IT-Benutzungsordnung

Version 2.0 (1.1.2017)

I. Gegenstand und Geltungsbereich

Diese IT-Benutzungsordnung (im Folgenden »ITBO« genannt) regelt den Umgang mit den IT-Systemen, -Diensten und Daten (im Folgenden kurz »IT« genannt) der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (im Folgenden »Fraunhofer-Gesellschaft« genannt). Sie richtet sich an alle Nutzerinnen und Nutzer der IT. [1] Rechte und Pflichten dieser ITBO gelten für alle Arbeitnehmerinnen und Arbeitnehmer der Fraunhofer-Gesellschaft; von anderen, externen Nutzerinnen und Nutzern sind die Pflichten zu beachten.

Regelungen der Gesamtbetriebsvereinbarung »Grundsätze des IT-Einsatzes – generische IT-Lösungen« und anderer Gesamtbetriebsvereinbarungen gehen vor.

II. Ziele

Diese ITBO dient

- dem Schutz der IT und der Persönlichkeitsrechte der Nutzerinnen und Nutzer,
- der Einhaltung von Gesetzen und vertraglichen Verpflichtungen der Fraunhofer-Gesellschaft gegenüber Projekt- und Geschäftspartnern sowie
- dem Schutz von Entwicklungen und geistigem Eigentum.

Zu diesem Zweck

- bringt die ITBO den Nutzerinnen und Nutzern allgemeine Bedingungen der IT-Nutzung zur Kenntnis,
- verpflichtet sie zur deren Beachtung und
- macht ihnen die Maßnahmen zur Protokollierung und Kontrolle der IT-Nutzung transparent.

III. Allgemeine Nutzungsbedingungen

Nachfolgende Bedingungen gelten für jegliche Nutzung der IT:

- Zur Förderung der wissenschaftlichen Arbeit gibt die Fraunhofer-Gesellschaft ihren Nutzerinnen und Nutzern große Freiheiten bei der IT-Nutzung. Viele Aspekte der IT-Nutzung sind nicht im Detail geregelt und technisch nicht reglementiert. Die Nutzer sind daher zu einem risikobewussten und verantwortungsvollen Handeln und Mitdenken verpflichtet, das die Ziele dieser ITBO fördert.
- Unzulässig ist jede IT-Nutzung, die gegen geltende Rechtsvorschriften verstößt, etwa gegen solche des Persönlichkeits- oder Urheberrechts, die die Sicherheit der IT gefährdet oder die dem Ansehen der Fraunhofer-Gesellschaft in der Öffentlichkeit schadet.
- Jede extremistischen, rassistischen, pornographischen oder kriminellen Zwecken dienende Nutzung ist unzulässig.
- Nutzerinnen und Nutzer haben i.d.R. persönliche Benutzerkonten auf Arbeitsplatzrechnern, persona-

[1] Für Nutzer selbständiger Fraunhofer-Einrichtungen im Ausland gibt es eine separate Benutzungsordnung.

lisierte E-Mail-Konten und persönliche Datenablagen in einigen anderen Systemen. Auf dort gespeicherte Daten greift die Fraunhofer-Gesellschaft nur im Notfall oder bei konkretem Missbrauchsverdacht zu.

- Die IT der Fraunhofer-Gesellschaft dient der Erfüllung betrieblicher Aufgaben. Die private Mitnutzung wird Arbeitnehmerinnen und Arbeitnehmern gestattet, soweit sich daraus keine nachteiligen Auswirkungen auf die IT und keine zusätzlichen Erfordernisse für Fraunhofer ergeben.[2]
- Die Fraunhofer-Gesellschaft übernimmt keine Garantie, Gewährleistung oder Haftung für die ständige Verfügbarkeit oder Mängelfreiheit der IT. Insbesondere kann sie IT-Dienste jederzeit, ganz oder teilweise, modifizieren, einschränken oder beenden und deren Nutzung untersagen.
- Nutzerinnen und Nutzer dürfen an Projekt- oder Domänennamen, Knowhow und anderen Informationen, die der Fraunhofer-Gesellschaft oder Ihren Geschäftspartnern gehören oder auf diese zurückzuführen sind, keine Patent-, Marken- oder sonstigen Rechte für sich oder Dritte geltend machen oder beantragen, es sei denn, der Rechteinhaber hat sein schriftliches Einverständnis erklärt.
- Lizenzbestimmungen sind bei der Installation von Software und der Verwendung von Inhalten wie Bildern und Texten zu beachten. Technische Vorrichtungen zum Schutz gegen unerlaubtes Kopieren oder zum Schutz von Urheberrechten dürfen nicht umgangen werden. Lizenzschlüssel und Berechtigungen dürfen nicht ohne Zustimmung der Fraunhofer-Gesellschaft weitergegeben werden. Wie die Genehmigung zu erhalten ist, kann über die IT-Abteilung, den Eigentümer der Inhalte oder Vorgesetzte ermittelt werden.
- Informationen sind entsprechend der Organisationsanweisung zur Informationsklassifizierung (2015/08/3C/O) und externen Vorgaben zu klassifizieren und zu schützen. Projektleiter/innen oder Vorgesetzte entscheiden, wie die Regeln im Arbeitsbereich umzusetzen sind.
- Anhaltspunkte für Missbrauch oder Sicherheitsschwachstellen der IT sind dem Informationssicherheits-Beauftragten der jeweiligen Einheit zu melden.
- Nutzungsbedingungen der Dienstanbieter sowie E-Mails, Aushänge und andere Mitteilungen zur IT-Nutzung sind zu beachten. Nutzerinnen und Nutzer sollen aber bei neuen Dienstangeboten oder im Zweifel auch selbst nachfragen, ob es Regeln zur Nutzung der IT gibt.

