IT-Benutzungsordnung

Version 3.0

Diese IT-Benutzungsordnung (im Folgenden »ITBO« genannt) enthält Grundregeln zum Umgang mit den IT-Systemen, -Diensten und Informationen der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. - im Folgenden »Fraunhofer-Gesellschaft« genannt. Sie richtet sich an alle Nutzerinnen und Nutzer der Fraunhofer-IT, auch externe, die ausnahmsweise Zugang zum Fraunhofer-Intranet erhalten. Die Pflichten dieser ITBO gelten für alle; die Rechte insbesondere auf private Mitnutzung sind Arbeitnehmerinnen und Arbeitnehmern der Fraunhofer-Gesellschaft vorbehalten.

I. Ziele

Diese ITBO dient:

- der Sicherstellung von Informationssicherheit und Datenschutz,
- dem Schutz der IT sowie der Persönlichkeitsrechte der Nutzerinnen und Nutzer,
- der Einhaltung von Gesetzen und Verträgen gegenüber Projekt- und Geschäftspartnern sowie
- dem Schutz von geistigem Eigentum.

Zu diesem Zweck:

- bringt die ITBO den Nutzerinnen und Nutzern allgemeine Bedingungen der IT-Nutzung zur Kenntnis,
- verpflichtet die ITBO diese zur deren Beachtung und
- macht ihnen die ITBO die Maßnahmen zur Protokollierung und Kontrolle sowie zur Verarbeitung personenbezogener Daten bei der IT-Nutzung transparent.

Wichtige IT-bezogene und für alle Nutzerinnen und Nutzer relevanten Regeln aus Organisationsanweisungen zur Informationssicherheit und einer grundlegenden Gesamtbetriebsvereinbarung sind berücksichtigt.[1]

II. Allgemeine Nutzungsbedingungen und Regeln

Nachfolgende Bedingungen gelten für jegliche Nutzung der IT:

- Zur Förderung wissenschaftlicher Arbeit gibt die Fraunhofer-Gesellschaft ihren Nutzerinnen und Nutzern große Freiheiten bei der IT-Nutzung. Viele Aspekte der IT-Nutzung sind nicht im Detail, sondern vorwiegend generisch geregelt und technisch nicht reglementiert. Die Nutzerinnen und Nutzer sind daher zu einem risikobewussten und verantwortungsvollen Handeln und Mitdenken verpflichtet, das die Ziele dieser ITBO fördert.
- Jede extremistischen, rassistischen, pornographischen oder kriminellen Zwecken dienende IT-Nutzung ist unzulässig.

[1] Gesamtbetriebsvereinbarung „Grundsätze des IT-Einsatzes“ sowie die Organisationsanweisung zur »Informationsklassifizierung« und zur »Informationssicherheit«

- Unzulässig sind weiterhin jede IT-Nutzung und Informationsverarbeitung, die gegen geltendes Recht verstößt, etwa gegen das Persönlichkeits- oder Urheberrecht, oder welche die Sicherheit der IT gefährdet oder die dem Ansehen der Fraunhofer-Gesellschaft in der Öffentlichkeit schadet.
- Nutzerinnen und Nutzer haben i. d. R. persönliche Benutzer-Accounts auf Arbeitsplatzrechnern, personalisierte E-Mail-Konten und persönliche Datenablagen in einigen anderen Systemen (der sog. »persönliche Bereich«). Auf dort gespeicherte Daten greift Fraunhofer nur im Notfall oder bei konkretem Missbrauchsverdacht gemäß den Regelungen der GBV „IT-Grundsätze" zu.
- Die IT der Fraunhofer-Gesellschaft dient vordringlich der Erfüllung dienstlicher 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. Bedingungen für die private Mitnutzung befinden sich in Ziffer III.
- 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 Fraunhofer oder Geschäftspartnern gehören oder auf diese zurückzuführen sind, keine Patent-, Marken- oder sonstigen Rechte für sich oder Dritte geltend machen oder beantragen, es sei denn, Rechteinhaber haben ihr schriftliches Einverständnis erklärt.
- Lizenzbestimmungen von Software und (Cloud-)Diensten sowie bei der Verwendung von Inhalten wie Bildern und Texten sind zu beachten. Lizenzschlüssel und Berechtigungen dürfen nicht ohne Zustimmung der Fraunhofer-Gesellschaft weitergegeben oder anderweitig genutzt werden.
- Informationen sind entsprechend der Organisationsanweisung zur Informationsklassifizierung und externen Vorgaben hinsichtlich ihres Schutzbedarfs zu klassifizieren und zu schützen. Projektleitungen oder Vorgesetzte entscheiden, wie die Regeln im jeweiligen Arbeitsbereich umzusetzen sind.
- Erkannte oder vermutete Sicherheitslücken, Informationssicherheits- oder Datenschutzvorfälle müssen unverzüglich gemeldet werden – sofern lokal nichts anders geregelt ist, beim Servicedesk servicedesk@fraunhofer.de bzw. telefonisch unter 02241-14-1414.
- Nutzungshinweise zu den intern angebotenen Diensten sowie Hinweise in E-Mails, Aushängen und anderen Mitteilungen zur IT-Nutzung sind zu beachten. Nutzerinnen und Nutzer sollen bei neuen Angeboten oder im Zweifel auch selbst nachfragen, ob es Regeln zur Nutzung der IT gibt.
- Nutzerinnen und Nutzer müssen entsprechend der Regelungen in ihrem Institut mindestens einmal jährlich an Sensibilisierungs- und Schulungsmaßnahmen zum Thema Informationssicherheit teilnehmen und sollen auch aktuelle Sicherheitshinweise beachten.

III. Bedingungen der privaten Mitnutzung

Die Fraunhofer-Gesellschaft geht davon aus, dass ein Verbot privater Mitnutzung der IT in der Forschung nicht sinnvoll und eine vollständige Trennung von dienstlicher und nicht-dienstlicher Nutzung auch aufgrund der engen Zusammenarbeit mit Universitäten kaum möglich ist. Daher ist Arbeitnehmerinnen und Arbeitnehmer der Fraunhofer Gesellschaft eine nicht-dienstliche Mitnutzung unter folgenden Bedingungen gestattet:

- 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.

- 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 der IT-Leitung.
- Datensicherung, Administration, Protokollierung, Kontrolle des Datenverkehrs, Störungsbeseitigung, Löschen von Daten und Neuaufsetzen von Geräten erfolgen ohne besondere Berücksichtigung der privaten Mitnutzung 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 kein Anspruch auf Datensicherung und Wiederherstellung privater Daten.
- Aus zuwendungsrechtlichen Gründen ist die Privatnutzung auf eine gelegentliche Mitnutzung beschränkt. Eine Nutzung für privat-geschäftliche Zwecke ist nicht erlaubt.
- Betriebliche E-Mail-Adressen, Social Media Accounts und andere dienstliche Adressen sollen nicht als Kontaktadressen für private Kommunikation im öffentlichen Raum verwendet 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.

IV. Protokollierung und Kontrolle

Im Rahmen des IT-Betriebs werden, um den Betrieb zu ermöglichen und seine Sicherheit zu gewährleisten, personenbezogene Daten der Nutzenden verarbeitet, die im Rahmen der erlaubten privaten Mitnutzung auch privat sein können:

- 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.
- Personenbezogene Auswertungen von Daten, die bei der Nutzung der IT anfallen, sind zur Systemadministration, z. B. zur Analyse und Beseitigung von Systemproblemen, zur Sicherstellung der IT-, Betriebs- und Informationssicherheit und zur Wartungsunterstützung durch berechtigtes Personal zulässig.
- Dies gilt auch für die Abwehr von Cyberangriffen. In bestimmten Fällen ist auch eine forensische Untersuchung der Systeme möglich. Daten des Betriebssystems, betriebssystemnaher Komponenten, Verkehrsdaten aus Internetdiensten und werkzeugbezogene Daten können protokolliert werden und personenbeziehbare Daten enthalten, die zur Abwehr oder Analyse ggf. untersucht werden. Die Protokolldaten werden i. d. R. nach 30 Tagen gelöscht.

V. Änderungen der IT-Benutzungsordnung 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-Version 2.0 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 Arbeitnehmende 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: Ergänzende Informationen zur Umsetzung

Version IIS-03 (16.07.2026)

In der Fraunhofer-Gesellschaft gibt es zur Sicherstellung eines angemessenen Schutzes, einer angemessenen Nutzung und eines angemessenen Umgangs mit Informationen und anderen damit verbundenen Werten Regeln, die für alle Nutzerinnen und Nutzer gültig sind. Im Rahmen ihrer Möglichkeiten haben sie alle Maßnahmen zu ergreifen, um Gefährdungen für Fraunhofer zu minimieren und die Ziele der ITBO zu fördern.
Grundsätzlich gilt: Schonender Umgang mit den Ressourcen, bewusster Umgang mit dem Speicherplatz auf Servern und im Backup, gesundes Misstrauen und sensibler Umgang mit Internet, E-Mail und dem Computer allgemein sind die Pflichten aller. Im Zweifelsfall hilft die Abteilung IT-Service gerne. Informationssicherheit ist auf Dauer nur durch einen vertrauensvollen Umgang zwischen Nutzenden und IT-Administration zu erreichen.

