dass Softwareupdates beim erforderlichen Neustart des Rechners wirksam werden. Außerdem wird durch das Herunterfahren des Rechners der Energieverbrauch gesenkt.

4.5 Die geltenden Vorschriften der Passwort-Richtlinie (Passwort-RL) sind zur Gewährleistung der Zugangssicherheit für die IT-Geräte und den auf ihnen befindlichen Daten einzuhalten. Die Weitergabe von persönlichen Passwörtern an Arbeitskollegen oder andere Personen ist untersagt.

4.6 Die Nutzung des Passwort-SelfService ist für alle Anwender verbindlich.

4.7 Die Übermittlung von Daten auf elektronischem Wege an Dritte außerhalb des FHH-Netzes, wie zum Beispiel an Private, ist nur im Rahmen der dienstlichen

Aufgaben zulässig. Die Übermittlungen sind zu dokumentieren. Bei Übermittlung von sensiblen personenbezogenen Daten sind diese zu verschlüsseln.

4.8 An vernetzten Standorten sollte die Kommunikation zwischen zwei oder mehreren IT-Geräten aus Sicherheitsgründen grundsätzlich nicht kabellos erfolgen. Ist kabellose Kommunikation für dienstliche Zwecke unumgänglich, sind die einschlägigen Vorschriften hierzu zu beachten.

5 Zusätzliche Sicherheitsmaßnahmen für mobile IT

5.1 Die Nutzer mobiler Endgeräte sind verantwortlich für die Einhaltung des Datenschutzes.

5.2 Die Anwender sind zu erhöhter Aufmerksamkeit im Umgang mit mobilen Endgeräten verpflichtet. Insbesondere dürfen die Geräte während des Transports nicht unbeaufsichtigt gelassen werden und sind effektiv gegen den Zugriff Unbefugter zu sichern. Kleingeräte wie USB-Sticks, Tablets und Smartphones sind stets in abschließbaren Behältnissen (verschließbarer Büroschrank, Aktenkoffer) aufzubewahren oder direkt am Körper (Jackentasche o.ä.) zu tragen. Die Aufbewahrung von mobilen Endgeräten in Fahrzeugen ist nicht gestattet.

5.3 Dienstlich genutzte mobile Endgeräte dürfen unbefugten Personen nicht zum Gebrauch überlassen werden.

5.4 Um einen vergleichbaren Schutz zu gewährleisten, gilt die Passwort-Richtlinie auch für mobile Endgeräte. Soweit möglich, sind komplexe Passworte mit mindestens 8 Zeichen zu nutzen, auch wenn die Technik dies nicht zwingend vorgibt. Wenn die Eingabe kürzerer Passworte technisch vorgegeben ist, sind dennoch die anderen Vorgaben der Passwortrichtlinie einzuhalten.

5.5 Grundsätzlich sind Smartphones und Tablets durch den Anwender mit einem Virenscanner auszustatten. Die ständige Aktualisierung der Virenscanner ist sicher zu stellen. Notebooks und Pentops sind vom Anwender grundsätzlich mindestens einmal wöchentlich für einen ausreichenden Zeitraum an das FHH-Netz anzuschließen.

5.6 Auf USB-Sticks dürfen grundsätzlich keine sensiblen personenbezogenen Daten gespeichert werden. Nur das von der IT-Dienststelle bereit gestellte Zubehör darf an den dienstlichen Endgeräten genutzt werden. Privates IT-Zubehör kann bei Vorliegen dienstlicher Interessen an die IT der FHH angeschlossen werden (Endgeräte-RL Teil A, Ziffer 5).

5.7 Nicht mehr benötigte oder defekte dienstliche externe Speichermedien (z.B. USB-Sticks und externe Festplatten) dürfen durch die Anwender nicht selbst entsorgt werden. Sie sind RS-IT zur weiteren Verwendung bzw. sicheren Entsorgung zu übergeben.

