B. Bekanntmachungen nach § 78 Abs. 2 NPersVG

Die nachfolgende Dienstvereinbarung, unterzeichnet vom Präsidenten der Gottfried Wilhelm Leibniz Universität Hannover sowie vom Personalrat der Gottfried Wilhelm Leibniz Universität Hannover, ist abgeschlossen worden. Sie tritt zum 01.04.2024 in Kraft.

Dienstvereinbarung gemäß § 78 NPersVG über Homeoffice und mobile Arbeit an der Leibniz Universität Hannover

zwischen

der Leibniz Universität Hannover, vertreten durch das Präsidium, dieses vertreten durch den Präsidenten

und

dem Personalrat der Leibniz Universität Hannover

Präambel

(1) Homeoffice und die mobile Arbeit an der Leibniz Universität Hannover sollen die Vereinbarkeit von Familie und Beruf für die Beschäftigten verbessern sowie den Bedürfnissen der Beschäftigten nach höherer Autonomie, Mobilität und Flexibilität Rechnung tragen. Die Teilnahme an Homeoffice und der mobilen Arbeit ist freiwillig und die Möglichkeiten dieser Arbeitsformen sind Ausdruck einer von Vertrauen und Wertschätzung getragenen Arbeitskultur an der Leibniz Universität Hannover.

(2) Mit Homeoffice und der mobilen Arbeit werden folgende Ziele verfolgt:
- Bessere Vereinbarkeit von Familie und Beruf. Unter Familie ist dabei ein soziales Netzwerk zu verstehen, in dem langfristig soziale Verantwortung für andere übernommen wird.[1]
- Bessere Inklusion von leistungsgewandelten Beschäftigten und schwerbehinderten Menschen im Sinne des Neunten Buch Sozialgesetzbuch (SGB IX)
- Beschäftigten mit Behinderungen und solchen, die von Behinderung bedroht sind zu helfen, im Beruf zu bleiben oder wieder zurück zu finden im Sinne des Aktionsplan Niedersachsen Inklusion 2017/18 zur Umsetzung der UN-Behindertenrechtskonvention
- Förderung der Diversität an der Leibniz Universität Hannover
- Bei Teilzeitbeschäftigten die Ermöglichung einer Aufstockung der Arbeitszeit
- Durch selbstbestimmtes Arbeiten eine höhere Flexibilität und größere Autonomie ermöglichen und dadurch eine Steigerung der Effizienz und Motivation zu erreichen
- Ökologischer Effekt durch Reduzierung des Berufsverkehrs und ein damit verbundener Beitrag zu Klimaschutz und Nachhaltigkeit
- Personalbindung
- Erhöhung der Attraktivität der Arbeitgeberin Leibniz Universität Hannover.

(3) Bei der mobilen Arbeit soll darüber hinaus berücksichtigt werden, dass bei den Beschäftigten vereinzelt kurzfristige Sondersituationen dienstlicher, familiärer oder persönlicher Art entstehen, die durch das Entbinden von der Präsenzpflicht in der Leibniz Universität Hannover bewältigt werden können.

(4) Die Leibniz Universität Hannover versteht Homeoffice und die mobile Arbeit als wichtige Bestandteile der Personalentwicklung. Diese beiden Arbeitsformen fordern ein verantwortungsvolles Handeln von Führungskräften und Beschäftigten. Homeoffice und mobile Arbeit sind geeignete Instrumente, um einerseits die Funktionsfähigkeit und Dienstleistungsqualität der Leibniz Universität Hannover sicherzustellen und andererseits die Interessen der Beschäftigten an einer den jeweiligen Lebensumständen flexibel angepassten Arbeitsform zu wahren, ohne dass dies zu einer Mehrbelastung der Beschäftigten führt.

[1] Zur Familie zählen u. a. die klassische Kernfamilie, alleinerziehende Mütter und Väter, nichteheliche und gleichgeschlechtliche Lebensgemeinschaften, Patchwork- und Pflegefamilien sowie andere Bezugspersonen, die regelmäßig Kinder oder Pflegebedürftige betreuen.

Teil A – Allgemeine Bestimmungen

A1 Gegenstand

Diese Dienstvereinbarung wird gemäß § 78 NPersVG (Niedersächsisches Personalvertretungsgesetz) geschlossen. Sie basiert auf der Vereinbarung gemäß § 81 NPersVG zu Telearbeit und mobile Arbeit (81er-Vereinbarung) in der niedersächsischen Landesverwaltung (Bek. D. MI v. 1. 6. 2021 – Z5.12-03082-02-01).