Alle Nutzerinnen und Nutzer sind angehalten, im Intranet veröffentlichte Meldungen der Abteilung IT-Service bzw. der Informationssicherheit regelmäßig zu lesen und darin evtl. ausgesprochene Anweisungen zeitnah zu befolgen.
Ebenso ist die jährliche Teilnahme an den Sicherheitsunterweisungen verpflichtend, siehe *Handlungshilfe »Unterweisung bezüglich Informationssicherheit«*.

Nachstehend werden die wichtigsten Maßnahmen wiedergegeben. Über Ausnahmen in Einzelfällen entscheidet die Abteilungs- oder Projektleitung in Abstimmung mit dem/der Informationssicherheits-Beauftragten unter Beachtung von Betriebsvereinbarungen und anderen Regelungen.

Hinweis
Gesamtbetriebsvereinbarungen (**GBV**) und Organisationsanweisungen (**OrgA**) finden sich in der Fraunhofer-Regelungsdatenbank:

- https://fraunhofer.sharepoint.com/sites/fraunhofer-recht/SitePages/Regelungsdatenbank.aspx

Zu den spezifischen Regelungen des Fraunhofer IIS siehe auch

- Handlungshilfen (**HaHi**): https://intern.iis.fhg.de/x/VRyWBQ
- Intranet, Bereich Informationssicherheit: https://intern.iis.fhg.de/x/l7o1C

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 wegzuschließen oder mitzunehmen. Systemzugänge sind auch bei kurzer Abwesenheit zu sperren, Computer bei längerer Nichtnutzung herunterzufahren. Büros sollten abgeschlossen werden, wenn sie nicht besetzt sind. Endpoint Protection (Virenscanner) und andere Sicherheitsmaßnahmen dürfen nicht umgangen werden.
Mobile Geräte sowie Geräte, die das Haus verlassen müssen nach Stand der Technik verschlüsselt sein.

2 Passwörter und Zertifikate

Passwörter (und andere Zugangsdaten wie PINs) sind in der Regel an die Person gebunden und dürfen nicht weitergegeben werden. Hiervon ausgenommen sind geteilte Accounts (z.B. siehe Abschnitt »In-

ternet- und Cloud-Dienste«), Funktions-Accounts, die Übergabe beim Ausscheiden oder gemäß besonderer Vereinbarung. Passwörter sind sicher zu wählen und geheim zu halten. Dienstliche Passwörter dürfen nicht für private Zwecke genutzt werden. Dienstlich verwendete Passwörter dürfen nicht in Privatgeräte und andere Fremdgeräte eingegeben werden, ausgenommen Dienste, die explizit für die Nutzung auf nicht-dienstlichen Geräten freigegeben wurden, wie z.B. Container-App, WebVPN und Webmail vom privaten Computer (jedoch nicht von fremdkontrollierten Rechnern z.B. im Internetcafé!) oder in absoluten Notfällen. Für externe bzw. Internet-Dienste dürfen keine auch für interne Dienste verwendeten Passwörter genutzt werden. Smartcards und persönliche elektronische Schlüssel bzw. Zertifikate sind vertraulich zu behandeln und diese sowie ihre PIN nicht weiterzugeben. Der Einsatz von Password-Safe-Software wird dringend empfohlen, um die Einhaltung obiger Vorgaben zu erleichtern.
Besteht der Verdacht, dass ein Passwort ausgespäht wurde, so ist es umgehend zu ändern. Hilfe zur sicheren Wahl von Passwörtern finden sich im Intranet, Bereich Informationssicherheit.
Werden Passwörter für Dienste, die vom Fraunhofer IIS im Internet genutzt werden (z.B. Facebook, Youtube, Dell-Gerätemanagement) Personen außerhalb des IIS (auch ausgeschiedene Mitarbeitende) bekannt, sind diese schnellstmöglich zu ändern.

3 Softwareinstallation

Neue Software darf, soweit es sich nicht um freigegebene Software aus institutsinternen Quellen handelt, nur nach Abstimmung mit der Abteilung IT-Service genutzt werden. Die Softwarelizenz muss eine betriebliche, nicht nur privaten Zwecken dienende, Nutzung durch die Fraunhofer-Gesellschaft erlauben. Wird ein Nutzerin oder ein Nutzer durch die Abteilung IT-Service zur manuellen Installation aufgefordert, ist diese so bald wie möglich durchzuführen. Soweit Nutzerinnen und Nutzer, z. B. an Entwicklerarbeitsplätzen, ausnahmsweise Administrationsrechte erhalten und Software selbst installieren dürfen, müssen sie besondere Sicherheitsregeln beachten, auf die sie die Abteilung IT-Service hinweist (u. a. Patches und Updates installieren): Software ist auch nur aus vertrauenswürdigen Quellen zu beschaffen. Updates sind stets zeitnah bzw. wenn möglich automatisch zu installieren. Dies gilt insbesondere für sicherheitsrelevante Aktualisierungen (Updates, Patches, Hotfixes) zu Sicherheitslücken.
Software, die offensichtlich den Zugriff auf Instituts-Ressourcen aus dem Internet gestattet, bedarf zwingend einer Genehmigung durch die Abteilung IT-Service! Dies gilt insbesondere auch für Dienste, die für externe Nutzerinnen und Nutzer über das Internet bereitgestellt werden (z.B. Web-Server, TeamViewer oder Gitlab Runner) – Näheres hierzu unter Abschnitt »Im Internet bereitgestellt Dienste und Daten«. Programme, die möglicherweise unkontrollierbar Daten an unbekannte Ziele ins Internet übertragen, dürfen nicht installiert werden.
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 die Fraunhofer-E-Mail-Adresse zu verwenden. Das automatische Weiterleiten dienstlicher E-Mails auf externe E-Mail-Accounts ist unzulässig. Die Nutzung dienstlicher Mailverteiler für private Zwecke wie Spendenaufrufe, Aufrufe zu Teilnahme an Umfragen, die nicht im dienstlichen Kontext stehen, 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. Private E-Mails sollen separat von dienstlichen E-Mails gespeichert werden, private E-Mail-Ordner sollen im Ordnernamen als »privat« gekennzeichnet werden.
Eingehende Mails bergen trotz Filterung ein nicht zu unterschätzendes Risiko durch Schadsoftware. Bei verdächtigen Mails mit Links und Anhängen, auch von vermeintlich bekannten Absendern, sollten diese erst nach vorheriger Überprüfung auf Schadsoftware bzw. Rücksprache mit der Abteilung IT-Service oder dem Absender geöffnet werden. Eine Weiterleitung bzw. Verbreitung von Warnmeldungen vor Schadsoftware darf ausschließlich durch die Abteilung IT-Service erfolgen.
Größere Anhänge sollten nicht per Mail an Verteilerlisten geschickt, sondern auf einem internen Server (siehe Abschnitte »Internet- und Cloud-Dienste« und »Im Internet bereitgestellt Dienste und Daten«) bereitgestellt werden.

5 Nutzung des Netzwerks

Fremdgeräte dürfen nur mit eduroam oder einem Gästenetz verbunden werden, nicht aber mit dem institutsinternen Netzwerk. Computer, Drucker, Telefone und andere Geräte dürfen nur nach Freigabe der Abteilung IT-Service ins interne Netz integriert werden. Geräte, die ins Netzwerk integriert werden sollen, dürfen nur von autorisierten Mitarbeitern 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 Mitarbeitende zu dienstlichen Zwecken oder mit Ausnahmegenehmigung des/der Informationssicherheits-Beauftragten oder der Abteilung IT-Service zulässig.

6 Internet- und Cloud-Dienste

Firmendaten sind grundsätzlich nur auf Systemen zu speichern, die von Fraunhofer selbst betrieben werden, von der Abteilung IT-Service dafür freigegeben wurden oder von Dienstleistern, die Fraunhofer beauftragt hat (siehe Office 365). Die selbstgewählte Speicherung in öffentlichen Cloud-Diensten wie Dropbox, Google-Accounts usw. ist aufgrund von Datenschutzbestimmungen und anderen Gesetzen, Verträgen und Betriebsvereinbarungen hingegen vielfach unzulässig. Vor einer Übertragung von Firmendaten zu den Dienstanbietern sind Projektleitungen und Vorgesetzte zu fragen, die die Zulässigkeit sowie eventuelle Sicherheitsmaßnahmen abklären müssen.

Durch Dokumentation der Zugangsdaten zu dienstlichen Accounts, insbesondere zu Social Media-Accounts, und durch Meldung bei der/dem Vorgesetzten oder Projektleitungen ist sicherzustellen, dass solche Accounts zugreifbar bleiben und nicht vergessen werden, z. B. beim Wechsel der Mitarbeitenden.
Die Freigabe von internen Adressverzeichnissen für einen Betreiber zum Abgleich von Kontaktdaten 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 Künstliche Intelligenz

KI-Systeme können die Arbeit erleichtern. Es muss jedoch vermieden werden, dass bei deren Verwendung schützenswerte interne oder gar vertrauliche Daten an Diensteanbieter weitergegeben werden

oder über lernende Systeme indirekt an Dritte gelangen. Aus diesem Grund dürfen nur Fraunhofer-interne oder für bestimmte Projekte, Aufgaben oder Daten freigegebene Systeme verwendet werden. Zu beachten sind auch Urheberrechte an generierten Inhalten. Ob und in welcher Weise KI-Systeme für die Arbeit verwendet werden, ist mit dem jeweiligen Projektleitung bzw. Vorgesetzten zu erörtern. Dabei ist die Zulässigkeit für die konkreten Zwecke zu bewerten und es sind rechtliche Anforderungen aus dem AI-Act sowie innerbetrieblichen Regelungen zu beachten, wie u. a. eine Registrierungspflicht für Anbieter von KI-Systemen mit hohem Risiko. Bedacht werden muss auch die teilweise zweifelhafte Zuverlässigkeit der generierten Ergebnisse von KI-Systemen.

