

Dienstanweisung

**für Einsatz und Nutzung von stationärer und mobiler IT
im Bezirksamt Hamburg-Nord**

(DA-Bez-IT)

**vom 01.11.2008
in der Fassung vom 01.10.2015**

Einleitung.....	2
1. Begriffsdefinition	2
2. Organisation, Rollen, Verantwortlichkeiten.....	2
3. Mitbestimmung	3
4. Beschaffung und Nutzung von IT-Geräten	3
5. Allgemeine Sicherheitsmaßnahmen	4
6. Zusätzliche Sicherheitsmaßnahmen für mobile IT.....	5
7. Nicht vernetzte Arbeitsplatzrechner.....	6
8. Nutzung von Software	6
9. Internetzugang	7
10. Revisionssicherung	7
11. Schlussbestimmungen.....	8
12. Vorschriftenverzeichnis und Vertragsvereinbarungen.....	8
13. Inkrafttreten	9

Einleitung

Diese Dienstanweisung gilt für alle Fachbereiche des Bezirksamtes. Sie legt 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 fest.

Ziel dieser Dienstanweisung ist der bestimmungsgemäße Einsatz von und der Umgang mit der genutzten Informationstechnologie. Insbesondere stehen hierbei Sicherheitsbedürfnisse, datenschutzrechtliche Erfordernisse, die Einhaltung von getroffenen Rahmenvertragsvereinbarungen sowie die gesetzliche und arbeitsrechtliche Absicherung der Mitarbeiterinnen und Mitarbeiter im Vordergrund. Aus Gründen der besseren Lesbarkeit wird im Folgenden bei Personen ausschließlich die männliche Form verwendet. Für die Anwender werden die wichtigsten zu beachtenden Regelungen in dieser Dienstanweisung aufgeführt.

1. Begriffsdefinition

1.1 Als stationäre IT werden Arbeitsplatzrechner (Desktop oder Tower) sowie Peripheriegeräte wie Monitor, Drucker, Scanner und Multifunktionsgeräte bezeichnet.

1.2 Als mobile IT werden unter anderem folgende Geräte bezeichnet:

- Notebook
- Pentop
- Smartphone
- Tablet
- Externes Speichermedium (z.B. USB-Stick)

1.3 Die unter 1.1 und 1.2 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 Bezirksamtern zuständige Dienststelle ist die Zentralstelle für IT-Angelegenheiten der Bezirksverwaltung. N/ITB ist unter anderem Auftraggeber gegenüber Dataport für die Softwareprodukte und regelt übergreifende Betriebsaufgaben.

2.3 RS22

Die für IT-Angelegenheiten im Bezirksamt zuständige Organisationseinheit im Dezernat für Steuerung und Service wird im folgenden RS22 genannt. Sie 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. Jeder Anwender ist zum verantwortungsbewussten und pfleglichen Umgang mit den überlassenen Geräten, den Verfahren und den genutzten Daten entsprechend datenschutzrechtlicher Anforderungen verpflichtet. Die einschlägigen Regelungen sind zu beachten.

2.5 Dataport

Dataport ist der zentrale IT-Dienstleister der Freien und Hansestadt Hamburg. Die Bezirksverwaltung als Auftraggeber lässt grundsätzlich ihre eingesetzte Hard- und Software durch Dataport auf der Grundlage bestehender Vereinbarungen betreiben. Die Leistungen von Dataport sind in „Service Level Agreements“ (SLA) sowie weiteren Vereinbarungen festgelegt.

3 Mitbestimmung

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

3.2 Erforderliche Mitbestimmungsverfahren werden regelhaft durch RS22 initiiert und durchgeführt.

4 Beschaffung und Nutzung von IT-Geräten und Software

4.1 IT-Geräte und Software dürfen ausschließlich durch oder mit Zustimmung von RS22 und N/ITB beschafft werden.

4.2 Alle mit der Nutzung von IT-Geräten zusammenhängenden Tätigkeiten, wie z.B. Inbetriebnahme, Administration, Umzug, Reparatur, Öffnung, Veränderung, erfolgt ausschließlich durch Dataport oder von Dataport beauftragte Subunternehmen. In Ausnahmefällen kann die Administration von IT-Geräten auch durch Mitarbeiter von RS22 erfolgen.

4.3 RS22 veranlasst die Überprüfung der Einhaltung der einschlägigen Bestimmungen in den Bereichen Arbeitsschutz und Ergonomie im Zuge der Erstausrüstung von Arbeitsplätzen mit IT-Technik. Eine regelmäßige Überprüfung der Arbeitsplätze ist durch den jeweiligen Fachbereich durchzuführen. Anwender oder Personalrat haben die Möglichkeit, den Fachbereich anlassbezogen um eine Überprüfung zu bitten. Die

Prüfungsergebnisse greifen Anwender, Fachbereich und RS22 auf, um festgestellten Gefährdungen kurzfristig wirksam zu begegnen.

