Richtlinie für mobiles Arbeiten und Homeoffice

Stand: April 2019

Einleitung

Moderne Endgeräte (Smartphones, Tablets, Notebooks etc.) machen es möglich, dienstliche Aufgaben nicht nur in den Räumen und Gebäuden DESYs zu erledigen, sondern auch unterwegs (bspw. In der Bahn oder im Wartebereich auf dem Flughafen), auf Dienstreisen (Tagungen, Konferenzen, Aufenthalt in anderen Forschungseinrichtungen), oder von zuhause aus. Da bei einer mobilen Arbeitsumgebung nicht immer die Rahmenbedingungen (Vertraulichkeit, Arbeitsumgebung usw.) wie in den DESY-Büroräumen gegeben sind, gilt es einige Regelungen zu beachten, um beispielsweise den Anforderungen des Datenschutzes gerecht zu werden.

Diese Richtlinie informiert insofern über Risiken, die sich beim mobilen Arbeiten ergeben und gibt Handlungsempfehlungen, mit denen sich diese Risiken verringern lassen, lässt aber Aspekte der Arbeitsplatzergonomie und der allgemeinen Sicherheit außen vor.

Umgebung

Angemessene Arbeitsumgebung

Die Wahl einer geeigneten Arbeitsumgebung ist der erste wichtige Schritt. Sie sollte dem Arbeitsumfang und den Sicherheits- bzw. Vertraulichkeitsanforderungen angemessen gewählt werden. Das bloße Bearbeiten von E-Mails ist dabei anders zu bewerten als das Erstellen eines Zeugnisses, für das ggf. noch weitere Informationsquellen (Unterlagen) erforderlich sind.

Insbesondere bei der Bearbeitung vertraulicher Informationen ist abzuschätzen, ob diese dadurch Dritten bekannt werden und welchen Schaden dies haben kann. Dies gilt beispielsweise beim Telefonieren in der Öffentlichkeit, bei Gesprächen, etwa in der Bahn oder beim Arbeiten am Rechner in der Bahn oder im Flugzeug.

Das Mitlesen vertraulicher Informationen auf Bildschirmen durch Dritte kann beispielsweise durch das Anbringen von **Sichtschutzfolien** auf dem Display des Rechners verhindert werden.

Weiterhin sollte **angemessen viel Platz** für die Arbeiten vorgesehen werden, so dass bspw. vertrauliche Informationen auf Ausdrucken nicht für Dritte frei sichtbar herum liegen.
Ist das Schaffen einer vertraulichen Arbeitsumgebung nicht möglich, sollten auch keine vertraulichen Daten verarbeitet werden.

Arbeiten mit mobilen Geräten

Ein weiterer wichtiger Schritt ist die Wahl der richtigen Arbeitsweise. Hier ist zu entscheiden, ob die Daten direkt auf Geräten innerhalb des DESY-Netzwerkes bearbeitet und gespeichert

werden sollen, oder ob die Bearbeitung und Speicherung der Daten lokal auf dem mobilen Endgerät erfolgen muss, da eine störungsfreie Netzanbindung nicht vorausgesetzt werden kann oder große Datenmengen übertragen werden müssen.

Grundsätzlich ist eine Arbeitsweise vorzuziehen, bei der die **Daten auf Systemen innerhalb DESYs verbleiben** und die Endgeräte lediglich einen Zugang zu ihnen haben.

VPN vs. SSH

Sind Verbindungen in das DESY-Netzwerk erforderlich, ist die Wahl des richtigen Zugangs festzulegen. Diese richtet sich unter anderem danach, mit welcher Art von Endgerät die Verbindung aufgebaut werden und welche Infrastruktur innerhalb DESYs genutzt werden soll.

VPN (Virtuelles Privates Netzwerk) Verbindungen sollen grundsätzlich nur mit von DESY administrierten oder vergleichbaren Endgeräten hergestellt werden. Ansonsten sind per SSH (Secure Shell) getunnelte Verbindungen vorzuziehen. Diese können genutzt werden, um DESY interne Arbeitsumgebungen bspw. die eines Terminalservers zu nutzen.

Siehe hierzu auch:
http://rechnersicherheit.desy.de/regeln_und_empfehlungen/ssh_versus_vpn/index_ger.html

Lokale Speicherung vs. DESY Speicher

Dem potentiellen Verlust vertraulicher Informationen können Sie wirkungsvoll entgegenwirken, indem Sie diese Daten nur innerhalb des DESY-Netzwerkes verarbeiten und keine lokalen Kopien mit sich nehmen. Verbinden Sie sich hierzu über einen geeigneten Weg (VPN/SSH) mit dem DESY-Netz und bearbeiten und speichern Sie die Daten direkt auf den Systemen im DESY-Netz.

