Richtlinie zur Nutzung von IT-Arbeitsmitteln in der DEVK

letzte Änderung: 5. Dezember 2017
Ersterstellung: 12. Februar 2015
Version: 3.0

Inhaltsverzeichnis

1 Einleitung 2
1.1 Beteiligte an diesem Dokument 3
2 Geltungsbereich 3
3 Umgang mit IT-Arbeitsmitteln 3
4 Lokale Daten 5
5 Nutzung von Internet und E-Mail 5
6 Übergabe und Rückgabe von IT-Arbeitsmitteln 5
7 Technische Sicherheitsmaßnahmen 5
7.1 Passwörter 5
7.2 Schutz des IT-Systems bei kurzzeitigem Verlassen (Bildschirmschoner) 5
7.3 Schutz vor Schadprogrammen (Computerviren) 6
7.4 Verbindung zwischen dem IT-System der DEVK und dem Internet 6
8 Sicherheitsvorfälle 7
9 Datenschutz 7
10 Aufgeräumter Arbeitsplatz (Der „Clear Desk“ Grundsatz) 7
11 Glossar 8
11.1 Vertrauliche Daten 8

Änderungshistorie

Version	Bear-beitungs-datum	Bearbeiter	Status / Art der Änderung
3.0	2016-05-24	Guido Tesch (hv14872)	Aktualisierung der Version 2.1 vom 21.2.2013 im Zusammenhang mit Veröffentlichung der Richtlinie zur Nutzung von Internet und E-Mail

1 Einleitung

Die "Richtlinie zur Nutzung von IT-Arbeitsmitteln in der DEVK" regelt den Umgang mit den IT-Arbeitsmitteln, die Sie im Rahmen der Erfüllung Ihrer Aufgaben einsetzen. Ziel ist es, durch einen sachgerechten Umgang mit den dienstlichen IT-Arbeitsmitteln die Sicherheit der Informationsverarbeitung zu erhöhen und dadurch materielle und immaterielle Schäden für die DEVK zu vermeiden.

Die Richtlinie ist zu beachten vorbehaltlich anderweitiger arbeitsrechtlich festgelegter Regelungen.

Die jeweils gültige Fassung des vorliegenden Dokuments finden Sie im DEVK-Intranet.

1.1 Beteiligte an diesem Dokument

Veröffentlich durch:	Hauptabteilung IA
Autoren:	• Achim Zekoll (hv11400), Fachgebietsmanager IT-Security, HA XI • Dr. Holger Taday (hv035), Datenschutzbeauftragter • Stefan Rohr (hv14840), Abt. Anforderungsmgmt., HA XIV
Zielgruppe:	• DEVK-Mitarbeiter, die im Rahmen ihrer dienstlichen Aufgaben IT-Arbeitsmittel der DEVK nutzen

2 Geltungsbereich

Diese Richtlinie gilt verbindlich für alle

- im Innendienst tätigen Mitarbeiter der DEVK, egal ob sie in den Räumlichkeiten der DEVK arbeiten oder außerhalb (z.B. am Telearbeitsplatz) und egal, ob sie einen Innendienst- oder Außendienstvertrag haben und
- sonstige von der DEVK beauftragte Personen (externe Mitarbeiter)

bei der Nutzung der für Arbeitszwecke eingesetzten IT-Arbeitsmittel.

Als „ IT-Arbeitsmittel“ gelten alle stationären und mobilen Computer (Thin Clients, Notebooks, Tablet-PCs, etc.), die Computer-Peripherie (externe Festplatten, Memorysticks, Speicherkarten, Scanner, Drucker etc.), das firmeninterne Netzwerk, Geräte zur Telekommunikation (z. B. Smartphones), Software und Datenbestände.

Diese Richtlinie kann ergänzt werden durch weitere Richtlinien, die die Nutzung spezieller Arbeitsmittel detaillierter regeln.

Die Regeln für die nicht im Innendienst tätigen Außendienstmitarbeiter werden in einer gesonderten Richtlinie geregelt.

3 Umgang mit IT-Arbeitsmitteln

Die IT-Arbeitsmittel werden Ihnen von der DEVK zur Verfügung gestellt und dürfen nur zur Erfüllung der Arbeitsaufgaben im Rahmen der Unternehmenszwecke genutzt werden. Grundsätzlich gilt, dass Sie im Rahmen der üblichen Sorgfalt mit dafür Sorge tragen, dass die IT-Arbeitsmittel vor Zerstörung, Verfälschung, Missbrauch, unbefugtem Zugriff und Diebstahl geschützt sind.