- 4.4 Bei Störfällen an IT- Geräten und Software ist der User-Help-Desk von Dataport (UHD) durch den betroffenen Anwender zu kontaktieren.
- 4.5 Die Installation und Nutzung von privater Software auf dienstlichen IT-Geräten ist untersagt. Das gilt auch für Software, die ohne Installation über USB-Stick gestartet und betrieben werden kann.
- 4.6 Die Nutzung von privaten stationären IT-Geräten und Notebooks für dienstliche Zwecke, insbesondere die Verarbeitung dienstlicher Daten, ist grundsätzlich unzulässig (Ausnahme: Zuvex). Zuvex ermöglicht einen gesicherten Zugriff auf interne Anwendungen aus dem Internet heraus. Der Zugriff erfolgt nur auf freigegebene Anwendungen und nicht auf das gesamte FHH Netz.
- 4.7 Die private Nutzung dienstlicher stationärer IT-Geräte und Notebooks ist bis auf generell geregelte Ausnahmen in anderen Vorschriften und Vereinbarungen ebenfalls grundsätzlich untersagt.

5 Allgemeine Sicherheitsmaßnahmen

- 5.1 Bei der Verarbeitung personenbezogener Daten sind die entsprechenden Bestimmungen des HmbDSG zu berücksichtigen.
- 5.2 Bei Verlust oder Diebstahl von IT-Geräten ist unverzüglich RS22 zu informieren.
- 5.3 Durch den Anwender ist sicher zu stellen, dass unbefugten Personen keine Einsicht in dienstliche Daten ermöglicht wird. Bei Verlassen des Raumes hat der Anwender den verlassenen Dienstraum zu verschließen und/oder aus Sicherheitsgründen seinen Arbeitsplatzrechner zu sperren, denn bei Nutzungsunterbrechung des Arbeitsplatzrechners wird erst nach 15 Minuten der automatische Bildschirmschutz aktiviert. Eine Veränderung dieser Standardeinstellung des Bildschirmschutzes durch Anwender ist nicht möglich.
- 5.4 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.
- 5.5 Die geltenden Vorschriften der Passwort-Richtlinie (Passwort-RL) sind zur Gewährleistung der Zugangssicherheit für die IT-Geräte und den auf ihnen befindlichen Daten zu beachten. Insbesondere die Weitergabe von persönlichen Passwörtern an Arbeitskollegen oder andere Personen ist untersagt.
- 5.6 Bei vergessenem Anmeldepasswort ist die Nutzung des Passwort-SelfService für alle Anwender verbindlich.
- 5.7 Die Übermittlung von Daten auf elektronischem Wege an Dritte außerhalb des FHH-Netzes ist nur im Rahmen der dienstlichen Aufgaben zulässig. Die

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

5.8 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.

5.9 Freie USB-Schnittstellen von Daten verarbeitenden oder speichernden IT-Geräten sind grundsätzlich durch eine geeignete Software zu sperren, sobald ein Standard für die FHH festgelegt ist. Werden auf einem IT-Gerät keine sensiblen personenbezogenen Daten verarbeitet, können aus dienstlich erforderlichen Gründen USB-Schnittstellen freigeschaltet werden. Die Prüfung und Entscheidung über die Freischaltung erfolgt durch RS22. Die Verwendung der offenen USB-Schnittstellen bleibt ausschließlich dienstlichen Zwecken vorbehalten. Der Anschluss privater Geräte ist grundsätzlich nicht zulässig.

6 Zusätzliche Sicherheitsmaßnahmen für mobile IT

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

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

6.3 Dienstlich genutzte mobile IT-Geräte dürfen unbefugten Personen nicht zum Gebrauch überlassen werden.

6.4 Um einen vergleichbaren Schutz zu gewährleisten, gilt die Passwort-Richtlinie auch für mobile IT-Geräte. 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.

6.5 Grundsätzlich sind mobile IT-Geräte durch die zuständige Administration mit einem Virens Scanner auszustatten. Die ständige Aktualisierung der Virens Scanner ist sicher zu stellen. Hierzu sollen Notebooks und Pentops grundsätzlich mindestens einmal wöchentlich für einen ausreichenden Zeitraum an das FHH-Net angeschlossen werden.

6.6 Grundsätzlich sollen auf USB-Sticks keine sensiblen personenbezogenen Daten gespeichert werden. Ist dies aus dienstlichen Gründen erforderlich, sind die Daten zu verschlüsseln.

- 6.7 Nicht mehr benötigte oder defekte dienstliche externe Speichermedien (z.B. USB-Sticks) dürfen durch die Anwender nicht selbst entsorgt werden. Sie sind RS22 zur weiteren Verwendung bzw. sicheren Entsorgung zu übergeben.
- 6.8 Dienstliche und private Smartphones und Tablets dürfen zu dienstlichen Zwecken nur in Verbindung mit der Applikation Excitor DME (Dynamic Mobile Exchange) oder Zuvex verwendet werden. Diese Lösungen ermöglichen die Anbindung mobiler Endgeräte und die Synchronisation von Unternehmensdaten innerhalb eines abgesicherten Containers. Die Kenntnisnahme der Benutzerhinweise Excitor DME oder Zuvex ist gegenüber RS22 zu quittieren.