8 Umgang mit vertraulichen Daten

Zum Schutz der Vertraulichkeit von Daten sind die Vorgaben zur Informationsklassifizierung zu beachten. Informationen, die nicht als »Public« klassifiziert sind und keine Kennzeichnung tragen, sind als »Restricted« anzusehen. Sie sind nur den Personen zugänglich zu machen, die sie für ihre Aufgabenerfüllung benötigen und dürfen ohne Zustimmung des Informationsverantwortlichen Fraunhofer nicht verlassen, d. h. insbesondere nicht an Externe weitergeleitet oder in externen Cloud-Diensten (nicht vertraglich verpflichteter Anbieter) gespeichert werden. Als »Confidential« oder »Strictly confidential« klassifizierte Daten sind besonders zu schützen, insbesondere sind sie sichtbar zu kennzeichnen und verschlüsselt zu versenden, sofern die Abteilungs- oder Projektleitung keine strengeren Maßstäbe festgelegt hat. Als »Public« 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 *HaHi »Informationsklassifizierung«*.

9 Nutzung mobiler Endgeräte

Dienstlich genutzte Notebooks, Smartphones und Tablets erfordern gesonderte Sicherheitsvorkehrungen.[2]

- Mobile Endgeräte, die zur Bearbeitung, Verwaltung, Speicherung oder Nutzung geschäftlicher Informationen verwendet werden, müssen von der Abteilung IT-Service zentral verwaltet und überwacht werden.
- Mobile Endgeräte sind vor unberechtigtem Zugriff und Diebstahl zu schützen, siehe auch Abschnitt »Mobiles Arbeiten und Verhalten auf Reisen«.
- Bei Geräteverlust ist die Abteilung IT-Service umgehend zu informieren. Nach Möglichkeit wird dann ein Fernlöschen durchgeführt und eine Diebstahl-/Verlustanzeige aufgegeben.

Besonders für Smartphones und Tablets relevant (z.B. Geräte mit Android, iOS oder iPadOS):

- Soweit die Abteilung IT-Service die Sicherheitseinstellungen nicht fest vorgegeben eingestellt hat, muss die Nutzerin bzw. der Nutzer diese selbst vornehmen.
  - Die Geräte sind mit einer PIN-Sperre/Passwort-Sperre (mindestens 6 Zeichen lang) zu konfigurieren. Diese Sperre muss bei Nichtbenutzung automatisch aktiv werden, vorzugsweise nach 2 Minuten, spätestens nach 10 Minuten.
  - Die Geräte müssen so konfiguriert sein, dass sie alle Informationen löschen, wenn mehrfach ein falscher Code eingegeben wurde. Zulässig sind maximal 10 Fehleingaben.

[2] Für Test- und Entwicklungsgeräte können abweichende Vorgaben vereinbart werden.

- Sicherheitsfunktionen der Betriebssysteme dürfen nicht außer Kraft gesetzt werden. Eingriffe wie »jailbreak« oder »rooten« sind verboten.
- Die Änderung der SIM-PIN muss umgehend an den Institutseinkauf gemeldet werden.
- Bei Ausscheiden oder Benutzerwechsel müssen persönliche Informationen vom Gerät entfernt werden. Dazu zählt vor allem das Löschen des Apple Account um auch die Gerätesperre (Wo ist?) zu deaktivieren. Dies kann durch die Nutzerin oder den Nutzer persönlich oder zusammen mit der Abteilung IT-Service passieren. Die Geräte werden dabei auf Werkseinstellungen zurückgesetzt. Der Institutseinkauf muss die Information über das Ausscheiden erhalten, um ggf. vertragliche Bedingungen zu ändern oder zu kündigen.
- Wird ein mobiles Endgerät durch ein neues ersetzt, muss das alte bei der Abteilung IT-Service umgehend abgegeben werden. Die Abteilung IT-Service stellt sicher, dass das alte Gerät entsprechend zurückgesetzt und/oder entsorgt wird. Soll das Gerät für Forschungszwecke oder als Zweitgerät weitergenutzt werden, muss der Institutseinkauf informiert werden.
- Zum besseren Schutz betrieblicher Daten wird auf den Geräten in der Regel eine Container-App installiert (SecurePIM).
  Bei geöffnetem Container darf das Gerät nicht an Dritte ausgehändigt werden.
  Aus dem Container darf mit der folgenden Ausnahme kein Datenexport erfolgen: Um Anrufer zu identifizieren, ist der Export von Name und Telefonnummer zulässig.
  Der Zugriff auf E-Mail- bzw. Groupware-Systeme darf nur über die Container-App erfolgen. Ein direkter Zugriff auf den Exchange-Server über Mittel des Betriebssystems ist nicht zulässig.
- Betriebliche Daten, insbesondere Adressbücher und E-Mails, dürfen nicht bei externen Diensten unverschlüsselt gespeichert oder über die Cloud des Herstellers unverschlüsselt synchronisiert werden.
- Anwendungen dürfen nur aus den App-Shops der Gerätehersteller oder anderen von der Abteilung IT-Service als vertrauenswürdig eingestuften Quellen bezogen werden. Die Abteilung IT-Service behält sich vor, einzelne als eindeutig schädlich erkannte Apps zu blockieren.
  Bei der Installation von Anwendungen (»Apps«) auf Mobilgeräten ohne Container-App ist besondere Sorgfalt geboten, da viele Apps Daten auslesen und ins Internet übertragen.

9.1 Private Mitnutzung

- Die Nutzung von dienstlichen Smartphones sollte ausschließlich in dienstlichem Interesse erfolgen. Findet darüber hinaus auch eine zulässige Privatnutzung statt, so kann diese abrechnungspflichtig sein. Details, siehe Abschnitt »Abschluss, Verlängerung und Kündigung von Mobilfunk- oder Datenverträgen«.
- Die Genehmigung für private Mitnutzung gilt nur für Mitarbeitende und erstreckt sich nicht auf Familienangehörige, Freunde oder andere Dritte.
- Das Einrichten zusätzlicher privater E-Mail-Konten auf den Geräten ist zulässig. Es muss für eine Trennung von privaten und dienstlichen Konten gesorgt werden (z.B. Container-App), damit dienstliche E-Mails nicht versehentlich über ein privates E-Mail-Konto verschickt werden.
- Private Termine und private Kontakte dürfen auf dem Gerät gespeichert und mit dem Exchange-Server des Institutes synchronisiert werden.
- Private Daten (Bilder, Musik, z.B. MP3) dürfen auf dem Smartphone gespeichert werden, wenn deren Besitz oder Nutzung nicht gegen urheberschutzrechtliche Bestimmungen verstoßen.
- Anwendungen für private Zwecke dürfen unter der Beachtung besonderer Sorgfalt installiert und genutzt werden, wenn dadurch die dienstliche Nutzung des Gerätes nicht beeinträchtigt wird und kein höheres Risiko entsteht.

- Bei Diebstahl, Verlust oder begründetem Missbrauchsverdacht kann ein Fernlöschen (»Remote Wipe«) durchgeführt werden: Hierbei werden alle Daten vom Gerät gelöscht. Die Nutzerinnen und Nutzer sind für ein regelmäßiges Backup selbst verantwortlich, das Institut haftet nicht für den Verlust privater Daten! Backups dürfen nicht bei Cloud-Dienstleistern gespeichert werden, sondern sind verschlüsselt auf lokalen Datenträgern abzulegen.
- Smartphones dürfen auch im privaten Umfeld und auf privaten Reisen mitgeführt werden. Tablets und Notebooks dürfen nur bei nachgewiesener besonderer dienstlicher Notwendigkeit auf privaten (Auslands-) Reisen mitgeführt werden. Voraussetzung hierfür ist eine vorherige Prüfung durch die Exportkontrolle, die auf Anfrage des Reisenden erfolgt. Mitarbeitende und Gruppenleitungen müssen vor der Anfrage die dienstliche Notwendigkeit von ihrer Abteilungsleitung bestätigen lassen. Abteilungs- und Bereichsleitungen können die Exportkontroll-Prüfung direkt anfragen. Details, siehe auch *HaHi »Exportkontrolle*«.
  Bei Auslandsreisen sind mögliche Roaming-Gebühren zu beachten und ggf. die Internetverbindung zu deaktivieren. Die Regelungen in Abschnitt »Mobiles Arbeiten und Verhalten auf Reisen« gelten sinngemäß auch für die Mitnahme von Geräten auf private Reisen.