Die Konfiguration der IT-Arbeitsmittel ist auf die jeweilige Arbeitsaufgabe und die IT-Sicherheitsanforderungen der DEVK abgestimmt. Es ist nicht gestattet, hinsichtlich Sicherheitseinstellungen die Konfiguration von Hard- oder Software zu ändern. Firmenfremde Hardware darf nicht direkt an das Netzwerk der DEVK angeschlossen

werden. (Eine Verbindung via VPN über das Internet ist hiermit nicht gemeint. Ebenso ist nicht das Anschließen an das DSL-Netz in den Räumlichkeiten der DEVK gemeint.)

Außerdem sind bei der Nutzung von Hard- und Software folgende Regelungen einzuhalten:

- Es darf nur von der IT zentral zur Verfügung gestellte oder von der IT genehmigte Software genutzt werden. Dies betrifft auch funktionale Erweiterungen von bereits genehmigter Software, zum Beispiel Browser-Plugins.
- Daten dürfen nur im fachlich notwendigen Umfang und nur mit den vom verantwortlichen Fachbereich autorisierten Programmen und Verfahren verarbeitet werden.
- Stationäre Arbeitsplatzsysteme dürfen nur vom UserHelpDesk (Zentraler UHD, dezentraler UHD inkl. der Kommunikationsbeauftragten der RDen) und von dafür ausdrücklich autorisierten Stellen aufgestellt, angeschlossen, abgebaut oder umgezogen werden.
- Bei mobilen IT-Arbeitsmitteln (z.B. Notebooks, USB-Sticks, externe Festplatten, RSA-Token) muss der Benutzer zu jeder Zeit wissen, wo sich das Gerät befindet und er muss den Zugriff durch Unbefugte aktiv verhindern, z.B. durch Beaufsichtigung, Anschließen mittels Kabelschloss oder Wegschließen.
- Externe Datenträger (z. B. CD/DVD, externe Festplatte, USB-Sticks) sollten nur in begründeten Ausnahmefällen genutzt werden. Ihre Nutzung ist im Wesentlichen beschränkt auf die Datensicherung für mobile Computer und den zweckgebundenen Datenaustausch. Die Datenträger sind geeignet aufzubewahren und zu transportieren, um sie vor unbefugtem Zugriff zu schützen.
- Zur fachgerechten Entsorgung von vertraulichen Daten (Definition siehe Glossar) auf externen Datenträgern gilt folgende Vorgehensweise:
  - Nur einmal beschreibbare Datenträger (z. B. DVD-ROMs, CD-ROMs) sind zur Entsorgung in die dafür vorgesehenen Entsorgungsbehälter zu werfen.
  - Externe Datenträger, die mehrfach verwendet werden können (z. B. USB-Sticks, externe Festplatten) und nicht mehr benötigt werden sind an die Gruppe IT-Arbeitsplatzservice zu geben. Dort erfolgt eine sichere Löschung aller Daten auf dem Datenträger.
- Auf Notebooks können wichtige Aktualisierungen zur Schließung von Sicherheitslücken nur erfolgen, wenn das Netzwerkkabel vor der Anmeldung am Notebook angeschlossen wird.

  Notebooks sind daher möglichst mindestens einmal pro Woche in den Räumlichkeiten der DEVK an das interne Datennetz anzuschließen und eine Anmeldung am Notebook durchzuführen.

  Wurde ein Notebook längere Zeit nicht genutzt (z. B. ein selten genutztes Abteilungsnotebook), dann ist für die erneute Anmeldung das Netzwerkkabel anzuschließen.
- Außerhalb der Dienstzeiten soll der Energieverbrauch der IT-Systeme minimiert werden. Hierzu sind die IT-Systeme abzuschalten oder in einen Energiesparmodus (Standby) zu versetzen.

4 Lokale Daten

Unternehmenskritische Daten müssen auf den zentralen Servern gespeichert werden.

Lokal gespeicherte Daten (z. B. auf Notebook oder USB-Wechselmedien) werden nicht automatisch gesichert. Einzige Ausnahme ist das Benutzerverzeichnis (Laufwerk H) bei Innendienst-Notebooks, dieses wird bei Anmeldung am DEVK-Netzwerk mit den zentralen Servern synchronisiert.

5 Nutzung von Internet und E-Mail

Die „Sicherheitsrichtlinie zur Nutzung von Internet und E-Mail“ ist zu beachten.

6 Übergabe und Rückgabe von IT-Arbeitsmitteln

Jeder Besitzerwechsel eines IT-Arbeitsmittels muss nachvollziehbar dokumentiert werden, mindestens mit Angaben zum Übergabezeitpunkt und Gerätezustand.

Sollten ein IT-Arbeitsmittel nicht mehr benötigt werden, z.B. weil die Aufgaben des Benutzers sich geändert haben oder weil er das Unternehmen verlässt, so ist das IT-Arbeitsmittel umgehend an die IT zurückzugeben. Hierzu soll die IT-Hotline kontaktiert werden.