A2 Geltungsbereich

Diese Vereinbarung gilt für alle Beschäftigten gemäß § 4 NPersVG der Leibniz Universität Hannover, die nicht gemäß § 105 NPersVG von dem Geltungsbereich der Mitbestimmung ausgenommen sind. Diese Vereinbarung gilt nicht für in Ausbildung befindliche Beschäftigte (Auszubildende und Beamtinnen und Beamte auf Widerruf im Vorbereitungsdienst).

A3 Geltung dienstlicher und gesetzlicher Regelungen

(1) Alle gesetzlichen Regelungen sowie Regelungen der Dienststelle gelten unverändert auch für Homeoffice und die mobile Arbeit, soweit in dieser Dienstvereinbarung nicht ausdrücklich etwas anderes vereinbart ist.

(2) Der rechtliche Rahmen für Homeoffice und mobile Arbeit an der Leibniz Universität Hannover ergibt sich insbesondere aus den folgenden Grundlagen, die bei der Teilnahme an Homeoffice und mobiler Arbeit von der Dienststelle und den Beschäftigten in der jeweils geltenden Fassung zu beachten sind:
- Regelungen zur festen und gleitenden Arbeitszeit gemäß Rundschreiben (Vademecum)
- Arbeitsschutzgesetz (ArbSchG)
- Neuntes Buch Sozialgesetzbuch (SGB IX)
- Arbeitszeitgesetz (ArbZG)
- Niedersächsisches Beamtengesetz (NBG)
- Niedersächsisches Gleichberechtigungsgesetz (NGG)
- Nds. Personalvertretungsgesetz (NPersVG)
- Niedersächsisches Datenschutzgesetz (NDSG), EU-Datenschutzgrundverordnung (EU-DSGVO)
- Leitlinie zur Gewährleistung der Informationssicherheit (ISLL)
- Tarifvertrag für den öffentlichen Dienst der Länder (TV-L)
- Niedersächsische Verordnung über die Arbeitszeit der Beamtinnen und Beamten (Nds. ArbZVO)
- Schwerbehindertenrichtlinie (SchwbRl)
- Für das Homeoffice: Arbeitsstättenverordnung (ArbStättV)

(3) Es gelten ausschließlich die Bestimmungen des Niedersächsischen Gesetzes über die Feiertage (NFeiertagsG), unabhängig davon, an welchem Ort in Deutschland die Arbeit verrichtet wird.

A4 Benachteiligungsverbot

(1) Die Ausübung von Homeoffice oder mobiler Arbeit darf sich nicht nachteilig auf den beruflichen Werdegang der Beschäftigten auswirken.

(2) Es ist sowohl von den Vorgesetzten als auch den Beschäftigten sicherzustellen, dass der dienstlich notwendige Informationsfluss uneingeschränkt gewährleistet wird.

A5 Begriffsbestimmungen

A5.1 Homeoffice

(1) Homeoffice liegt vor, wenn Beschäftigte ihre individuelle regelmäßige Arbeitszeit teilweise an einem fest eingerichteten Arbeitsplatz im Privatbereich und teilweise in der betrieblichen Arbeitsstätte (Dienststelle) erbringen (analog des Begriffs „Telearbeit“ der 81er-Vereinbarung). Ein Arbeitsplatz im Privatbereich im Sinne dieser Vereinbarung liegt vor, wenn die bzw. der Beschäftigte zu Hause oder in einer privaten Räumlichkeit, die ihr oder ihm von Dritten zur Verfügung gestellt worden ist, arbeitet.

(2) Die Beschäftigten werden bei ihrem Homeoffice durch Geräte und Einrichtungen der Informationsverarbeitungs- und Kommunikationstechnik unterstützt. Die außerbetriebliche Arbeitsstätte ist mit der Dienststelle online verbunden. Die Gesunderhaltung der Beschäftigten im Homeoffice wird durch eine von der Dienststelle bereitgestellte ergonomische Arbeitsplatzausstattung gefördert.