Nutzerinnen und Nutzer haben im Rahmen ihrer Handlungsmöglichkeiten alle Maßnahmen zu ergreifen, um Gefährdungen für die IT der Fraunhofer-Gesellschaft zu minimieren. Im Anhang werden die wichtigsten konkreten Maßnahmen wiedergegeben.

IV. Bedingungen der privaten Mitnutzung

Die Fraunhofer-Gesellschaft geht davon aus, dass ein Verbot privater Mitnutzung nicht sinnvoll und eine vollständige Trennung von betrieblicher und privater Nutzung von Kommunikationsmedien kaum möglich ist. Daher ist die private Mitnutzung der IT-Infrastruktur für Arbeitnehmerinnen und Arbeitnehmer der Fraunhofer Gesellschaft unter folgenden Bedingungen zulässig:

- Aus der Mitnutzung der IT zu privaten Zwecken dürfen sich für die Fraunhofer-Gesellschaft keine Zusatzerfordernisse oder zusätzlichen Haftungsrisiken ergeben. Die Sicherheit und die Funktionsfähigkeit der IT-Dienste dürfen durch die private Mitnutzung nicht beeinträchtigt werden. Eventuelle gesetzliche Einschränkungen oder Vorgaben von Auftraggebern sind zu beachten.

[2] Siehe Abschnitt IV und § 4 GBV »Grundsätze des IT-Einsatzes – generische IT-Lösungen«.

- Ein Anspruch, private Geräte an dienstlichen Internetzugängen betreiben zu dürfen oder Software für private Zwecke auf dienstlichen Geräten installieren zu dürfen, besteht nicht. Dies erfordert die Erlaubnis von Vorgesetzen und dem/der IT-Verantwortlichen.
- Datensicherung, Administration, Protokollierung, Kontrolle des Datenverkehrs, Störungsbeseitigung, Löschen von Daten und Neuaufsetzen von Geräten erfolgen ohne besondere Berücksichtigung der privaten Mitnutzung alleine nach betrieblichen Erfordernissen. Ein individuelles Recht, private Daten von der Datensicherung auszunehmen oder private Verbindungen von der für betriebliche Daten zulässigen Protokollierung und Datenauswertung auszunehmen, besteht nicht.
- Es besteht auch kein Anspruch auf Datensicherung und Wiederherstellung privater Daten.
- Aus zuwendungsrechtlichen Gründen ist die Privatnutzung auf eine gelegentliche Mitnutzung beschränkt.
- Betriebliche E-Mail-Adressen, Social Media Accounts und andere betriebliche Adressen sollen nicht als Kontaktadressen für private Kommunikation öffentlich bekanntgemacht werden. Private Daten sollen im persönlichen Bereich gespeichert und als privat gekennzeichnet werden.
- Aus betrieblichen Belangen kann bei besonderen Sicherheitsanforderungen die private Mitnutzung eingeschränkt oder untersagt werden.

V. Spam und Viren, Kontrolle und Protokollierung

Dienstliche und private E-Mails mit Verdacht auf Schadcode, Viren oder Spam dürfen nach Ermessen der Fraunhofer-Gesellschaft in Quarantäne genommen oder zentral gelöscht werden. Nach der Gesamtbetriebsvereinbarung »Grundsätze des IT-Einsatzes – generische IT-Lösungen« sind personenbezogene Auswertungen von Daten, die bei der Nutzung der IT anfallen, u.a. zur Systemadministration möglich, z.B. zur Analyse und Beseitigung von Systemproblemen, zur Sicherstellung der IT-, Betriebs- und Informationssicherheit und zur Wartungsunterstützung. Dies gilt auch für die Abwehr von Cyberangriffen. In bestimmten Fällen ist auch eine forensische Untersuchung der Hardware möglich. Daten des Betriebssystems, betriebssystemnaher Komponenten, Verkehrsdaten aus Internetdiensten und werkzeugbezogene Daten können nach der Gesamtbetriebsvereinbarung protokolliert werden und personenbeziehbare Daten enthalten. Die Protokolle werden i.d.R. nach 30 Tagen gelöscht, Protokolle der IT-Nutzung einer Auslandsanbindung i.d.R. nach 3 Monaten.