Achten Sie dabei auf eine angemessene Arbeitsumgebung (Siehe oben).

Lässt sich ein lokales Abspeichern vertraulicher Informationen nicht vermeiden, ist durch geeignete Maßnahmen (bspw. Verschlüsselung von Ordnerinhalten unter Windows über die erweiterten Attribute der Ordnereigenschaften) sicher zu stellen, dass Unbefugte z.B. nach Verlust des Endgerätes keinen Zugriff auf die Daten haben.

Endgerät

Regelmäßige Updates für Betriebssystem, Anwendungen und Antivirus-Programme

Verwenden Sie für Ihre Arbeit nur Geräte, die über ein **aktuelles** und vom Hersteller noch unterstütztes **Betriebssystem** verfügen und auf einem **aktuellen Patchstand** sind, d.h. bei dem alle verfügbaren Sicherheitsupdates eingespielt sind und des System - falls erforderlich - neu gestartet wurde.

Gleiches gilt für die von Ihnen eingesetzten Anwendungen. Achten Sie dabei auch auf die **Einhaltung der Lizenzbedingungen**. Unter Umständen dürfen Sie Software, die sie auf ihrem privaten Endgerät installiert haben, nicht für dienstliche Zwecke einsetzen.

Der Einsatz eines **aktuellen Antiviren-Programms** wird dringend empfohlen, auf Geräten mit Microsoft Windows sogar vorausgesetzt. Aktualisieren Sie die Signaturen des Antivirus-Programms regelmäßig, mindestens einmal am Tag.

Einsatz privater Endgeräte

Der Einsatz von zentral administrierten DESY-Systemen ist dem Einsatz privater Endgeräte vorzuziehen. Werden private Geräte genutzt, müssen sie die **erforderlichen Sicherheitsanforderungen** erfüllen (aktuelles Betriebssystem mit allen erforderlichen Sicherheitsupdates, aktuelle Anwendungssoftware). Die **Lizenzbedingungen** der installierten Software sind dabei zu beachten. Ggf. ist eine dienstliche Nutzung privat erworbener Software durch die Lizenzbedingungen des Herstellers ausgeschlossen.

Bei der Nutzung privater Geräte empfiehlt es sich, eine **Trennung der dienstlichen von der privaten Nutzung** vorzunehmen, bspw. durch das Anlegen eines separaten Accounts/Profils. Dadurch wird eine bessere Trennung der Daten, die bei der dienstlichen Tätigkeit anfallen, von den Daten aus der privaten Nutzung erreicht. Ist eine weitere dienstliche Nutzung des Gerätes nicht mehr erforderlich, sollte das Profil wieder gelöscht werden.

Einsatz fremder Systeme

Gelegentlich kommt es vor, dass Sie zur Erfüllung dienstlicher Aufgaben auf Endgeräte Dritter zugreifen müssen. Hierbei sind folgende Punkte zu beachten:

- Es muss abgeschätzt werden, ob das Sicherheitsniveau des Endgerätes angemessen zur geplanten Aufgabenerfüllung ist (Wie und von wem wird es administriert? Ist es auf einem aktuellen Stand?). Ist dies nicht der Fall, darf das Gerät nicht verwendet werden.
- Nach getaner Arbeit sind alle genutzten Programme zu schließen und es sich abzumelden. Bestehende Verbindungen zu DESY-Diensten oder -Systemen sind zu beenden.
- Autovervollständigungen sollten deaktiviert und Passwörter dürfen nicht gespeichert werden.
- Temporäre und gecachte Daten sollten gelöscht werden. Wenn sie Dateien bspw. über eine Webbrowser einsehen, werden in aller Regel lokal Kopien des Dokuments abgelegt. Diese sollten gelöscht werden. Dies kann in aller Regel über das Einstellungsmenü des verwendeten Webbrowsers erfolgen.
- Werden Kopien von Daten im temporären Verzeichnis abgelegt sollten auch diese gelöscht werden. Das Verzeichnis der temporären Dateien erreicht man unter Windows, indem an die Eingabeaufforderung öffnet (Win-Taste + R) und %TEMP% eingibt.

Datenträger und Dokumente

Verschlüsselung von Datenträgern mit vertraulichen Inhalten

Werden vertrauliche Daten oder personenbezogene Daten auf Datenträgern mit sich genommen, sind diese ausreichend vor möglichen Einsichten durch Unbefugte bspw. nach Verlust des Datenträgers zu schützen.

Dies lässt sich durch **Verschlüsselung** erreichen, am einfachstem indem man sie in einer **Passwort-geschützten Zipdatei** abspeichert oder unter Windows in einem **Ordner, dessen Inhalte automatisch verschlüsselt** werden (Einstellung über die Erweiterten Attribute unter den allgemeinen Eigenschaften).