A5.2 Mobile Arbeit

(1) Unter mobile Arbeit fällt die dienstliche Tätigkeit, die Beschäftigte bis zu 30 Prozent ihrer individuellen Arbeitszeit im Kalenderhalbjahr außerhalb der Dienststelle erbringen. Dieses kann sowohl tageweise als auch stundenweise erfolgen. Wenn IKT-Geräte (Informations- und Kommunikationstechnik) dabei zum Einsatz kommen, so sind diese von der Leibniz Universität Hannover zu stellen. Die Gesunderhaltung der mobil Arbeitenden durch ergonomische Arbeitsausstattung sowie die Beschaffung der geeigneten Ausstattung obliegt den Beschäftigten. Dabei werden sie auf Wunsch durch eine individuelle Beratung durch die Arbeitssicherheit unterstützt.

(2) Mobile Arbeit ist nicht gedacht als Ersatz für die Möglichkeiten der Arbeitsbefreiung oder Gewährung von Sonderurlaub unter Fortzahlung der Bezüge gemäß § 29 TV-L, §§ 9 und 9a Niedersächsische Sonderurlaubsverordnung (Nds. SUrlVO), § 45 SGB V und anderer tariflicher und gesetzlicher Bestimmungen.
Bei kurzfristigen Sondersituationen familiärer oder persönlicher Art, bei denen die Möglichkeit der Arbeitsbefreiung oder Sonderurlaub unter Fortzahlung der Bezüge besteht, sollen diese Möglichkeiten ausgeschöpft werden, bevor mobile Arbeit beantragt wird.

(3) Die Obergrenze nach Abs. 1 kann für schwerbehinderte und ihnen gleichgestellte Beschäftigte und im Rahmen des betrieblichen Eingliederungsmanagements (BEM) im Einzelfall überschritten werden.

A6 Freiwilligkeit

Homeoffice und mobile Arbeit unterliegen dem Grundsatz der Freiwilligkeit und können nur von den Beschäftigten beantragt, nicht aber von den Vorgesetzten angeordnet werden.

A7 Qualifizierung

(1) Beschäftigte in Homeoffice und mobil Arbeitende und ihre Vorgesetzten werden in geeigneter Weise über die Konsequenzen und Anforderungen dieser Arbeitsformen informiert. Insbesondere zu den Themen Führung und Kooperation, Selbstorganisation, Datenschutz sowie in der Handhabung der zur Verfügung gestellten Programme und Geräte werden sie geschult und fortgebildet. Hierzu werden entsprechende interne und/oder externe Formate durch die Dienststelle angeboten. Zudem ist der zielgruppenspezifische Qualifizierungsbedarf zu ermitteln.

(2) Die Dienststelle unterstützt den Aufbau eines Austauschformats für Beschäftigte, die Homeoffice wahrnehmen. An diesem Austauschformat sind die Dienststelle und der Personalrat beteiligt.

A8 Urlaub und Krankheit

Für Urlaub und Krankheit gelten dieselben Regelungen wie in der Dienststelle.

A9 Zeiterfassung

(1) Die Erfassung der Arbeitszeit muss auf die jeweilig geltende Regelung der Dienststelle (z. B. Dienstvereinbarung zur Gleitzeit und Dienstvereinbarung zur Zeiterfassung) abgestimmt sein, wobei die Einschaltzeit des Rechners nicht mit der Arbeitszeit gleichgesetzt werden kann. Die Erfassung der Arbeitszeit erfolgt durch manuelle Selbstaufzeichnung oder, falls vorhanden, durch ein entsprechendes elektronisches Zeiterfassungssystem.

(2) Im Rahmen der mobilen Arbeit gelten Wege zwischen dem Ort der mobilen Arbeit und der Leibniz Universität Hannover weder als Arbeitszeit noch als Dienstreise. Fahrtkosten werden nicht erstattet.

A10 Versicherungsschutz

Arbeitsunfälle an der außerbetrieblichen Arbeitsstätte sowie Unfälle auf dem Weg von und zur Dienststelle im Sinne des SGB VII fallen grundsätzlich bei Vorliegen der übrigen Voraussetzungen unter den gesetzlichen Unfallschutz.

A11 Haftung

(1) Die Haftung der oder des Beschäftigten, und im Falle von Homeoffice und mobiler Arbeit im Haushalt lebender Personen und berechtigter Besucher ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Schadensersatzansprüche Dritter – auch aus Verletzungen des Datenschutzes –, sofern sie ursächlich auf die außerbetriebliche Arbeitsstätte zurückzuführen sind, übernimmt die Leibniz Universität Hannover außer bei Vorsatz und grober Fahrlässigkeit.