VI. Änderungen der ITBO und Inkrafttreten

Die Fraunhofer-Gesellschaft kann diese ITBO jederzeit ändern oder ergänzen, insbesondere im Interesse ihrer betrieblichen Abläufe und der Informationssicherheit.

Diese ITBO ersetzt die bisherige ITBO V1.5 und tritt mit ihrer Bekanntgabe in Kraft. Die Bekanntgabe erfolgt in geeigneter Weise, z.B. per Aushändigung, Rundmail oder Veröffentlichung im Intranet. Gleiches gilt für zukünftige Änderungen oder Ergänzungen der ITBO.

Abweichend davon gilt eine Änderung oder Ergänzung gegenüber Nutzerinnen und Nutzern, die nicht Arbeitnehmer/-in der Fraunhofer-Gesellschaft sind, dann als genehmigt, wenn nicht innerhalb eines Monats nach Bekanntgabe der Änderung oder Ergänzung widersprochen wird, oder wenn die Fraunhofer-IT nach Ablauf der Widerspruchsfrist weiter genutzt wird. Hierauf wird bei Bekanntgabe der Änderung oder Ergänzung hingewiesen. Im Falle eines Widerspruchs kann die Nutzungsbefugnis entzogen werden.

Anhang zur IT-Benutzungsordnung

Version IIS-01 (13.3.2017)

Nutzerinnen und Nutzer haben im Rahmen ihrer Handlungsmöglichkeiten alle Maßnahmen zu ergreifen, um Gefährdungen für die IT der Fraunhofer Gesellschaft zu minimieren und die Ziele der ITBO zu fördern. Nachstehend werden die wichtigsten Maßnahmen wiedergegeben. Über Ausnahmen in besonderen Einzelfällen entscheidet die Abteilungs- oder Projektleitung in Abstimmung mit dem/der Informationssicherheits-Beauftragten unter Beachtung von Betriebsvereinbarungen und anderen Regelungen.

Hinweis

Die aktuell gültigen Gesamtbetriebsvereinbarungen, Organisationsanweisungen und Rundschreiben finden sich in der Compliance-Datenbank der Fraunhofer-Gesellschaft:
http://ocs.zv.fraunhofer.de/OTCS/livelink.exe?func=ll&objId=27180

Zu den IT-Regelungen des Fraunhofer IIS siehe auch die Handlungshilfen
http://www-intern.iis.fhg.de/dienstleister/quorg/hahi_overview/index_html
und die Dokumentensammlung im Intranet
http://www-intern.iis.fhg.de/dienstleister/it/informationssicherheit.

1. Sicherung der Geräte

Der Zugang Unbefugter zu den IT-Systemen des Arbeitsplatzes, den IT-Diensten und Datenträgern und deren Daten ist zu unterbinden. Smartcards sind bei Nichtnutzung sicher wegzuschließen oder mitzunehmen. Systemzugänge sind auch bei kurzer Abwesenheit zu sperren, Computer bei längerer Nichtnutzung herunterzufahren. Virenscanner und andere Sicherheitsmaßnahmen dürfen nicht umgangen werden.
Bei mobilen Rechnern (z.B. Laptops, Tablets, Smartphones, ...), die schützenswerte Daten enthalten, sind diese Daten entsprechend der technischen Machbarkeit ausreichend zu verschlüsseln und der Schlüssel getrennt vom Laptop aufzubewahren. Hierfür sind dem Nutzer durch die IT geeignete Werkzeuge zur Verfügung zu stellen.

2. Passwörter

Passwörter (und PINs) sind sicher zu wählen, geheim zu halten und keinesfalls an andere Personen weiterzugegeben. Hiervon ausgenommen ist die Übergabe beim Ausscheiden, siehe 16), sowie eine Sicherheitshinterlegung im verschlossenen Umschlag gemäß besonderer Vereinbarung. Dienstliche Passwörter dürfen nicht für private Zwecke genutzt werden und für Internet-Dienste sollen andere Passwörter verwendet werden als für interne IT-Dienste.
Dienstlich verwendete Passwörter dürfen nicht in Privatgeräte und andere Fremdgeräte eingegeben werden, ausgenommen die Nutzung des Containers bei »Bring Your Own Device« (BYOD) und Webmail vom privaten Rechner (nicht im Internetcafé!) oder in absoluten Notfällen.
Besteht der Verdacht, dass ein Passwort ausgespäht wurde, so ist es umgehend zu ändern. Details zur sicheren Wahl von Passwörtern können der Anleitung im Intranet (siehe obiger Link) entnommen werden.