5.8 Dienstliche und private Smartphones und Tablets dürfen zu dienstlichen Zwecken nur in Verbindung mit dSmartDesk oder Zuvex verwendet werden. Diese Lösungen ermöglichen die Anbindung mobiler Endgeräte und die Synchronisation von Daten innerhalb eines abgesicherten Containers. Die Kenntnisnahme der Benutzerhinweise, dSmartDesk oder Zuvex ist gegenüber RS-IT zu quittieren. Die Nutzung weiterer spezieller Applikationen (sog. Apps) wird von der Finanzbehörde vorgegeben und ist verbindlich.

5.9 Apps können auf dienstlichen Endgeräten installiert werden, wenn sichergestellt ist, dass diese nicht auf schutzwürdige Daten, die im Wege der Synchronisation auf das mobile Endgerät gelangt sind, zugreifen oder zugreifen können und dienstliche Belange des Einzelnen oder der FHH nicht entgegenstehen. Bevor eine App (mit Ausnahme von W-10 Apps) installiert wird, sind von den Beschäftigten die Berechtigungen zu prüfen, die die App erhalten soll (vgl. Endgeräte-RL, Teil B, Ziffer 8, Stand 10/2017).

6 Nutzung von Software

6.1 Nutzung von Software allgemein

Die Installation von Software durch Anwender ist untersagt. Es darf nur Software genutzt werden, die Bestandteil des Softwarewarenkorbes der Bezirksverwaltung ist. Die Aufnahme neuer Software in den Warenkorb erfolgt ausschließlich durch das ITAB (IT-Architekturboard) der FHH oder N/ITB.

6.2 Nutzung von Microsoft Access

Mit Microsoft Access können Anwendungen und Datensammlungen entwickelt werden, deren Pflege, Rechtmäßigkeit, Wirtschaftlichkeit und Betrieb durch die IT der Bezirksverwaltung nicht sicher zu stellen sind. Um Anwendern dennoch die Nutzung von Access zu ermöglichen, sind zur Sicherstellung der technischen und rechtlichen Bedingungen zum Softwarebetrieb der FHH nachstehende Nutzungsbedingungen einzuhalten:

- Access darf von Mitarbeitern der Bezirksverwaltung nicht zur Programmierung von IT-Verfahren für mehrere Anwender genutzt werden. Es ist lediglich ein Werkzeug zur Gestaltung von eigenen individuellen Arbeitsprozessen.

- Die Verantwortung für die Wirtschaftlichkeit und Rechtmäßigkeit der Speicherung und Verarbeitung von Daten liegt beim Anwender. Es ist untersagt, sensible personenbezogene Daten in Access zu speichern.

- Bei Access-Dateien finden keine Tests auf Kompatibilität zum aktuellen BASIS-PC statt, und die Funktionsfähigkeit wird durch Dataport und die IT der Bezirksverwaltung nicht gewährleistet.

- Erforderliche Anpassungen an die Softwareumgebung seines BASIS-PC sind durch den Anwender selbst vorzunehmen.

- Fragen zum Umgang mit Access sind an den UHD zu stellen. Fragen zur Programmierung sind vertraglich ausgenommen.

Von diesen Regelungen ausgenommen sind die auf Microsoft Access basierenden Fachanwendungen des Softwarewarenkorbes der Bezirksverwaltung.

7 Internetzugang

7.1 Der Zugang der Anwender zum Internet wird in der Bezirksverwaltung regelhaft als freier Internetzugang realisiert. Wenn auf einem IT-Gerät jedoch ein IT-Verfahren installiert ist, das sensible personenbezogene Daten verarbeitet, wird der freie Internetzugang aus Datenschutzgründen durch einen Zugang über Windows Terminal Server (WTS) ersetzt. Unter diese sensiblen Daten fallen insbesondere

- Daten, die einem Berufs- oder Amtsgeheimnis unterliegen, wie etwa dem Steuergeheimnis
- Sozialdaten
- Personenbezogene Daten, aus denen ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit oder ähnliches hervorgehen
- Daten über Gesundheit oder Sexualleben

Zusätzlich werden für alle Nutzer des Internetzuganges über WTS einzelne dienstlich erforderliche Internetadressen (URLs) in einer gesonderten Liste (White-List) erfasst und ohne die Einschränkungen der WTS-Lösung zur Verfügung gestellt. Der Prozess zur Erweiterung der White-List ist auf dem Sharepoint von N/ITB hinterlegt.