9.2 Maßnahmen im Notfall

Smartphones haben ein besonders hohes Verlustrisiko. Dieses Problem wird dadurch verschärft, dass auf Smartphones kritische Daten gespeichert sind. Dazu zählen insbesondere Credentials (Passwörter) für den Zugang zu den Ressourcen des Instituts. Als Abwehrmöglichkeit sind die Geräte dazu mit einer Fernlösch-Option (»Remote-Wipe«) ausgestattet. Über die Funktionsweise der Fernlösch-Option muss sich der Mitarbeiter bereits bei der Inbetriebnahme des Gerätes informieren.

- Bei Verlust des mobilen Endgerätes oder bei Verdacht von Missbrauch durch Fremde (z.B. Installation von Schadsoftware) ist umgehend das Institut zu informieren und, soweit möglich, eine Fernlöschung auszulösen. Die Meldung wird zu üblichen Geschäftszeiten unter der Nummer 09131 776 2777 von der Hotline der Abteilung IT-Service entgegengenommen, die dann die notwendigen Maßnahmen einleitet. Wenn die Hotline nicht erreicht werden kann, ist zumindest eine Sperrung der SIM-Karte und das Deaktivieren der WLAN/Internetverbindung (Flugmodus) vom Nutzenden zu veranlassen.
- Gemeinsam mit dem/der Informationssicherheits-Beauftragten und der Abteilung IT-Service ist eine Aufklärung des Schadens durchzuführen, insbesondere sind Datenverluste zu benennen und mögliche Zugriffe Fremder auf Institutsdaten zu ermitteln. Alle Benutzerkennwörter und PINs sind zu ändern.

9.3 Hinweise zu Maßnahmen der Systemadministration

Die Änderung des Codes der Zugangssperre aus der Ferne ist nur bei Gefahr im Verzug auf Wunsch der Nutzerin oder des Nutzers zulässig.
Das Fernlöschen des Geräts durch die Abteilung IT-Service ist nur unter den folgenden Randbedingungen zulässig:

- Verlust des Gerätes nach Anzeige durch oder auf Wunsch der Nutzerin bzw. des Nutzers
- bei begründetem Verdacht auf Missbrauch
- bei begründetem Verdacht auf Schadsoftware-Befall des Gerätes, nach folgendem Ablauf:
  - Wenn möglich Vorabinformation der Nutzerin bzw. des Nutzers, Dokumentation des Kontaktversuchs
  - Dokumentation der Gefahrensituation und der Entscheidung für die Fernlöschung

- Information der Nutzerin bzw. des Nutzers über die erfolgte Löschung unter Vorlage der Dokumentation

Eine Ortung von mobilen Geräten ist nur im Ausnahmefall zulässig. Dabei gelten folgende Regeln:

- Soll eine Ortung von mobilen Geräten erfolgen, so sind die Nutzerinnen und Nutzer vorab hierüber zu informieren und es muss eine konkrete Zweckbestimmung (z. B die Ortung des Gerätes bei Verlust) vorliegen.
- Nur bei Gefahr für Leib und Leben (z.B. die Ortung im Ausland via International SOS im Fall von Katastrophen oder in Hochrisikogebieten.) ist die Fernaktivierung der Ortungsfunktion ohne vorheriges Einverständnis des Users zulässig.

9.4 Abschluss, Verlängerung und Kündigung von Mobilfunk- oder Datenverträgen

Die *»GBV über den Einsatz von Mobiltelefonen (V. 1.1)«* regelt die Festlegung von Abläufen und Verantwortlichkeiten in Zusammenhang mit der Bereitstellung und Kostenübernahme bei mobilen Kommunikationsgeräten (in der GBV Mobiltelefone genannt) und Nutzung eines dienstlichen Mobilfunkvertrages in der Fraunhofer-Gesellschaft.
Die zentrale Beschaffung der notwendigen Endgeräte und der dienstlichen Mobilfunkverträge unterliegt ausschließlich dem Institutseinkauf. Nur dieser darf im Auftrag der Verwaltungsdirektion Kommunikationsverträge (in der GBV dienstliche Mobilfunkverträge genannt) abschließen, anpassen oder verlängern. Grundsätzlich gilt, dass die Bereitstellung von Kommunikationsgeräten in Art und Umfang in Abstimmung mit der/dem Budgetverantwortlichen bzw. der/dem Vorgesetzten unter Berücksichtigung von Wirtschaftlichkeitsaspekten festzulegen sind.
Im Intranet findet sich eine Aufstellung der zur Verfügung stehenden dienstlichen Mobilfunktarife, Laufzeiten, Kündigungsfristen und Bedingungen der privaten Mitnutzung
(https://intern.iis.fhg.de/x/3hyWBQ).
Des Weiteren bieten wir eine Übersicht der mobilen Endgeräte, unserem präferierten Standardmodell (bestes Preis-/Leistungsverhältnis) und dazugehörigen Bestell-Link (https://intern.iis.fhg.de/x/BWAsN) an.

Aufstellung von freizugebenden Ausnahmen:

- Eine Rufnummernportierung von privaten zu geschäftlichen Verträgen ist nur nach Freigabe durch den Institutseinkauf möglich.
- Eine Rückportierung der privaten Rufnummer bedarf der Freigabe des Vorgesetzten und der Verwaltungsdirektion.
- Die Portierung von geschäftlichen Altverträgen zu privaten Neuverträgen ist generell nicht möglich.
- Das dienstlich beschaffte Endgerät bleibt Eigentum der Fraunhofer-Gesellschaft, ist bei Ausscheiden des Mitarbeitenden zwingend abzugeben und kann nicht privat übereignet werden.
- Eine Abweichung von unseren vorgegebenen Standardverträgen und Standardmodellen muss begründet und von der Abteilungsleitung und Verwaltungsdirektion (ab 1.000 EUR netto) freigegeben werden.

10 Nutzung eigener Hardware

Die Nutzung nicht von der Fraunhofer-Gesellschaft bereitgestellter, insbesondere privater Hardware (auch Kameras, USB-Sticks) zu betrieblichen Zwecken der Fraunhofer-Gesellschaft (»Bring Your Own Device«, BYOD) erfolgt nur nach Genehmigung durch die Abteilung IT-Service und Rücksprache mit dem/der Informationssicherheits-Beauftragten des Instituts.

Die Nutzung privater Geräte kann weder vom Nutzenden noch von der Fraunhofer-Gesellschaft verlangt werden. Betriebliche Daten sind von privaten zu trennen und besonders zu schützen. Familienangehörige und andere Personen dürfen auf betriebliche Daten nicht zugreifen können. Beim Ausscheiden aus der Fraunhofer-Gesellschaft sind betriebliche Daten zu löschen, sofern mit der Projekt- bzw. Abteilungsleitung nichts anderes vereinbart wurde.

Der Abteilung IT-Service ist die Kontrolle von Sicherheitseinstellungen zu gestatten. Für die Fraunhofer-Gesellschaft besteht die Möglichkeit der Einsichtnahme auf dienstliche Daten des Geräts im Notfall oder bei Missbrauchsverdacht, gemäß der Regeln der GBV »IT-Grundsätze«. Falls bei Fernlöschung oder Fernzugriffen private Daten unabsichtlich gelöscht werden, besteht kein Schadensersatzanspruch.
Vollzugang zum internen Institutsnetz ist nur möglich für Geräte, die vollständig von der Abteilung IT-Service administriert werden und allen Sicherheitsanforderungen entsprechen.
Sofern BYOD für Smartphones oder Tablets gestattet wird, gelten die Bestimmungen des Abschnitts »Nutzung mobiler Endgeräte«. Die von der Abteilung IT-Service bereitgestellte Container-App ist dann verpflichtend zu verwenden. Dies ermöglicht einen eingeschränkten Zugang (z.B. nur Kalender und Mail) zum internen Institutsnetz. Voraussetzung ist ein als ausreichend sicher eingestuftes Endgerät, dessen Sicherheitsstatus anhand der Aktualität des Betriebssystems bewertet wird.
Software des Instituts darf nur in Einzelfällen und nach Genehmigung durch die Abteilung IT-Service auf eigener Hardware eingesetzt werden. Eventuelle Einschränkungen in der Art und Dauer der Nutzung sind einzuhalten.
Die Nutzung von Microsoft Teams (mit dem Fraunhofer Account) ist auf privaten Geräten nicht erlaubt.

11 Mobiles Arbeiten und Verhalten auf Reisen

Die Nutzung von IT-Diensten außerhalb der betrieblichen Arbeitsplätze, beispielsweise am Heimarbeitsplatz oder 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 oder durch Einschließen. Auf Reisen ist gegebenenfalls jemand zu bitten, auf das Gerät kurz aufzupassen. Bei längerer Abwesenheit oder im Hotel sind Geräte ganz auszuschalten (Herunterfahren). Die Hinterlegung im Hotel-Safe oder zumindest in einem separat verschließbaren Objekt wird empfohlen, sofern die Endgeräte unbeaufsichtigt im Hotel verbleiben. Bei Auslandsreisen ist eine Risikoabwägung zu treffen. Ggf. ist ein gesondertes Reisegerät zu verwenden, das nur die für das Dienstgeschäft benötigten Daten enthält (siehe gesondertes Angebot der Abteilung IT-Service). Dies gilt insbesondere für Reisen in Risikoländer. Das Merkblatt Auslandsreisen und die *HaHi »Dienstreise«* sind zu beachten.
Folgende Fälle müssen unverzüglich (mit Gerätenamen) der Abteilung IT-Service oder der Informationssicherheit gemeldet und die Hinweise beachtet werden:

- Das Gerät musste im nicht vollständig heruntergefahrenen Zustand (oder sogar unverschlüsselt) unbeaufsichtigt an Dritte (z.B. Zollbeamte etc.) ausgehändigt werden oder wurde inspiziert (Berechtigter Zugriff Dritter).
  → Das Gerät darf erst nach Freigabe durch die Abteilung IT-Service wieder am Institutsnetz betrieben werden (auch VPN-Zugang).
- Geräteverlust (verloren, gestohlen etc.) → Bei Diebstahl zusätzlich Anzeige bei der Polizei.
- Verlust von SIM-Karten.
  → Karten sofort beim Netzbetreiber sperren lassen. Bei Diebstahl zusätzlich Anzeige bei der Polizei.