3. Softwareinstallation und -verwendung

Grundsätzlich ist vor der Installation von nicht-Standard-Software - auch Add-Ons oder Plug-Ins - die IT-Administration (für Mitarbeiter) bzw. der Betreuer (für Studenten) zu befragen. Software, die offensichtlich den Zugriff auf Instituts-Ressourcen aus dem Internet gestattet, bedarf unbedingt einer Genehmigung

durch die IT-Administration! Dies gilt insbesondere auch für Dienste, die für externe Nutzer über das Internet bereitgestellt werden (z.B. Web-Server) – Näheres hierzu unter Abschnitt 7.
Software ist so zu konfigurieren, dass Korrekturprogramme (Updates, Patches, Hotfixes) zu Sicherheitslücken soweit möglich automatisch installiert werden.
Soweit Nutzer Administrationsrechte erhalten haben und Software selbst installieren dürfen, müssen sie besondere Sicherheitsregeln beachten. V.a. ist Software ausschließlich aus vertrauenswürdigen Quellen zu beschaffen und Updates sind zeitnah zu installieren. Programme, die möglicherweise unkontrollierbar Daten an unbekannte Ziele ins Internet übertragen, dürfen nicht installiert werden.
Grundsätzlich sind die einschlägigen gesetzlichen und rechtlichen Vorschriften einzuhalten. Dies betrifft insbesondere die ausschließliche Verwendung ausreichend lizensierter Software und die Beachtung urheberrechtlicher Vorschriften. Die Softwarelizenz muss eine betriebliche, nicht nur privaten Zwecken dienende, Nutzung durch die Fraunhofer-Gesellschaft erlauben.
Das Herunterladen und Bereitstellen möglicherweise urheberrechtlich geschützter Dateien (z.B. Filesharing, Tauschbörsen) ist verboten; derartige Programme dürfen weder installiert noch genutzt werden.
Verboten ist die Bereithaltung, Verwendung oder Weiterverbreitung von kopierschutzbefreiter Software oder von Programmen zur Umgehung von Kopierschutzmaßnahmen. Nicht gestattet sind die Verwendung von Programmen zur Ermittlung normalerweise verborgener Lizenzinformationen (z.B. Seriennummern oder Zugangscodes) sowie die Weitergabe solcher Informationen an Dritte.

4. E-Mail-Nutzung

Für Arbeiten für die Fraunhofer-Gesellschaft ist nur die Fraunhofer-E-Mail-Adresse zu verwenden. Das automatische Weiterleiten dienstlicher E-Mails auf externe E-Mail-Accounts ist unzulässig. Die Nutzung der dienstlichen Mailverteiler für private Zwecke wie Spendenaufrufe, Aufrufe zu Teilnahme an Umfragen oder zur Verbreitung politischer oder sonstige Meinungsäußerungen ist zu unterlassen.
Die Veröffentlichung von Fraunhofer-Mailadressen darf nur im dienstlichen Kontext erfolgen. Die private Nutzung der dienstlichen Mailadresse ist zulässig, sollte aber vermieden werden. Alternativ sollten für private Kommunikation getrennte Mailadressen gewählt werden. Private E-Mails sollen separat von dienstlichen E-Mails in Ordnern gespeichert werden, die im Ordnernamen das Wort »privat« beinhalten.
Eingehende Mails bergen trotz Filterung ein nicht zu unterschätzendes Risiko durch Malware. Bei verdächtigen Mails mit Anhängen, auch von vermeintlich bekannten Absendern, sollten diese erst nach vorheriger Virenprüfung bzw. Rücksprache mit der IT-Administration oder dem Absender geöffnet werden.
Eine Weiterleitung bzw. Verbreitung von Warnmeldungen vor Schadsoftware darf ausschließlich durch die IT-Administration erfolgen.
Beim Versand von Mails sind immer die datenschutzrechtlichen Bestimmungen zu beachten, besonders bei vertraulichen oder sensitiven personenbezogenen Inhalten.
Größere Anhänge sollten nicht per Mail an Verteilerlisten geschickt, sondern auf einem internen Server (siehe Abschnitte 6 und 7) bereitgestellt werden.