(2) Um die Gefahr einer Unterversicherung beim Homeoffice auszuschließen, müssen die Beschäftigten ihrer privaten Hausratversicherung mitteilen, dass die von der Dienststelle gestellten Gegenstände am außerbetrieblichen Arbeitsplatz nicht zum versicherten Hausrat gehören. Ein der oder dem Beschäftigten durch das Unterlassen dieser Mitteilung entstehender Schaden wird nicht durch die Leibniz Universität Hannover erstattet.

A12 Verhaltens- und Leistungskontrolle

Verhaltens- und Leistungskontrollen durch die beim Homeoffice oder mobilen Arbeiten verwendeten technischen Systeme oder individuelle und vergleichende Auswertungen sind untersagt.

Teil B – Homeoffice

B1 Voraussetzungen für die Teilnahme am Homeoffice

Die Teilnahme am Homeoffice setzt voraus, dass:

a) die jeweiligen Tätigkeiten hierfür geeignet sind,
b) eine persönliche Arbeitszeit von mindestens 50% der regelmäßigen wöchentlichen Arbeitszeit gegeben ist; bei weniger als 50% ist eine Einzelfallprüfung möglich,
c) dringende dienstliche Belange nicht entgegenstehen,
d) die häusliche Umgebung für die Einrichtung eines Arbeitsplatzes für Homeoffice entsprechend den allgemeinen Anforderungen hinsichtlich Ergonomie, Arbeitssicherheit, des Datenschutzes und der Informationssicherheit geeignet ist,
e) die Beschäftigten – soweit erforderlich - den Zugang zum Privatbereich (häuslicher Arbeitsplatz) durch die Dienststelle, den Personalrat, die Fachkraft für Arbeitssicherheit der Dienststelle, die Schwerbehindertenvertretung, die Beauftragten für den Datenschutz und für die Informationssicherheit nach vorheriger Absprache ermöglichen,
f) die Beschäftigten vor Beginn der Arbeit im Homeoffice über Sicherheit und Gesundheitsschutz bei der Arbeit (§12 ArbSchG) unterwiesen werden.

B2 Antrags – und Genehmigungsverfahren für Homeoffice

(1) Die oder der Beschäftigte beantragt bei der Personalverwaltung mit dem als Anlage 1 dieser Dienstvereinbarung angefügten Vordruck die Teilnahme am Homeoffice

(2) Die Personalverwaltung prüft den Antrag und holt gegebenenfalls fehlende Stellungnahmen ein. Soweit die oder der Antragstellende schwerbehindert ist, ist die Schwerbehindertenvertretung auf Grundlage von § 178 SGB IX zu beteiligen.

(3) Genehmigt die Personalverwaltung den Antrag, informiert sie den Personalrat hierüber. Die Information enthält in Kopie den Antrag auf Homeoffice, die Stellungnahme der oder des Vorgesetzten sowie das Genehmigungsschreiben. Im Falle der Genehmigung von Homeoffice schließt die Dienststelle mit den Beschäftigten eine schriftliche Vereinbarung nach Anlage 3 über die Durchführung von Homeoffice ab.

(4) Beim Wechsel des Arbeitsplatzes innerhalb der Leibniz Universität Hannover kann der genehmigte Antrag im Einvernehmen mit der dann vorgesetzten Person weitergelten, sofern die Tätigkeiten und das ausgewählte Technikszenario dies ermöglichen. Das Einvernehmen ist zu dokumentieren.

(5) Möchte die Personalverwaltung einen Antrag auf Homeoffice ablehnen, so wird sie dies vor der formalen Ablehnung mit dem Personalrat und – falls die Antragstellerin oder der Antragsteller schwerbehindert oder gleichgestellt ist, auch mit der Schwerbehindertenvertretung – in einem Termin erörtern. Erst nach einem solchen Erörterungstermin wird sie dem Personalrat die Ablehnung Homeoffice-Antrages als Maßnahme vorlegen. Bei der Ablehnung von Anträgen auf Homeoffice beteiligt die Dienststelle den Personalrat auf Grundlage des § 65 Abs. 1 Nr. 26 oder § 65 Abs. 2 Nr. 20 NPersVG. Sollte nach der Durchführung des Mitbestimmungsverfahrens die Dienststelle an der Ablehnung festhalten, hat sie die schriftlich der oder dem Beschäftigten unter Angabe der Gründe mitzuteilen.