12 Datensicherung

Backups erfolgen durch die Fraunhofer-Gesellschaft oder durch deren Einrichtungen, jedoch nicht von privaten Datenspeichern der Nutzenden. Aus diesem Grund werden Projektdaten und andere wichtigen Dokumente grundsätzlich in einer mit dem Projektleiter abgesprochenen Struktur auf den Institutsservern gespeichert. Nutzende 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. Die Nutzerin bzw. der Nutzer muss dann in Rücksprache mit der Abteilung IT-Service und dem Vorgesetzten selbst für eine geeignete Datensicherung sorgen und ist für diese verantwortlich.
Wird längere Zeit auf einem Computer ohne Serverkontakt gearbeitet, sind von wichtigen Dateien verschlüsselte, lokale Sicherheitskopien zu erstellen (z.B. auf USB-Stick oder externen Datenträgern). Die *HaHi »Informationsklassifizierung«* ist zu beachten.

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. Projektergebnisse sowie die zu ihrer Nachvollziehbarkeit erforderlichen Daten müssen unter Umständen länger aufbewahrt werden. Die Ablage administrativer Daten (insbesondere Verträge, Geschäftsbriefe) erfolgt zeitnah in der zum Projekt bzw. der Abteilung gehörenden Projektablage/bzw. Akte. Andere Daten (z. B. Projektinhalte) werden entsprechend den institutslokalen Regelungen evtl. auch anders archiviert. Die Projekt- und Abteilungsleitungen informieren über anzuwendende Regeln und Verfahren.

14 Rückgabe von Betriebsmitteln und Übergabe von Daten beim Ausscheiden

Nutzerinnen und Nutzer haben vor ihrem Ausscheiden aus der Fraunhofer-Gesellschaft alle erhaltenen Betriebsmittel der Organisation, wie zum Beispiel Smartphones, Notebooks, tragbare Speichergeräte, sowie Projektergebnisse und andere dienstliche Daten, entsprechend den zuvor genannten Regeln für die Weiterarbeit zu übergeben und in den vorgesehenen Projektakten oder Ablagen zu speichern sowie ihre privaten Daten auf den Fraunhofer-Speichermedien zu löschen. Da eine zielgenaue Selektion und Übergabe insbesondere bei E-Mails mitunter nicht gelingen, 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 Betriebsrat 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, eingehende E-Mails mit einer Autonachricht abgelehnt und später gelöscht.

15 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 Abteilung IT-Service 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 Ansprechpartner ist auch für eine zeitnahe Reaktion bzw. Abhilfe bei bekanntwerdenden Sicherheitslücken der betriebenen Plattform zuständig.
Die Beantragung und Reservierung von Internet-Domains dürfen ausschließlich über die Abteilung IT-Service erfolgen.

16 Entsorgen von Datenträgern

Die zu Entsorgung bzw. Vernichtung von Datenträgern erforderlichen Maßnahmen richten sich nach der Schutzklasse der darauf enthaltenen Daten und sind in der *HaHi »Informationsklassifizierung«* formuliert. Einfaches Löschen ist unzureichend!
Nicht mehr benötigte Datenträger (wie CDs, DVDs, USB-Sticks) oder Geräte mit eingebauten Speichern können unter Hinweis auf die Schutzklasse der gespeicherten Daten bei der Abteilung IT-Service zur Löschung bzw. Vernichtung abgegeben werden.

17 Schutz vor Schadsoftware

Jeder Computer wird durch eine von der Abteilung IT-Service vorgegebene Endpoint Protection (Virenscanner) geschützt.
Die Aktualisierung des Betriebssystems, der Standardprogramme und der Endpoint Protection (Virenscanner) wird von der Abteilung IT-Service aktiv betrieben. Das Behindern oder Deaktivieren der Aktualisierungen oder des Scans auf Schadsoftware (Malware) ist unzulässig.
Bei Verfügbarkeit von sicherheitsrelevanten Aktualisierungen sind diese spätestens nach Aufforderung durch die Abteilung IT-Service zeitnah zu installieren. Hierzu müssen die Geräte mindestens einmal monatlich für zumindest einige Stunden Kontakt mit dem IIS-Netzwerk haben. Geräten mit veraltetem Betriebssystem wird der Zugang entzogen.
Auf Geräten, die direkten Zugang zum Internet haben können (also ohne die Firewall des Institutsnetzes), ist eine »Personal Firewall« einzusetzen. Auswahl, Installation und Konfiguration dieser Firewall erfolgt durch die Abteilung IT-Service.

18 Bearbeitung und Speicherung personenbezogener Daten, Auftragsdatenverarbeitung

Vor der Verarbeitung oder Speicherung personenbezogener Daten sind besondere Schutzkonzepte zu erstellen. Hierzu müssen rechtzeitig vor Projektbeginn die Datenschutzansprechperson und die Abteilung IT-Service einbezogen werden. Alle Datenschutzbestimmungen sind strikt einzuhalten.
Werden externe Dienstleister mit der Verarbeitung personenbezogener Daten betraut, ist (unter Einbeziehung von Institutseinkauf und der Gruppe Recht) eine separate Vereinbarung zur Auftragsdatenvereinbarung abzuschließen.

Kenntnisnahme und Anerkennung der IT-Benutzungsordnung der Fraunhofer-Gesellschaft

- for the English version of the IT-Terms of Use, please see below -

Bitte Online, sonst Formularkopf handschriftlich in GROSSBUCHSTABEN ausfüllen!

Institutsnummer / institute No	Institutskürzel / Institute short name	Personalnummer / Personnel number (sofern vorhanden)
Vorname / First name		Name / Last name

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

Ich erkläre hiermit, die Bestimmungen dieser IT-Benutzungsordnung (ITBO) 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.

English Translation:

I hereby declare that I have read and understood the provisions of this IT Usage Policy (ITBO) and its appendix and undertake to comply with them.
If I use the Fraunhofer-Gesellschaft's IT for private purposes, I expressly consent to the conditions of private use according to section IV of this ITBO.
Unless I am an employee of the Fraunhofer-Gesellschaft, but rather another external user, the obligations and regulations stipulated in the IT Usage Regulations also apply to me accordingly. However, rights described in the IT Usage Regulations for employees, such as those for private use, do not apply to me for legal reasons.

Disclaimer: The english translation of the declaration above and the english version of the policy (»IT terms of use«) is to be used as a reading version for information purposes only. It is neither a self-contained nor a legally binding document. In the event of any inconsistency between the German version and the English version, the German version shall prevail.

Ort und Datum / place and date

Unterschrift oder el. Signatur / signature or electr. signature

IT Terms of Use

Version 3.0

These IT Terms of Use (hereinafter referred to as "ITBO") contain basic rules for using the IT systems, services and data of Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V. (hereafter referred to as "Fraunhofer-Gesellschaft" or "Fraunhofer"). They are aimed at all users of Fraunhofer IT, including external parties who receive access to the Fraunhofer intranet on an exceptional basis. The obligations set out in this ITBO apply to everyone; the rights, especially those to private use, are limited to employees of the Fraunhofer-Gesellschaft.

I. Objectives

This ITBO serves:

- to ensure information security and data protection,
- to protect IT and the personal rights of users,
- to observe laws and contracts vis-à-vis project and business partners, and
- to protect intellectual property.

For this purpose, the ITBO:

- informs users about the general terms related to IT use,
- requires them to observe these terms and
- makes measures for logging and monitoring IT use and for processing personal data resulting from IT use clear.

Important IT-related rules that are relevant to all users from internal regulations on information security and the relevant central works council agreement are taken into account.[3]

II. General terms of use

The following terms apply to all types of IT use:

- To support scientific work, the Fraunhofer-Gesellschaft grants the users of its IT great freedom in their IT use. Many aspects of IT use are not regulated in detail but are set out generically and are not enforced with technical measures. Therefore, users are bound to act and think in a risk-conscious and responsible manner that promotes the objectives of this ITBO.
- Any IT use for extremist, racist, pornographic, or criminal purposes is prohibited.
- Any IT use and information processing that violates applicable law (e.g., personal rights or copyright laws), compromises IT security, or damages the reputation of the Fraunhofer-Gesellschaft is also forbidden.
- Users generally have personalized user accounts on workplace computers, personalized email accounts, and personal data storage on other systems (known as the "personal area"). Fraunhofer only accesses the data stored there in cases of emergency or suspected abuse in accordance with the regulations of the central works council agreement "IT Principles."