5. Nutzung des Netzwerks

Fremdgeräte dürfen nur mit eduroam oder einem Gästenetz verbunden werden, nicht aber mit dem institutsinternen Netzwerk. Rechner, Drucker, Telefone und andere Geräte dürfen nur nach Freigabe der IT-Administration ins interne Netz integriert werden. Geräte, die ins Netzwerk integriert werden sollen, dürfen nur von der IT-Administration oder nach deren Vorgaben konfiguriert werden. Die eigenmächtige Änderung der Netzwerkkonfiguration sowie die Installation von WLAN-Accesspoints, Switches und anderen Netzwerkkomponenten sind verboten. Der Einsatz von Programmen, die den Netzwerkverkehr überwachen, ist nur durch dazu explizit befugte Mitarbeiter der IT-Administration zu dienstlichen Zwecken oder mit Ausnahmegenehmigung des Informationssicherheits-Beauftragten oder des IT-Verantwortlichen

zulässig.

6. Internet- und Cloud-Dienste

Firmendaten sind grundsätzlich nur auf Systemen zu speichern, die von Fraunhofer betrieben werden oder von der IT-Administration dafür freigegeben wurden. Die selbstgewählte Speicherung in öffentlichen Cloud-Diensten wie Dropbox ist aufgrund von Datenschutzbestimmungen und anderen Gesetzen, Verträgen und Betriebsvereinbarungen vielfach unzulässig und teilweise sogar strafbar. Vor einem Transfer von Firmendaten ins Internet sind Projektleitungen und Vorgesetzte zu fragen, die die Zulässigkeit sowie eventuelle Sicherheitsmaßnahmen abklären und eine Genehmigung erteilen. Durch Aufzeichnung der Zugangsdaten zu rein dienstlichen Accounts, insbesondere zu Social Media-Accounts, und durch Meldung bei der/dem Vorgesetzten ist sicherzustellen, dass solche Accounts zugreifbar bleiben und vergessene Accounts vermieden werden. Die generelle Freigabe von vollständigen Adressverzeichnissen für einen Betreiber zum Abgleich von Kontakten ist nicht zulässig.
Internetseiten mit vermutlich oder offensichtlich illegalen Inhalten sind zu meiden. Um das ungewollte automatische Installieren von Schadfunktionen beim Besuch von Internet-Seiten zu verhindern, sollten mit geeigneten Browsereinstellungen und Browser-Plugins aktive Inhalte möglichst selektiv geblockt werden. Hinweise hierzu findet man im Intranet des IIS.

7. Im Internet bereitgestellt Dienste und Daten

Sollen – z.B. im Rahmen von Projekten – Daten und Dienste im Internet öffentlich oder für bestimmte Benutzergruppen bereitgestellt werden, müssen diese Dienste vorher von der IT-Administration genehmigt werden. Weiterhin muss für den Betrieb dieser Dienste eine verantwortliche Person als technischer und inhaltlicher Ansprechpartner des Betreibers benannt werden. Scheidet dieser Ansprechpartner aus dem Dienst der Fraunhofer-Gesellschaft aus, muss rechtzeitig vorher ein Nachfolger benannt und eingewiesen werden, andernfalls darf der Dienst nicht weiter betrieben werden. Der Verantwortliche ist auch für eine zeitnahe Reaktion bzw. Abhilfe bei bekannt werdenden Sicherheitslücken der betriebenen Plattform zuständig.
Die Beantragung und Reservierung von Internet-Domains darf ausschließlich über die IT-Administration erfolgen. Nähere Einzelheiten zur Beantragung und zum Betrieb von Internet-Domains werden in einem gesonderten Merkblatt geregelt.

8. Umgang mit vertraulichen Daten

Zum Schutz der Vertraulichkeit von Daten sind die Vorgaben der Organisationsanweisung zur Informationsklassifizierung 2015/08/3C/O zu beachten. Informationen, die nicht als »offen« klassifiziert sind, sind als »intern« anzusehen und dürfen ohne Zustimmung der/des Vorgesetzten oder der Projektleitung Fraunhofer nicht verlassen, d.h. insbesondere nicht an Externe weitergeleitet oder in nicht freigegebenen Cloud-Diensten gespeichert werden. Als »vertraulich« klassifizierte Daten sind besonders zu schützen, insbesondere sind sie sichtbar zu kennzeichnen und verschlüsselt zu versenden, sofern die Abteilungs- oder Projektleitung nichts anderes festgelegt hat. Als »offen« klassifizierte Daten unterliegen diesen Einschränkungen nicht, jedoch sind Rechte Dritter, wie z.B. Urheberrechte, vor der Weitergabe zu beachten. Über weitere Vorgaben und Ausnahmen informiert die zuständige Projekt- und Abteilungsleitung. Details regelt die Handlungshilfe »Informationsklassifizierung«.