B3 Zusätzliche Anwesenheit der Beschäftigten im Homeoffice in der Dienststelle

(1) Dienstlich dringend bedingte zusätzliche Anwesenheit in der Dienststelle der Beschäftigten im Homeoffice darf von ihnen nur aus wichtigem Grund abgelehnt werden. In diesen Fällen dürfen sich aus der Ablehnung keine arbeits-/dienstrechtlichen Konsequenzen ergeben.

(2) Für den Tag, an dem sich die Beschäftigten bereits im Homeoffice befinden, kann ihre Anwesenheit in der Dienststelle auch bei Vorliegen wichtiger dienstlicher Gründe nicht mehr angeordnet werden.

B4 Ausstattung der Homeoffice-Arbeitsplätze und Kosten

(1) Die Leibniz Universität Hannover stattet die außerbetriebliche Arbeitsstätte mit Beteiligung der oder des Beschäftigten - soweit erforderlich - mit den notwendigen technischen Arbeitsmitteln und mit notwendigen Möbeln sowie bei Bedarf mit einem Telefon aus. Die Finanzierung erfolgt durch die jeweilige Einrichtung. Dabei kann auf Wunsch der Beschäftigten auch eigenes Mobiliar genutzt werden, wenn dieses den ergonomischen Gesichtspunkten entspricht. Die Leibniz Universität Hannover stellt die Betreuung, Wartung und die Einhaltung der gesetzlichen Normen hinsichtlich der ergonomischen Gesichtspunkte sicher und trägt die Kosten der erforderlichen Verbrauchsmittel.

(2) Für den Zugriff auf dienstliche Daten (z.B. Netzwerkablage, E-Mail, e-Akte) wird den Beschäftigten die erforderliche Informations- und Kommunikationstechnik zur Verfügung gestellt. Die Bereitstellung der EDV-Ausstattung zur Abholung durch die Beschäftigten erfolgt durch die Leibniz Universität IT Services (LUIS) oder die Einrichtung. Die Beschäftigten stellen einen geeigneten Internetzugang auf eigene Kosten zur Verfügung. Gleiches gilt für einen Telefonanschluss, soweit dieser nicht mit anderen technischen Mitteln dienstlich zur Verfügung gestellt wird (z. B. Diensthandy, Voice-Over-IP). Miete, Heizung, Strom und sonstige Nebenkosten sowie laufende Kosten der Telekommunikation werden nicht erstattet.

B5 Ablauf zur Einrichtung eines Homeoffice-Arbeitsplatzes

Um Homeoffice als Arbeitsform zu nutzen, sind die folgenden Schritte zu durchlaufen:

a) Ausfüllen des Antrags auf Homeoffice und Einreichung im Sachgebiet 21 der Personalverwaltung,
b) Prüfung des Antrags durch die Personalverwaltung,
c) Entscheidung über den Antrag,
d) Ausstattung der außerbetrieblichen Arbeitsstätte mit Büromöbeln,
e) Bereitstellung der EDV-Ausstattung,
f) Abnahme der außerbetrieblichen Arbeitsstätte durch die Stabstelle für Arbeitssicherheit unter Beteiligung des Personalrates bezüglich der Einhaltung ergonomischer, sicherheitstechnischer Vorschriften. Im Einvernehmen zwischen der Dienststelle, dem Personalrat und den Beschäftigten kann die Abnahme in begründeten Einzelfällen auch durch eine verbindliche und geeignete Selbstauskunft der Beschäftigten erfolgen.
g) Aushändigung der Vereinbarung nach Anlage 3 an die Beschäftigte oder den Beschäftigten.

B6 Arbeitszeit und Aufteilung der Arbeitszeit auf die Arbeitsstätten

(1) Bei Homeoffice sind mindestens 20 % der individuellen Wochenarbeitszeit am Arbeitsplatz in der Dienststelle abzuleisten, mindestens 20 % soll am außerbetrieblichen Arbeitsplatz gearbeitet werden.

(2) Die Arbeitszeit ist innerhalb des Arbeitszeitrahmens auf die betriebliche und die außerbetriebliche Arbeitsstätte aufzuteilen. Die Aufteilung der Arbeitszeit auf die Arbeitsstätten wird in der Regel in der schriftlichen Vereinbarung nach Anlage 3 festgelegt. Bei besonderen Anlässen kann im Einvernehmen mit der oder dem Vorgesetzten von der festgelegten Aufteilung abgewichen werden.