[3] Central works council agreement Principles of IT Use as well as the internal regulations Information Classification and Information Security

- Fraunhofer IT is to be primarily used to fulfill work-related tasks. Private use is allowed to employees insofar as there are no disadvantageous effects on the IT and provided that this does not result in additional requirements for Fraunhofer. Conditions for private use can be found in section III.
- The Fraunhofer-Gesellschaft neither offers nor assumes a guarantee, warranty, or liability for the continuous availability or freedom from defects of the IT. Moreover, it may completely or partially modify, limit, or end IT services and prohibit their use at any time.
- Users can neither apply for nor assert patents, brands, or other rights (for themselves or third parties) for project or domain names, expertise, and other information that belongs to or can be attributed to Fraunhofer or its business partners unless the rights holders have given their written consent.
- The terms of licenses for software and services, including cloud services, and those that apply to the use of content such as images and texts must be observed. License keys and rights must not be passed on to others or used otherwise without permission from the Fraunhofer-Gesellschaft.
- Information is to be classified and protected with regard to the level of protection it requires in accordance with the internal regulation on information classification and with external regulations. Project managers or managers decide how these rules are to be implemented in their respective area of responsibility.
- Identified or suspected security vulnerabilities or information security / data protection incidents must be reported without delay. Unless otherwise specified at the local level, these must be reported to the Fraunhofer ServiceDesk (email: servicedesk@fraunhofer.de, phone: +49 2241-14-1414).
- Instructions on the use of internal services as well as emails, announcements, and other information regarding IT use are to be observed. Upon introduction of new services or in the event of doubt, users need to proactively check whether there are specific rules for IT use.
- In keeping with the rules that apply at their institute, users must participate at least once annually in awareness and training measures on the topic of information security and should also observe current security information.

III. Terms of private use

The Fraunhofer-Gesellschaft assumes that prohibiting private use of IT in research is not productive and that entirely separating work-related and non-work-related use is virtually impossible owing to various factors, including the close collaboration that exists with universities. For that reason, employees of the Fraunhofer-Gesellschaft are permitted to engage in non-work-related use subject to the following conditions:

- No additional requirement or risk of liability for the Fraunhofer-Gesellschaft may result from the private use of IT. The security and functionality of IT services must not be impaired by private use. Possible legal restrictions or requirements from clients are to be observed.
- Users are not entitled to operate private devices using work-related internet access or to install software for private use on work-related devices. Such use requires permission from the manager and the head of the IT department.
- Data storage, administration, logging, monitoring of data traffic, troubleshooting, deleting data, and setting up devices take place according to operational requirements and without specific consideration of private use. There is no individual right to exclude private data from data storage or private connections from logging and data analysis admissible for work-related data. There is no claim for private data to be backed up or recovered.

- For reasons of provisions related to funding, private use is limited to occasional use. Use for private business purposes is not permitted.
- Work-related email addresses, social media accounts, and other work-related addresses should not be used publicly as contact addresses for private communication. Private data should be saved in a personal area and labeled as private.
- For operational reasons, private use may be restricted or prohibited in cases of special security requirements.

IV. Logging and monitoring

Within the scope of IT operations, personal data concerning users is processed in order to enable operation and ensure the security thereof. This data may include private data from permitted private use.

- Work-related and private emails suspected of containing malicious code, viruses, or spam may be quarantined at the discretion of the Fraunhofer-Gesellschaft or deleted centrally.
- Authorized staff may analyze personal data resulting from IT use for purposes of system administration, such as for analyzing and removing system errors, ensuring IT security, operational security, and information security, and supporting maintenance.
- This also applies to preventing cyberattacks. In certain cases, a forensic examination of the systems may be carried out. Data from the operating system and related software, traffic data from internet services, and tool-related data can be logged and may contain personal data, which may be examined to prevent or analyze cyberattacks. The log data is usually deleted after 30 days.

V. Changes to the IT Terms of Use and entry into force

The Fraunhofer-Gesellschaft may change or amend this ITBO at any time, in particular in the interest of its operational procedures and of information security. This ITBO replaces the previous ITBO version 2.0 and enters into force with its announcement. The announcement is made in a suitable manner, e.g., via hard-copy distribution, email, or publication on the intranet. The same applies to future changes or amendments to the ITBO. Notwithstanding this, a change or amendment shall be deemed approved with respect to users who are not employees of the Fraunhofer-Gesellschaft if no objection is raised within one month of notification of the change or amendment, or if Fraunhofer IT continues to be used after the end of the objection period. This will be pointed out on announcement of the change or amendment. In case of an objection, the right of use may be withdrawn.

Annex: Supplementary Information on Implementation

Version IIS-03 (16.07.2026)

The Fraunhofer-Gesellschaft has rules that apply to all users in order to ensure appropriate protection, use, and handling of information and other associated assets. As much as they possibly can, users must take all measures to minimize risks to Fraunhofer and promote the objectives of the ITBO.
As a general rule, everyone has a duty to use resources sparingly, to be mindful of storage space on servers and in backups, to maintain a healthy scepticism, and to exercise caution when using the internet, email and computers in general. If in doubt, the IT-Service Department will be happy to help. In the long term, information security can only be achieved through a relationship of trust between users and the IT administration team.

All users are required to read the notices published on the intranet by the IT-Service Department or the Information Security on a regular basis and to follow any instructions contained therein without delay.
Attendance at the annual security training sessions is also mandatory; please refer to the *Guideline 'Instruction regarding information security'*.

The most important measures are summarized below. Taking into account works council agreements and other regulations, department heads or project managers make decisions about specific exceptions in consultation with the information security officer.

Note
Central Works Council Agreements (**GBV**) and Organizational Instructions (**OrgA**) can be found in the Fraunhofer Regulations Database:

- https://fraunhofer.sharepoint.com/sites/fraunhofer-recht/SitePages/Regelungsdatenbank.aspx

For further information on the specific regulations at Fraunhofer IIS, see also

- Guidelines (**HaHi**): https://intern.iis.fhg.de/x/VRyWBQ
- Intranet, section Information Security: https://intern.iis.fhg.de/x/l7o1C

1 Securing devices

Access by unauthorized persons to IT systems at the workplace, IT services, or data carriers and their data must be prevented. Smartcards are to be locked away or kept on one's person. Computers must be locked even in cases of brief absence; in cases of extended non-use, they must be shut down. Offices should be locked when unoccupied. Endpoint Protection (Virus scanners) and other security measures must not be circumvented.
Mobile devices and devices that need to leave the premises must be encrypted using state-of-the-art encryption technology.

2 Passwords and certificates

Passwords (and other credentials such as PINs) are usually bound to a specific person and may not be passed on to third parties. Exceptions to this include shared accounts (e.g., see the section "Internet and Cloud Services"), functional accounts, and the transfer of accounts upon termination of employment or pursuant to a special agreement. Passwords must be secure and be kept secret. Official passwords must

not be used for private purposes. Passwords used for work purposes must not be entered on personal devices or other third-party devices, with the exception of services that have been explicitly approved for use on non-work devices, such as the Container App, WebVPN, and Webmail accessed from a personal computer (but not from computers controlled by third parties, e.g. at an internet café!) or in absolute emergencies. Passwords that are used for internal services may not be used for external or internet services as well. Smartcards and personal electronic keys or certificates must be treated as confidential and not shared with others. The same applies to the corresponding PINs. Use of password manager software is strongly recommended in order to facilitate compliance with the above requirements.
If you suspect that a password has been compromised, you must change it immediately. Guidance on creating secure passwords can be found on the Intranet, section Information Security.
If passwords for services used by Fraunhofer IIS on the Internet (e.g., Facebook, YouTube, Dell device management) become known to individuals outside of IIS (including former employees), they must be changed as soon as possible.

3 Software installation

New software may only be used with the approval of the IT-Service Department unless it is authorized software from internal sources. The software license must cover use thereof by the Fraunhofer-Gesellschaft for work-related, not only for private purposes. Should a user be asked by the IT-Service Department to perform an installation manually, they should do so in a timely manner. Where users, such as those who work at developer workstations, receive administration rights on an exceptional basis and are permitted to install software themselves, they must observe special security rules pointed out to them by the IT administration (including installation of patches and updates). Software may only be obtained from trustworthy sources, and updates must always be installed promptly or, if possible, automatically. This applies in particular to security-related updates (updates, patches, hotfixes) addressing security vulnerabilities.
Software that clearly allows access to institutional resources from the Internet must be approved by the IT-Service Department! This applies in particular to services made available to external users via the Internet (e.g., web servers, TeamViewer, or GitLab Runner)—for more details, see the section "Services and data made available on the Internet". Programs that may uncontrollably transmit data to unknown destinations on the Internet must not be installed.
Downloading and making available files that may be protected by copyright (e.g., file sharing, peer-to-peer networks) is prohibited; such programs may neither be installed nor used. It is prohibited to possess, use, or distribute software with removed copy protection or programs designed to circumvent copy protection measures. The use of programs to determine normally hidden license information (e.g., serial numbers or access codes) and the disclosure of such information to third parties are not permitted.

4 Email use

The Fraunhofer email address is to be used for work related to the Fraunhofer-Gesellschaft. Automatically forwarding work-related emails to external email accounts is prohibited. The use of work email lists for personal purposes—such as appeals for donations, requests to participate in surveys that are not work-related, or the dissemination of political or other opinions—is prohibited. Fraunhofer email addresses may only be published in a work-related context. Personal use of work email addresses is permitted but should be avoided. Private emails should be stored separately from work-related emails, and private email folders should be designated as "private" in the folder name.