Falls auf dem IT-Arbeitsmittel lokale Daten gespeichert sind (z.B. bei Notebooks, Tablet-PCs, USB-Sticks oder externen Festplatten), sollten Sie diese Daten bei Bedarf auf ein Netzlaufwerk der DEVK kopieren und anschließend auf dem IT-Arbeitsmittel löschen.

7 Technische Sicherheitsmaßnahmen

7.1 Passwörter

Für den Schutz der Daten und Systeme der DEVK ist die Authentisierung durch Benutzerkennung und Passwort von wesentlicher Bedeutung.

Der vertrauliche Umgang mit Kennwörtern ist wichtig, damit der DEVK kein Schaden durch Missbrauch einer Kennung entsteht und damit Sie als Mitarbeiter davor geschützt werden, dass unautorisiert in Ihrem Namen Aktivitäten in den IT-Systemen erfolgen.

Passwörter dürfen daher nicht weitergegeben werden.

Bei der Wahl eines Passwortes ist zu berücksichtigen, dass keine trivialen Passwörter genutzt werden dürfen. Hilfestellung zur Bildung sicherer Passwörter geben die unter den Arbeitsrichtlinien der HA XI veröffentlichten „ Regelungen zur Gestaltung und Handhabung von IT-Passwörtern“.

7.2 Schutz des IT-Systems bei kurzzeitigem Verlassen (Bildschirmschoner)

Auf den Arbeitsplatzsystemen ist ein Bildschirmschoner installiert, der bei Aktivierung den Arbeitsplatz sperrt und nur mit dem Passwort des angemeldeten Benutzers wieder entsperrt werden kann. Der Bildschirmschoner schützt den Benutzer davor, dass das

IT-System bei Abwesenheit vom Arbeitsplatz unbefugt in seinem Namen missbraucht wird.

Vor Verlassen des Arbeitsplatzes ist der Bildschirmschoner vom Benutzer selbst zu aktivieren. Dies kann bei Windows-Systemen einfach z. B. durch Drücken der Tastenkombination „ Windowstaste + L“ erfolgen.

Den Arbeitsplatz bis zur automatischen Aktivierung des Bildschirmschoners ungeschützt zurückzulassen bietet keinen ausreichenden Schutz vor Missbrauch des Systems.

7.3 Schutz vor Schadprogrammen (Computerviren)

Ein Schadprogramm (oft auch „Computervirus“ genannt) ist ein schadenstiftendes Programm, das sich eventuell als nützliche Anwendung tarnt und bei Aktivierung im IT-System verbreitet. Das Schadprogramm kann Daten auf einem Computer oder im Netzwerk ändern, löschen oder den Computer blockieren.

Schadprogramme stellen daher eine starke Bedrohung für die DEVK dar.

Zum Schutz vor Schadprogrammen (Computerviren) sind auf allen DEVK-Systemen Virenscanner installiert. Der standardmäßig laufende Virenscanner darf keinesfalls deaktiviert werden.

Der Virenscanner alleine kann niemals einen 100%-igen Schutz vor Schadsoftware bieten. Die Sicherheit der Systeme hängt auch von der Wachsamkeit der Benutzer ab.

Eine besondere Gefährdung stellen Programme und Dokumente aus dem Internet oder E-Mails dar. Dies gilt insbesondere, da bei E-Mails aus dem Internet die Echtheit der Absender-Adresse nicht garantiert ist. Programme bzw. Dokumente, deren Herkunft fragwürdig erscheint, sollten nicht ausgeführt bzw. geöffnet werden.

In Zweifels- und Verdachtsfällen ist die IT-Hotline zu kontaktieren.

7.4 Verbindung zwischen dem IT-System der DEVK und dem Internet

Zum Schutz des Netzwerks der DEVK sind zwischen dem internen Netz und dem Internet zahlreiche Sicherheitsmaßnahmen wie Firewalls und zentraler Virenscanner installiert. Die Wirksamkeit dieser Maßnahmen ist entscheidend für den effektiven Schutz der Daten und IT-Systeme im internen Netz. Unkontrollierte Verbindungen zwischen dem DEVK-Netz und dem Internet stellen ein erhebliches Risiko für die DEVK dar. Die Einhaltung der folgenden Regelung ist daher von besonderer Bedeutung.

Bei einem an das interne DEVK-Netzwerk angeschlossenen IT-System darf der Nutzer niemals gleichzeitig eine Netzwerkverbindung zu einem anderen Datennetz oder dem Internet herstellen, weder über Modem, Mobilfunk, WLAN oder sonstigen Kommunikationsschnittstellen.