9. Nutzung mobiler Endgeräte

Dienstlich genutzte Notebooks, Smartphones und Tablets erfordern gesonderte Sicherheitsvorkehrungen. Sie sind nicht unbeaufsichtigt an frei zugänglichen Orten zurückzulassen. Um Updates und Sicherheitspat-

ches zeitnah zu installieren, muss dafür gesorgt werden, dass die Geräte mindestens einmal monatlich für mindestens eine Stunde Kontakt mit dem IIS-Netzwerk haben. Soweit die IT- Administration dem Nutzer die Sicherheitseinstellungen nicht fest vorgegeben eingestellt hat, muss der Nutzer diese selbst vornehmen. Die PIN- oder Passwort-Eingabe sowie deren Aktivierung bei Nichtbenutzung des Geräts ist einzuschalten, bei mehrfach (max. 10-mal) falscher Codeeingabe müssen (bei Smartphones und Tabletts und soweit möglich) alle Daten gelöscht werden. Jailbreaken und Rooten der Geräte ist untersagt.
Mobile Endgeräte sollen nicht als Datenträger (im Sinne eines USB-Sticks o.ä.) eingesetzt werden, da sie immer eingeschaltet sind und zahlreiche Internet-Schnittstellen haben. Ausnahmen gelten für den Transport verschlüsselter oder öffentlicher Daten, z.B. für Präsentationen für öffentliche Vorträge.
Apps dürfen nur aus dem App-Shop des Herstellers oder bekannt vertrauenswürdigen Quellen bezogen werden. Betriebliche Daten, insbesondere Adressbücher und E-Mails, dürfen nur bei freigegebenen externen Diensten gespeichert oder über dafür freigegebene Clouds synchronisiert werden. Der betriebliche E-Mail-Account muss der Standard-Account des mobilen Endgeräts sein. Bei Geräteverlust ist die IT-Abteilung oder der Fraunhofer-Servicedesk umgehend zu informieren. Nach Möglichkeit wird dann ein Fernlöschen durchgeführt und eine Diebstahl-/Verlustanzeige aufgegeben.
Weitere Details speziell für Smartphones und Tablets regelt eine gesonderte Benutzerordnung.
Für Test- und Entwicklungsgeräte können abweichende Vorgaben vereinbart werden.

10. Nutzung eigener Hardware

Die Nutzung nicht von Fraunhofer bereitgestellter, insbesondere privater Hardware (auch USB-Sticks) zu betrieblichen Zwecken der Fraunhofer-Gesellschaft (»Bring Your Own Device«, BYOD) erfolgt nur nach Genehmigung durch den IT-Verantwortlichen/die IT-Verantwortliche in Rücksprache mit dem/der Informationssicherheitsbeauftragten der Einheit. Die Nutzung privater Geräte kann weder vom Nutzer noch von Fraunhofer verlangt werden.
Vollzugang zum internen Institutsnetz ist nur möglich für Geräte, die vollständig vom Institut administriert werden und allen Sicherheitsanforderungen entsprechen. Ein eingeschränkter Zugang (z.B. nur Kalender und Mail) zum internen Institutsnetz kann über eine Container-App bereitgestellt werden. Näheres regelt die Benutzerordnung Mobilgeräte.
Software des Instituts darf nur in Einzelfällen und nach Genehmigung durch die IT-Administration auf diesen Rechnern eingesetzt werden. Eventuelle Einschränkungen in der Art und Dauer der Nutzung sind einzuhalten.
Grundsätzlich sind betriebliche Daten von privaten zu trennen und besonders zu schützen. Familienangehörige und andere Personen dürfen auf betriebliche Daten nicht zugreifen können. Beim Ausscheiden aus Fraunhofer sind betriebliche Daten zu löschen, wenn mit der Projekt- bzw. Abteilungsleitung nichts anderes vereinbart wurde. Der IT-Administration ist die Kontrolle von Sicherheitseinstellungen zu gestatten.
Sofern BYOD für Smartphones oder Tablets gestattet wird, gelten die Bestimmungen des vorherigen Abschnitts »Nutzung mobiler Endgeräte«.

11. Verhalten auf Reisen

Die Nutzung von IT-Diensten auf Reisen erfordert besondere Sicherungsmaßnahmen. Es ist darauf zu achten, dass Dritte vertrauliche Gespräche nicht mithören und angezeigte Daten nicht beobachten können, z.B. durch Dunkelstellen des Bildschirms und ggf. Sichtschutz für den Bildschirm. Geräte sind nicht unbeaufsichtigt zu lassen. Beim kurzzeitigen Verlassen sind Geräte zu sperren und, wenn möglich, auch physisch zu sichern, z.B. über ein Kabel mit Schloss oder durch Einschließen. Gegebenenfalls ist jemand zu bitten, auf das Gerät kurz aufzupassen. Bei längerer Abwesenheit oder im Hotel sind Geräte herunterzufahren, so dass die Schlüssel der Festplattenverschlüsselung nicht mehr im Arbeitsspeicher liegen. Bei Reisen in Risikoländer sollte ein gesondertes Reisegerät mit nur den für die Reise notwendigen Daten mitge-

nommen werden.