7 Nicht vernetzte Arbeitsplatzrechner

- 7.1 Grundsätzlich sollen alle Arbeitsplatzrechner an das FHH-Net angeschlossen werden.
- 7.2 Die Administration dienstlich genutzter Arbeitsplatzrechner außerhalb des FHH-Net wird durch RS22 geregelt.
- 7.3 Die Schutzmechanismen zur Sicherung der auf den IT-Geräten enthaltenen Daten gelten grundsätzlich auch für nicht vernetzte Arbeitsplatzrechner, wenn auf ihnen sensible personenbezogene Daten verarbeitet werden.
- 7.4 Die Datensicherung auf nicht vernetzten IT-Arbeitsplätzen ist regelmäßig von den dafür durch RS22 benannten und eingewiesenen Anwendern vorzunehmen. Dies geschieht durch Speicherung auf einer externen Festplatte, Sicherungskopien auf CD-ROM/DVD oder in anderer geeigneter Form (Backups). Die Backups sind sicher zu verwahren.
- 7.5 Bei Verarbeitung sensibler personenbezogener Daten wird durch RS22 veranlasst, dass eine Festplattenverschlüsselung installiert wird. Die regelmäßig vorzunehmenden Backups sind ebenfalls zu verschlüsseln. RS22 veranlasst außerdem die Aktualisierung von Virensignaturen sowie das Aufspielen von aktuellen Updates und Patches.

8 Nutzung von Software

8.1 Nutzung von Software allgemein

Die Installation von Software durch Anwender ist grundsätzlich untersagt (Ausnahme: Rechner der Modelllinie 2). Es darf nur Software genutzt werden, die entweder Bestandteil des Softwarewarenkorb der Bezirksverwaltung ist oder durch RS22 installiert wird (Modelllinie 1G). Die Aufnahme neuer Software in den Warenkorb erfolgt ausschließlich durch das ITAB (IT-Architekturboard) der FHH oder die Warenkorbverantwortlichen bei N/ITB.

8.2 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 individuellen Arbeitsprozessen für sich selbst.
- 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 Softwarewarenkorb der Bezirksverwaltung.

9 Internetzugang

9.1 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 Internetzuges 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.

10 Revisionssicherung

10.1 Daten über abgeschlossene Vorgänge sind in ELDORADO abzulegen. Bis zur flächendeckenden Einführung von ELDORADO werden abgeschlossene Vorgänge wieder auffindbar und nachvollziehbar auf Gruppenlaufwerken

abgelegt. Die dauerhafte und ausschließliche Speicherung von dienstlichen Daten auf der Festplatte (Laufwerk C oder D) des Arbeitsplatzrechners, auf dem Laufwerk H 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.

10.2 N/ITB legt Revisionsunterlagen für die IT-Verfahren an. Art und Umfang werden durch gesonderte Regelungen zu den IT-Verfahren festgelegt.

10.3 Bei IT-Anwendungen wie Textverarbeitung, Tabellenkalkulation und Datenbank-anwendungen sollen Log- und Wartungsprotokolle, Zugriffsberechtigungen der Anwender, Zuordnung der Anwender zu Anwendergruppen sowie Programm-dokumentationen in den Revisionsunterlagen enthalten sein, sofern die Sensibilität der verarbeiteten Daten dies erforderlich macht.

11 Schlussbestimmungen

11.1 Die Dienstanweisung wird regelmäßig, mindestens aber alle zwei Jahre, durch N/ITB und RS22 auf notwendige Aktualisierungen überprüft. Eventuell beabsichtigte Änderungen der Dienstanweisung durch ein Bezirksamt sind mit den anderen Bezirksamtern vorab zu erörtern.

11.2 Diese Dienstanweisung ist einmal jährlich als Umlauf allen Mitarbeitern des Bezirksamtes vorzulegen. 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. RS22 ist jederzeit Einsichtnahme zu gestatten.

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

12 Vorschriftenverzeichnis und Vertragsvereinbarungen

12.1 Im Zusammenhang mit der Dienstanweisung sind insbesondere die folgenden Rechts- und Verwaltungsvorschriften zu beachten:

- Richtlinie über die Sicherheit der Datenverarbeitung auf Arbeitsplatzrechnern und sonstigen Endgeräten (PC-Richtlinie)
- Informationssicherheitsleitlinie (IS-LL)
- Rahmensicherheitskonzept (RaSiKo)
- Hamburgisches Datenschutzgesetz (HmbDSG) mit Durchführungsbestimmungen, Zuständigkeitsanordnung und Hinweisen
- Datenschutzbestimmungen sonstiger Gesetze und Verordnungen
- 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

12.2 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

13 Inkrafttreten

13.1 Die Dienstanweisung tritt nach Bekanntmachung mit sofortiger Wirkung in Kraft.

Hamburg, den

01.12.2015

Bezirksamtsleiter