Despite filtering, incoming emails pose a risk of malware that should not be underestimated. Suspicious emails containing links or attachments—even those from seemingly familiar senders—should not be opened until they have been checked for malware or until you have consulted with the IT-Service Department or the sender. Only the IT-Service Department is authorized to forward or distribute malware warnings.
Large attachments should not be sent via email to distribution lists but should instead be made available on an internal server (see sections "Internet and Cloud Services" and "Services and data made available on the Internet").

5 Network use

External devices may only be connected to eduroam or a guest network but not to an internal network of the institute. Computers, printers, phones, and other devices may only be integrated into the internal network following permission from the IT-Services Department. Devices that need to be integrated into the network may only be configured by authorized employees or in accordance with their specifications. Unauthorized changes to the network configuration, as well as the installation of Wi-Fi access points, switches, and other network components, are prohibited. Programs that monitor network traffic may only be used by explicitly authorized employees for work-related purposes or by those with exemption authorization from the information security officer or the IT-Service Department.

6 Internet and cloud services

Company data may only be stored on IT systems that are operated by Fraunhofer itself, which have been approved by the IT-Service Department or by service providers commissioned by Fraunhofer (see Office 365). Saving company data in public cloud services like Dropbox, Google accounts, and so on is prohibited in many cases according to data protection regulations and other laws, contracts, and works council agreements. Prior to the transfer of company data to service providers, project managers and managers must be consulted, who will then decide whether such transfer is permissible and whether security measures are to be taken.

Users must ensure that such accounts remain accessible and their credentials are not forgotten (e.g., when they leave the department) by noting the credentials for work-related accounts, particularly for social media accounts, and reporting them to their manager or the project manager. Synchronizing internal address directories with external services is prohibited.
Websites with content that is suspected or known to be illegal should be avoided. To prevent the unintended automatic installation of malicious software when visiting websites, active content should be blocked as selectively as possible using appropriate browser settings and browser plugins. Instructions on how to do this can be found on the IIS intranet.

7 Artificial intelligence

AI systems can make people's work easier. However, when they are used, care must be taken to ensure that no internal — or worse, confidential — data requiring protection is shared with service providers or indirectly reaches third parties via systems that are capable of learning. For this reason, only internal Fraunhofer systems or systems approved for certain projects, tasks, or data may be used. Copyright to generated content must also be observed. Whether AI systems can be used for work and if so, how, must be discussed with the relevant project manager or manager. The admissibility of AI must be assessed for the specific purposes. Legal requirements from the AI Act and internal regulations, including

the registration requirement for providers of high-risk AI systems, must also be met. The fact that AI-generated output is not always reliable must also be taken into account.

8 Treatment of confidential data

To protect the confidentiality of data, the provisions on information classification are to be observed. Information that is not classified as "Public" and is unlabeled should be viewed as "Restricted." This information may only be made accessible to people who need it in order to perform their tasks and must not leave Fraunhofer without the consent of the information controller, meaning in particular that it must not be forwarded to external parties or stored in external cloud services (providers not under contract with Fraunhofer). Moreover, data classified as "Confidential" or "Strictly confidential" must be given special protection. In particular, it must be visibly labeled and sent with encryption unless the department head or project manager has set stricter standards. Data classified as "Public" is not subject to these limitations; however, any existing rights of third parties, such as copyrights, must be observed prior to distribution. The project manager and the department head provide information about further requirements and exceptions. Details are governed by the *HaHi* "*Information Classification*".

9 Use of mobile devices

Notebooks, smartphones, and tablets used for work-related purposes require special security measures.[4]

- Mobile devices used to process, manage, store, or access business information must be centrally managed and monitored by the IT-Service Department.
- Mobile devices must be protected against unauthorized access and theft; see also the section "Remote work and conduct when traveling".
- If a device is lost, the IT-Service Department must be notified immediately. If possible, a remote wipe will then be performed and a theft/loss report filed.

Particularly relevant for smartphones and tablets (e.g., devices running Android, iOS, or iPadOS):

- Unless the IT-Service Department has preconfigured the security settings, the user must configure them themselves.
    - Devices must be configured with a PIN lock or password lock (at least 6 characters long). This lock must activate automatically when the device is not in use, preferably after 2 minutes, and no later than 10 minutes.
    - Devices must be configured to delete all information if an incorrect code is entered multiple times. A maximum of 10 incorrect entries is permitted.
- Operating system security features must not be disabled. Interventions such as "jailbreaking" or "rooting" are prohibited.
- Any change to the SIM PIN must be reported immediately to the Institutional Procurement.
- Upon termination of employment or a change of user, personal information must be removed from the device. This includes, above all, deleting the Apple ID to also deactivate the device lock (Find My). This can be done by the user personally or in collaboration with the IT-Service Department. The devices are reset to factory settings during this process. The Institutional Procurement

[4] Different requirements may apply to test and development devices.

must be notified of the departure so that contractual terms can be amended or the contract terminated as necessary.

- If a mobile device is replaced with a new one, the old device must be returned to the IT-Service Department immediately. The IT-Service Department ensures that the old device is properly reset and/or disposed of. If the device is to be reused for research purposes or as a secondary device, the Institutional Procurement must be informed.
- To better protect company data, a container app (SecurePIM) is generally installed on the devices.
  When the container is open, the device must not be handed over to third parties.
  No data may be exported from the container, with the following exception: To identify callers, the export of name and phone number is permitted.
  Access to email or groupware systems may only be via the container app. Direct access to the Exchange server via the operating system is not permitted.
- Company data, particularly address books and emails, must not be stored unencrypted on external services or synchronized unencrypted via the manufacturer's cloud.
- Applications may only be obtained from the device manufacturers' app stores or other sources deemed trustworthy by the IT-Service Department. The IT-Service Department reserves the right to block individual apps that are clearly identified as harmful.
  Special care must be taken when installing applications ("apps") on mobile devices without a container app, as many apps read data and transmit it to the internet.

9.1 Personal use

- The use of work-issued smartphones should be exclusively for work-related purposes. If permissible personal use also takes place, it may be subject to billing. For details, see the section "Conclusion, extension, and termination of mobile Phone or data contracts".
- Authorization for personal use applies only to employees and does not extend to family members, friends, or other third parties.
- Setting up additional personal email accounts on the devices is permitted. Measures must be taken to separate personal and work accounts (e.g., a container app) to ensure that work emails are not accidentally sent via a personal email account.
- Personal appointments and contacts may be stored on the device and synchronized with the institute's Exchange server.
- Personal data (pictures, music, e.g., MP3s) may be stored on the smartphone provided that their possession or use does not violate copyright laws.
- Applications for personal use may be installed and used with due care, provided that this does not interfere with the device's work-related use and does not create a higher risk.
- In the event of theft, loss, or reasonable suspicion of misuse, a remote wipe may be performed: This deletes all data from the device. Users are personally responsible for performing regular backups; the institution is not liable for the loss of personal data! Backups must not be stored with cloud service providers but must be stored in encrypted form on local storage media.
- Smartphones may also be carried in private settings and on personal trips. Tablets and laptops may only be taken on private (international) trips if there is a proven special business necessity. This requires a prior Export Control Review, which is conducted at the traveler's request. Employees and team leaders must have the business necessity confirmed by their department head before making the request. Department and division heads may request the Export Control Review directly. For details, see also HaHi "Export control."

When traveling abroad, be aware of potential roaming charges and, if necessary, disable the internet connection. The regulations in the section "Remote work and conduct when traveling" apply mutatis mutandis to the carrying of devices on private trips.

9.2 Emergency Procedures

Smartphones are particularly prone to loss. This problem is exacerbated by the fact that smartphones store sensitive data. This includes, in particular, credentials (passwords) for accessing the resources of the Institute. As a security measure, the devices are equipped with a remote wipe feature. Employees must familiarize themselves with how the remote wipe option works as soon as the device is put into service.

- If the mobile device is lost or if misuse by third parties is suspected (e.g., installation of malware), the Institute must be notified immediately and, if possible, a remote wipe must be initiated. Reports are accepted during regular business hours at 09131 776 2777 by the IT-Service Department's hotline, which will then initiate the necessary measures. If the hotline cannot be reached, the user must at least block the SIM card and disable the Wi-Fi/internet connection (airplane mode).
- In collaboration with the Information Security Officer and the IT-Service Department, an investigation of the damage must be conducted; in particular, data losses must be identified and any unauthorized access to data of the Institute by third parties must be determined. All user passwords and PINs must be changed.

9.3 Notes on System Administration Tasks

Changing the passcode remotely is permitted only in cases of imminent danger and at the user's request. Remote wiping of the device by the IT-Service Department is permitted only under the following conditions:

- Loss of the device following a report by or at the request of the user
- In cases of reasonable suspicion of misuse
- In the event of reasonable suspicion of malware infection on the device, following this procedure:
  - If possible, prior notification of the user, documentation of the attempt to contact them
  - Documentation of the dangerous situation and the decision to perform remote deletion
  - Notification of the user regarding the deletion, accompanied by the documentation

Tracking of mobile devices is permitted only in exceptional cases. The following rules apply:

- If mobile devices are to be tracked, users must be informed in advance, and there must be a specific purpose (e.g., locating the device if lost).
- Remote activation of the location tracking function without the user's prior consent is permitted only in cases of danger to life and limb (e.g., location tracking abroad via International SOS in the event of disasters or in high-risk areas).