12. Datensicherung

Backups erfolgen durch die Fraunhofer-Gesellschaft oder durch deren Einrichtungen. Aus diesem Grund sollten Projektdaten und andere wichtigen Dokumente grundsätzlich in einer mit dem Projektleiter abgesprochenen Struktur auf den Institutsservern gespeichert werden. Nutzer sollen sich über die Vorgaben zur Datensicherung informieren. Wenn aus zwingenden Gründen Daten oder E-Mails nur auf einem Endgerät anstatt auf Servern gespeichert werden, unterliegen diese möglicherweise nicht der automatischen Datensicherung. Der Nutzer muss dann in Rücksprache mit der IT-Abteilung und dem Vorgesetzten selbst für eine geeignete Datensicherung sorgen und ist für diese verantwortlich.
Wird längere Zeit auf einem PC ohne Serverkontakt gearbeitet, sind von wichtigen Dateien lokale Sicherheitskopien zu erstellen (z.B. auf USB-Stick oder externen Festplatten).

13. Aufbewahrung von Daten

Projektergebnisse und andere betriebliche Daten sind entsprechend den gesetzlichen Vorgaben, den geltenden Verträgen und den Grundsätzen ordnungsgemäßer wissenschaftlicher Arbeit sicher aufzubewahren. In der Regel gilt eine Mindestaufbewahrungsfrist von 6 Jahren (insbesondere für geschäftliche E-Mails und Briefe); für Verträge und Buchungsbelege beträgt die Mindestaufbewahrungsfrist 10 Jahre. Es wird darauf hingewiesen, dass im Einzelfall die geforderten Aufbewahrungsfristen in Projekten auch länger sein können. Dies ist vor Projektbeginn abzuklären. Bei Unklarheiten bezüglich der Aufbewahrungsfristen ist immer von 10 Jahren Mindestaufbewahrungsfrist auszugehen. Die Ablage administrativer Daten (insbesondere Verträge, Geschäftsbriefe) erfolgt laufend und zeitnah in der zum Projekt bzw. der Abteilung gehörenden Projektakte. Andere Daten (z.B. Projektinhalte) werden entsprechend den institutslokalen Regelungen evtl. auch anders archiviert. Die Projekt- und Abteilungsleiter/innen informieren über anzuwendende Regeln und Verfahren.

14. Entsorgen von Datenträgern

Datenträger mit vertraulichen Daten oder anderweitig schützenswerten Inhalten dürfen nicht ohne Geheimhaltungsvereinbarung weitergegeben oder ohne sicheres Löschen bzw. Vernichten entsorgt werden; einfaches Löschen ist unzureichend! Hier bitte den Rat der IT-Administration einholen bzw. die Datenträger zur Vernichtung an diese weiterleiten!
Festplatten und Wechseldatenträger wie CDs, DVDs, USB-Sticks sind zu diesem Zweck an die IT-Administration weiterzugeben.

15. Schutz vor Schadsoftware

Jeder Rechner wird durch einen von der IT-Administration vorgegebenen Virenscanner geschützt.
Die Aktualisierung des Betriebssystems, der Standardprogramme und des Virenscanners wird von der IT-Administration aktiv betrieben. Das Behindern oder Deaktivieren der Aktualisierungen oder des Virenscans ist unzulässig. Dazu ist für einen regelmäßigen ausreichend langen Kontakt mobiler Rechner zum internen Netzwerk des IIS (via VPN) zu sorgen. (Siehe Punkt 9)
Auf Laptops bzw. Rechnern, die direkten Zugang zum Internet haben können (also ohne die Firewall des Institutsnetzes), ist eine »Personal Firewall« einzusetzen. Auswahl, Konfiguration und Installation dieser Firewall erfolgt durch die IT-Administration, um nicht den Netzwerkbetrieb oder die Rechnerverwaltung bzw. Wartung zu behindern.