8 Revisionssichere Ablage

8.1 Daten über abgeschlossene aktenwürdige Vorgänge sind in ELDORADO abzulegen. Die dauerhafte und ausschließliche Speicherung von dienstlichen Daten auf der Festplatte (Laufwerk C oder D) des Arbeitsplatzrechners, auf den Netzlaufwerken G, H und J oder in Outlook ist unzulässig. Die Laufwerke C und D werden durch Dataport nicht gesichert. Das Laufwerk H sowie Outlook werden zwar gesichert, sind aber für andere Mitarbeiter nicht zugänglich.

9 Schlussbestimmungen

9.1 Die Dienstanweisung wird regelmäßig, mindestens aber alle zwei Jahre, durch N/ITB und RS-IT auf notwendige Aktualisierungen überprüft. Eventuell beabsichtigte Änderungen der Dienstanweisung durch ein Bezirksamt sind mit den anderen Bezirksämtern vorab zu erörtern.

9.2 Diese Dienstanweisung ist einmal jährlich durch die Fachbereiche als Umlauf oder per HIM-Workflow allen Mitarbeitern des Bezirksamtes bekannt zu machen. Der Umlauf ist von jedem Mitarbeiter zur Kenntnis zu nehmen und zu quittieren. Die Erstinformation neuer Mitarbeiter erfolgt anlassbezogen durch den jeweiligen Vorgesetzten. Dokumentation und Archivierung des jährlichen

Umlaufs obliegen den Fachbereichen. RS-IT ist jederzeit Einsichtnahme zu gestatten.

9.3 Bei Verstößen gegen die Dienstanweisung kann das Bezirksamt arbeits-, dienst- und disziplinarrechtliche Konsequenzen veranlassen.

10 Vorschriftenverzeichnis und Vertragsvereinbarungen

10.1 Im Zusammenhang mit der Dienstanweisung sind insbesondere die von der Finanzbehörde der Freien und Hansestadt Hamburg herausgegebenen und im FHH Portal veröffentlichten IT-Vorschriften in ihrer jeweils gültigen Fassung zu beachten:

- Richtlinie über die Sicherheit der Datenverarbeitung auf Arbeitsplatzrechnern und sonstigen Endgeräten (Endgeräterichtlinie)
- Informationssicherheitsleitlinie (IS-LL)
- Rahmensicherheitskonzept (RaSiKo)
- Hamburgisches Datenschutzgesetz (HmbDSG) mit Durchführungsbestimmungen, Zuständigkeitsanordnung und Hinweisen
- Richtlinie zur Datensicherheit im IuK-Bereich (DS-Richtlinie)
- Freigaberichtlinie (Freigabe-RL)
- Passwort-Richtlinie (Passwort-RL)
- Hamburgisches Personalvertretungsgesetz (HmbPersVG)
- Bildschirmarbeitsverordnung i.V.m. dem Arbeitsschutzgesetz und Arbeitsschutz-Richtlinien

10.2 Außerdem gelten insbesondere folgende Vereinbarungen :

- Vereinbarung nach §94 HmbPersVG für die Bürokommunikation
- Service Level Agreements über Betriebs- und Supportleistungen
- Vorgaben zum Windows-Client-Betrieb in der FHH
- Hilfe zum Passwort-Selfservice
- Benutzerhinweise Excitor DME/ Zuvex

11 Inkrafttreten

Diese Dienstanweisung tritt mit sofortiger Wirkung in Kraft.

Hamburg, den

Bezirksamtsleiterin
Bezirksamt Harburg

Protokoll für Dienstanweisung Nr. 4/1-16,2 für den Einsatz und die Nutzung von stationärer und mobiler IT im BA Harburg

BAH4707