9.4 Conclusion, extension, and termination of mobile phone or data contracts

The *"GBV über den Einsatz von Mobiltelefonen (V. 1.1)"* governs the establishment of procedures and responsibilities related to the provision and cost coverage of mobile communication devices (referred to

as "Mobiltelefone" in the GBV) and the use of a business mobile phone contract within the Fraunhofer Society.
The central procurement of the necessary devices and business mobile phone contracts is the sole responsibility of the Institutional Procurement. Only this department is authorized to conclude, amend, or renew communication contracts (referred to as "dienstliche Mobilfunkverträge" in the GBV) on behalf of the Administrative Directorate.
As a general rule, the type and scope of communication devices to be provided must be determined in consultation with the budget officer or supervisor, taking cost-effectiveness into account.
The intranet contains a list of available business mobile phone plans, contract terms, notice periods, and conditions for personal use
(https://intern.iis.fhg.de/x/3hyWBQ).
Furthermore, we provide an overview of mobile devices, our preferred standard model (best value for money), and the corresponding order link (https://intern.iis.fhg.de/x/BWAsN).

List of exceptions that need to be approved:

- Porting a phone number from a personal contract to a business contract is only possible with approval from the Institutional Procurement.
- Porting a personal phone number back to a personal contract requires approval from the supervisor and the Administrative Directorate.
- Porting an existing business contract to a new personal contract is generally not possible.
- The device procured for work purposes remains the property of the Fraunhofer Society, must be returned upon the employee's departure, and cannot be transferred for private use.
- Any deviation from our standard contracts and standard models must be justified and approved by the department head and the Administrative Directorate (for amounts of 1,000 EUR net or more).

10 Use of private hardware

The use of hardware not provided by the Fraunhofer-Gesellschaft—in particular personal devices (including cameras and USB drives)—for Fraunhofer-Gesellschaft business purposes ("Bring Your Own Device," BYOD) is permitted only with the approval of the IT-Service Department and after consultation with the institute's Information Security Officer.
Neither the user nor the Fraunhofer-Gesellschaft may require the use of personal devices. Work-related data must be kept separate from personal data and given special protection. Family members and other individuals must not be able to access work-related data. Upon leaving the Fraunhofer-Gesellschaft, work-related data must be deleted unless otherwise agreed with the project or department management.
The IT-Service department must be permitted to monitor security settings.
The Fraunhofer Society reserves the right to access work-related data on the device in an emergency or in the event of suspected misuse, in accordance with the rules of the GBV "*IT-Grundsätze*". If private data is unintentionally deleted during remote deletion or remote access, there is no claim for damages.
Full access to the internal institute network is only possible for devices that are fully administrated by the IT-Service Department and meet all security requirements.
If BYOD is permitted for smartphones or tablets, the provisions of the section "Use of mobile devices" apply. The container app provided by the IT-Service Department must then be used. This enables restricted access (e.g., only calendar and email) to the internal institute network. A prerequisite is a device

classified as sufficiently secure, whose security status is assessed based on the operating system's up-to-date status.
Institute software may only be used on personal hardware in individual cases and with the approval of the IT-Service Department. Any restrictions regarding the type and duration of use must be observed.
The use of Microsoft Teams (with the Fraunhofer account) is not permitted on personal devices.

11 Remote work and conduct when traveling

Use of IT services outside the workplace, such as when working from home or working while traveling, requires special safeguards. Users must ensure that third parties cannot overhear confidential conversations and cannot observe any data displayed, for example, by reducing display brightness or protecting the display from being viewed. Devices may not be left unattended. Devices are to be locked during brief absences and secured physically where possible, e.g., by using a cable or by locking them away. When traveling, it may be necessary to ask someone to watch the device for a short time. Devices must be turned off entirely (Shutdown) in the event of a longer absence or at a hotel. It is recommended that you store the devices in the hotel safe or at least in a separate, lockable container if they are to be left unattended in the hotel. Risks must be weighed in the case of foreign travel. It may be necessary to use a separate travel device that contains only the data needed for the specific job at hand (see the separate proposal from the IT-Service Department). This especially applies to travel to high-risk countries. The info sheet on foreign travel and the *HaHi "Business trip"* must be observed.
The following situations must be reported immediately (including the device name) to the IT-Service Department or Information Security, and the instructions must be followed:

- The device had to be handed over to a third party (e.g., customs officials, etc.) while it was not fully shut down (or even unencrypted) or was inspected (authorized third-party access).
  → The device may only be used on the institute's network again (including VPN access) after approval by the IT-Service Department.
- Device loss (lost, stolen, etc.) → In case of theft, additionally file a report with the police.
- Loss of SIM cards.
  → Have the cards blocked immediately by the network operator. In case of theft, also file a police report.

12 Data back-up

Back-ups are to be taken care of by the Fraunhofer-Gesellschaft or its entities but not from users' personal data storage devices. For this reason, project data and other important documents are always stored on servers of the institute in a structure agreed upon with the project manager. The use of private data storage for this purpose is prohibited. Users must read up on back-up regulations. If, for compelling reasons, data or emails can only be stored on an end device instead of a server, this data might not be backed up automatically. In such cases, the user must confer with the IT-Service Department and their manager to ensure appropriate data storage and will take responsibility thereof.
If you are working on a computer without server access for an extended period of time, you must create encrypted local backups of important files (e.g., on a USB flash drive or external storage devices). The *HaHi "Information classification"* guidelines must be followed.

13 Storing data

Project results and other work-related data must be stored securely in accordance with legal requirements, contracts in force, and the rules of good scientific practice. In general, data must be retained for

at least 6 years (official emails and letters in particular); the minimum retention period for contracts and accounting records is 10 years. Project results and data required for their traceability may require even longer retention periods. Administrative data (contracts and business correspondence in particular) is stored in a timely manner in the project folder or file belonging to the project or department. Other data (such as project content) may be archived in different ways in accordance with the local institute's rules. The project managers and department heads provide information about applicable rules and procedures.

14 Returning equipment and turning over data upon departure from Fraunhofer

Users shall, prior to their departure from the Fraunhofer-Gesellschaft, hand over all equipment received from the organization, such as smartcell phones, laptopsnotebooks, and portable storage devices, and save project results as well as other work-related data in the appropriate project files or folders according to the previously mentioned rules for further work. Moreover, they should delete their private data from Fraunhofer storage media. Since selection and transfer of emails, in particular, may not always be possible, the institute may store private data (home directory and email account) beyond the employment relationship and within legally permissible time limits (usually for 10 years) when there is a valid reason. Data inspection is only admissible in the presence of the responsible employee representative or a representative appointed by the works council. Users who have left Fraunhofer have no right to Fraunhofer continuing to store their private data or making it accessible to them on a further basis. Email accounts are disabled after the owner of the account has left Fraunhofer and deleted later on, incoming emails will be rejected with an auto-reply.

15 Services and data made available on the Internet

If—for example, as part of projects—data and services are to be made available on the Internet to the public or to specific user groups, these services must first be approved by the IT-Service Department. Furthermore, a responsible person must be designated as the operator's technical and content contact for the operation of these services. If this contact person leaves the Fraunhofer-Gesellschaft, a successor must be designated and trained in a timely manner; otherwise, the service may not continue to be operated. The contact person is also responsible for responding promptly and taking corrective action in the event of known security vulnerabilities in the operated platform.
The application for and reservation of Internet domains may only be carried out through the IT-Service Department.

16 Disposal of data storage media

The measures required for the disposal or destruction of data storage media depend on the security classification of the data they contain and are outlined in the *HaHi "Information classification"* document. Simply deleting the data is insufficient!
Data storage media (such as CDs, DVDs, and USB drives) or devices with built-in storage that are no longer needed may be submitted to the IT-Service Department for deletion or destruction, provided the protection class of the stored data is specified.

17 Protection against malware

Every computer is protected by an endpoint protection solution (virus scanner) provided by the IT-Service Department.

The IT-Service Department actively manages updates to the operating system, standard programs, and the endpoint protection solution (virus scanner). Interfering with or disabling updates or malware scans is prohibited.
When security-related updates are available, they must be installed promptly, at the latest upon request by the IT-Service Department. To this end, devices must be connected to the IIS network for at least a few hours at least once a month. Devices with outdated operating systems will be denied access.
On devices that can access the Internet directly (i.e., without the institute network's firewall), a "personal firewall" must be used. The selection, installation, and configuration of this firewall are handled by the IT-Service Department.

18 Processing and storage of personal data, data processing on behalf of a client

Before processing or storing personal data, specific data protection plans must be developed. To this end, the Data Protection Contact Person and the IT-Service Department must be involved well in advance of the project's start. All data protection regulations must be strictly adhered to.
If external service providers are entrusted with the processing of personal data, a separate agreement regarding commissioned data processing must be concluded (in consultation with Institutional Procurement and the Legal Department).

Bernhard Grill

Digital unterschrieben von Bernhard Grill
Datum: 2026.07.23 16:38:00 +02'00'