16. Übergabe von Daten beim Ausscheiden

Nutzerinnen und Nutzer haben vor ihrem Ausscheiden aus der Fraunhofer-Gesellschaft Projektergebnisse und andere dienstliche Daten für die Weiterarbeit zu übergeben und in den vorgesehenen Projektakten oder Ablagen zu speichern. Privaten Daten sind von den Fraunhofer-Speichermedien zu löschen.
Alle erstellten Wechseldatenträger bleiben nach dem Ausscheiden am Institut; weiterhin gelten die Regelungen der Datenübergabeerklärung (Auszufüllen beim Ausscheiden). Es hat eine sorgfältige Dokumentation und Übergabe aller dienstlichen Daten sowie bei verschlüsselten Daten der zugehörigen Schlüssel an den Vorgesetzten oder den durch diesen Beauftragten zu erfolgen. Ebenso zu übergeben sind ggf. gesetzte BIOS-Passwörter oder Passwörter für Festplattenverschlüsselung.
Da eine zielgenaue Selektion und Übergabe insbesondere bei E-Mails mitunter nicht gelingt, kann das Institut die Daten des persönlichen Bereichs (Homeverzeichnis und E-Mail-Account) in begründeten Fällen über das Beschäftigungsverhältnis hinaus innerhalb rechtlich zulässiger Fristen (in der Regel 10 Jahre) speichern. Eine Einsichtnahme in diese Daten erfolgt nur mit einem Mitglied des zuständigen Betriebsrats oder einer vom Gesamtbetriebsrat benannten Vertretung. Ausgeschiedene Nutzerinnen und Nutzer haben keinen Anspruch darauf, dass Fraunhofer ihre privaten Daten weiter speichert oder ihnen weiter zugänglich macht. E-Mail-Accounts werden nach dem Ausscheiden deaktiviert und eingehende E-Mails mit einer Autonachricht abgelehnt.

17. Bearbeitung und Speicherung personenbezogener Daten, Auftragsdatenverarbeitung

Vor der Verarbeitung oder Speicherung personenbezogener Daten sind besondere Schutzkonzepte zu erstellen. Hierzu muss rechtzeitig vor Projektbeginn die Gruppe Recht und die IT-Administration einbezogen werden. Alle Datenschutzbestimmungen sind strikt einzuhalten.
Werden externe Dienstleister mit der Verarbeitung personenbezogener Daten betraut, ist (unter Einbeziehung von Einkauf und Recht) eine separate Vereinbarung zur Auftragsdatenvereinbarung abzuschließen, in der alle in §11 BDSG angesprochenen Pflichten geregelt sein müssen. Dies trifft auch auf Aufträge zu, bei denen der Auftragnehmer Zugriff auf Datenbestände mit personenbezogenen Daten unserer Mitarbeiter oder Partner bekommen bzw. derartige Daten in unserem Auftrag erheben soll.

18. Allgemeine Regeln

Grundsätzlich gilt: Schonender Umgang mit den Ressourcen, bewusster Umgang mit dem Speicherplatz auf Servern und im Backup, gesundes Misstrauen und sensibler Umgang mit Internet, Email und dem Rechner allgemein sind die Pflichten aller Mitarbeiterinnen und Mitarbeiter. Im Zweifelsfall hilft die IT-Administration gerne. Informationssicherheit ist auf Dauer nur durch einen vertrauensvollen Umgang zwischen Nutzern und IT-Administration zu erreichen.
Alle Mitarbeiterinnen und Mitarbeiter sind angehalten, im Intranet veröffentlichte Meldungen der IT zu lesen und darin evtl. ausgesprochene Anweisungen zeitnah zu befolgen. Ebenso ist die jährliche Teilnahme an den regelmäßig stattfindenden IT-Sicherheitsunterweisungen verpflichtend.

Kenntnisnahme und Anerkennung der IT-Benutzungsordnung der Fraunhofer-Gesellschaft

Bitte Online, sonst Formularkopf handschriftlich in GROSSBUCHSTABEN ausfüllen!

Institutsnummer	Institutskürzel	Personalnummer (sofern vorhanden)
Vorname		Name

— Auszufüllen vom IT-Nutzer/ der IT-Nutzerin: —

Ich erkläre hiermit, die Bestimmungen dieser IT-Benutzungsordnung und ihres Anhangs zur Kenntnis genommen zu haben und verpflichte mich, diese einzuhalten.

Sofern ich die IT der Fraunhofer-Gesellschaft privat mitnutze, willige ich ausdrücklich in die Bedingungen der privaten Mitnutzung gem. Ziffer IV dieser ITBO ein.

Sofern ich nicht Arbeitnehmerin oder Arbeitnehmer der Fraunhofer-Gesellschaft bin, sondern eine andere externe Nutzerin / ein anderer externer Nutzer, gelten die in der ITBO festgelegten Pflichten und Regelungen sinngemäß auch für mich. Rechte, die in der IT-Benutzungsordnung für die Arbeitnehmerinnen und Arbeitnehmer beschrieben sind, wie zum Beispiel die zur privaten Mitnutzung, stehen mir dagegen aus rechtlichen Gründen nicht zu.

Ort und Datum	Unterschrift