Ist ein IT-Arbeitsmittel nicht mit dem internen DEVK-Netzwerk verbunden (via Kabel in den Räumlichkeiten der DEVK), darf eine Verbindung mit dem Internet über die technisch verfügbaren Wege hergestellt werden. (Typischerweise WLAN oder Mobilfunk)

8 Sicherheitsvorfälle

Als Sicherheitsvorfall gelten alle Ereignisse, die die Vertraulichkeit, Verfügbarkeit oder Integrität unserer Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen derart beeinträchtigen, dass dadurch ein Schaden für die DEVK entstanden ist oder entstehen kann. Solche Ereignisse sind z. B.:

- der Verlust eines Notebooks oder eines Datenträgers
- auf einen Missbrauch hinweisende Veränderung von Daten / Programmen
- Verdacht auf ein Schadprogramm
- die plötzliche Verfügbarkeit von sonst nicht freigegebenen Diensten
- Kenntnis oder Verdacht eines unbefugten Zugriffs auf Daten
- Verdacht auf Missbrauch der eigenen oder einer fremden Benutzerkennung

Sicherheitsvorfälle sind sofort der IT-Hotline zu melden.

9 Datenschutz

Mit der Datenschutzerklärung hat sich jeder Mitarbeiter verpflichtet, das Datengeheimnis gemäß Bundesdatenschutzgesetz zu wahren und personenbezogene Daten nur entsprechend der datenschutzrechtlichen Vorschriften zu verwenden.

Jeder Mitarbeiter ist verpflichtet, die ihm anvertrauten personenbezogenen Daten nur im Rahmen seiner Aufgabenstellung zu nutzen und zu verarbeiten (speichern, verändern, übermitteln, sperren, löschen). Der Missbrauch und jede unbefugte Weitergabe dieser Daten ist unzulässig und kann strafbar sein.

Zur Klärung von Zweifelsfällen ist der Datenschutzbeauftragte der DEVK einzuschalten.

10 Aufgeräumter Arbeitsplatz (Der „Clear Desk“ Grundsatz)

Der „Clear Desk“ Grundsatz stellt Anforderungen an die Verwendung von IT-Arbeitsmitteln sowie Dokumenten und Objekten am Arbeitsplatz. Ziel ist vor allem, unbefugten Dritten einen Zugriff auf Daten und Geräte zu verwehren.

- IT-Arbeitsmittel, bei denen ein Zugriff durch unbefugte Dritte die Gefahr birgt, dass vertrauliche Daten den unbefugten Dritten bekannt werden, sind gegen Zugriff zu sichern.
  - Notebooks sind sicher zu transportieren und wenn stationär eingesetzt mittels Kabelschloss anzuschließen.
  - Tablet-PCs, externe Festplatten, Memorysticks, Speicherkarten und Smartphones sind sicher zu transportieren und sicher wegzuschließen.

  (Hinweis: Thin Clients müssen nicht abgeschlossen werden, da ein Thin Client selbst keinerlei vertrauliche Daten speichert.)
- Dokumente und Ausdrucke, die vertrauliche Daten enthalten, müssen über Nacht und bei längerer Abwesenheit des Mitarbeiters sicher weggeschlossen werden.

- Sofern vorhanden (z.B. am Telearbeitsplatz), sind Türen und Fenster des Arbeitsraums – insbesondere bei längerer Abwesenheit – sicher geschlossen zu halten. Es müssen angemessene Maßnahmen zum Einbruchschutz getroffen werden.
- Fehlausdrucke oder Abfall-Objekte, die vertrauliche Daten enthalten, müssen fachgerecht vernichtet werden. (d.h. nicht einfach in den normalen Papierkorb legen, in den Räumlichkeiten der DEVK sind spezielle Behälter zur Dokumentenvernichtung verfügbar.)

11 Glossar

11.1 Vertrauliche Daten

Vertrauliche Daten sind nur für einen beschränkten Empfängerkreis vorgesehen und dürfen anderen Personen oder Systemen nicht zugänglich werden.

Es gibt keine trennscharfe Definition, genau welche Daten vertraulich sind. Zur Orientierung werden hier Hinweise genannt.

Zum einen sind personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes in der Regel vertrauliche Daten. Beispiele sind: Vertragsdaten, Bankverbindung, Kfz-Kennzeichen, Gesundheitsdaten, Daten zu Gewerkschaftszugehörigkeit, Partei-Mitgliedschaft, Religionszugehörigkeit, evtl. auch Name oder Kontaktdaten (Adresse, E-Mail Adresse, Telefonnummer).

Zum anderen kann sich die Vertraulichkeit von Daten an dem Ausmaß der Schäden orientieren, die für das Unternehmen sowie für Betroffene entstehen können, wenn die Daten unbefugten Dritten bekannt und durch diese missbraucht werden. Beispiele sind: Login-Daten (Benutzername, Passwort), Betriebsgeheimnisse, Ausschreibungen.