Bei Smartphones und Tablets ist eine Verschlüsselung des gesamten Speichers oft einfach über die Systemeinstellungen zu aktivieren.

Aufbewahrung von Datenträgern und Dokumenten

Unterlagen und Datenträger sollten stets so aufbewahrt werden, dass sie vor Zugriffen Unbefugter ausreichend geschützt sind und **nicht frei herum liegen**. Das heißt auch, das Räumlichkeiten, in denen diese Unterlagen aufbewahrt werden, bei Abwesenheit ausreichend vor unbefugten Zugriffen gesichert werden müssen.

Zurücklassen von Geräten / Unterlagen

Müssen Sie bspw. auf einer Tagung Ihr Gerät oder andere Unterlagen für kurze Zeit unbeaufsichtigt lassen, sind Vorkehrungen zu treffen, die einen unbefugten Zugriff auf das Gerät oder die Unterlagen angemessen erschweren. Dazu gehören u.a. das **Sperren des Bildschirms** und das **Zusammenräumen von Unterlagen**. Bei längeren Abwesenheiten sind zusätzlich ggf. mechanische Sicherungen (Kensington-Schloss) vorzusehen, die ein Entwenden des Gerätes, mobiler Datenträger oder der Unterlagen verhindern bzw. ausreichend angemessen erschweren.

Datensicherung

Auch beim Arbeiten von unterwegs oder zuhause sind regelmäßige Sicherungen der Daten erforderlich. Dies kann entweder dadurch geschehen, dass **Daten nur auf zentralen DESY-Speichern** abgelegt werden und somit automatisch gesichert werden, oder durch das Anlegen unabhängiger Sicherungskopien. Hier sind die Anforderungen an die Vertraulichkeit und die Regelungen zur Entsorgung mit zu berücksichtigen (Siehe Entsorgung). Es ist darauf zu achten, dass nach Abschluss der Arbeit keine Arbeitskopien, die nicht mehr benötigt werden, auf Speichermedien verbleiben.

Entsorgung von Dokumenten und Datenträgern

Werden Unterlagen, Ausdrucke oder Datenträger nicht mehr benötigt, sind sie **geeignet zu entsorgen**. Dies kann bspw. durch eine mechanische Zerstörung erfolgen (**Schredder**). Mögliche Aufbewahrungsfristen sind dabei zu berücksichtigen.

Sollte eine angemessene Entsorgung unterwegs nicht möglich sein, sind die Unterlagen bzw. Datenträger bei DESY über die üblichen Wege zu entsorgen.

Weiteres zur Entsorgung von Datenträgern:
http://datenschutz.desy.de/regeln_fuer_desy/datentraegerentsorgung/index_ger.html

Weiteres zur Entsorgung von Dokumenten:
http://datenschutz.desy.de/regeln_fuer_desy/dokumentenentsorgung/index_ger.html

Sonstiges

Nutzung für private Zwecke

Die Nutzung der von DESY bereit gestellten Ressourcen dient dienstlichen Zwecken. Eine davon abweichende Nutzung für private Zwecke ist nur in Übereinstimmung mit der **DESY Benutzungsordnung für IT-Systeme** gestattet.

Zeitnahe Verlustmeldung

Beim **Verlust** von Hardware ist **zeitnahe eine entsprechende Meldung** vorzunehmen. Details hierzu finden sich hier:
http://rechnersicherheit.desy.de/themen/stolenhardware/index_ger.html

Verschlüsselte Protokolle

Achten Sie bei der Anmeldung bei Diensten darauf, dass Ihr Anmeldedaten nur über **verschlüsselte Protokolle** übertragen werden. Dies gilt auch für den Austausch vertraulicher Informationen.

DESY-Informationen auf privaten Geräten

DESY-interne Informationen gehören grundsätzlich nicht auf private Endgeräte. Sollte dies in Ausnahmefällen notwendig sein, ist darauf zu achten, das mögliche Arbeitskopien oder temporär erstelle Dateien gelöscht, vorzugweise überschrieben werden.

Löschen von zur Ansicht herunter geladener Dokumente

Löschen Sie regelmäßig nicht mehr benötigte Dateien in Ihrem Download-Ordner, im Cache Ihres Webbrowsers und im TEMP-Verzeichnis Ihres Betriebssystems. Unter Windows können Sie durch die Tastenkombination „*Win* + *R*“ und die anschließende Eingabe von *%TEMP%* in das Verzeichnis wechseln und manuell temporäre Dateien löschen. Vergessen Sie nicht abschließend auch den Papierkorb zu entleeren.