(3) Einvernehmlich kann Homeoffice auch ohne Festlegung der Wochentage vereinbart werden.

B7 Datenschutz

Die Beschäftigten sind verpflichtet, die Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit (Anlage 6) einzuhalten.

B8 Aufnahme und Beendigung von Homeoffice

(1) Homeoffice wird in der Regel befristet für drei Jahre vereinbart. Spätestens drei Monate vor Ablauf des Bewilligungszeitraumes muss das Homeoffice bei weiterhin bestehendem Interesse durch die Beschäftigten neu beantragt werden.

(2) Die Beschäftigten haben das Recht, aus wichtigem Grund durch einseitige, schriftliche Erklärung zum Ende des folgenden Monats die außerbetriebliche Arbeitsstätte aufzugeben und an ihren bzw. seinen Arbeitsplatz in der Dienststelle zurückzukehren.

(3) Die Leibniz Universität Hannover darf die Einrichtung des außerbetrieblichen Arbeitsplatzes aus wichtigem dienstlichem Grund mit Beteiligung des Personalrats schriftlich und mit Dreimonatsfrist zum Monatsende widerrufen. Das Interesse der Beschäftigten am Fortbestand des Homeoffice wird im Falle des Widerrufs gegen das Interesse der Leibniz Universität Hannover an der Beendigung des Homeoffice umfassend abgewogen. Ein Widerruf erfolgt nur bei überwiegendem Interesse der Leibniz Universität Hannover gegenüber den Interessen der oder des Beschäftigten. Der Widerruf der Genehmigung von Homeoffice ist eine Ablehnung des Antrags auf Telearbeit im Sinne des § 65 Abs. 1 Nr. 26 oder § 65 Abs. 2 Nr. 20 NPersVG und muss dem Personalrat zur Mitbestimmung vorgelegt werden.

(4) Als wichtiger Grund im Sinne des Absatzes (2) und (3) kann vor allem die Änderung der persönlichen sozialen Rahmenbedingungen, eine wesentliche Änderung des Arbeitsinhaltes, der internen Arbeitsabläufe, organisatorische Veränderungen, die Verweigerung des Zutritts zur außerbetrieblichen Arbeitsstätte oder ein Verstoß gegen arbeits- oder datenschutzrechtliche Bestimmungen gelten.

(5) Bei Beendigung des Homeoffice ist die Rücknahme der Arbeitsmittel durch die Leibniz Universität Hannover unverzüglich zu ermöglichen. Der Transport zur Verfügung gestellter Gegenstände erfolgt in der Regel durch die Dienststelle. Es erfolgt kein Vor- oder Nachteilsausgleich.

Teil C – Mobile Arbeit

C1 Voraussetzungen für die mobile Arbeit

(1) Die in der mobilen Arbeit zu verrichtenden Tätigkeiten der oder des Beschäftigten muss für mobiles Arbeiten geeignet sein. Die dienstlichen Abläufe dürfen durch das mobile Arbeiten nicht gestört werden. Dienstliche Termine oder Veranstaltungen, bei denen die physische Anwesenheit der oder des Beschäftigten erforderlich ist, genießen stets den Vorrang vor dem mobilen Arbeiten. Mobiles Arbeiten ist vor diesem Hintergrund grundsätzlich möglich, wenn und soweit dienstliche Interessen nicht entgegenstehen. Entgegenstehende dienstliche Interessen können sich beispielsweise aus einer notwendigen Präsenz an der Leibniz Universität Hannover und der Art der zu verrichtenden Tätigkeiten ergeben.

(2) Das mobile Arbeiten erfordert die telefonische Erreichbarkeit während der jeweils geltenden Arbeitszeit.

(3) Für das mobile Arbeiten eignen sich im Regelfall nur solche Tätigkeiten, die eigenständig durchgeführt und ohne Beeinträchtigung des Dienstablaufs außerhalb der Räumlichkeiten der Leibniz Universität Hannover erledigt werden können.

(4) Erforderlich für die Teilnahme ist ein genehmigter Antrag nach C2 dieser Dienstvereinbarung.

(5) Die Vorgesetzten sorgen für eine rechtzeitige, regelmäßige und ausreichende Unterweisung der Beschäftigten zu Arbeitssicherheit sowie Arbeits- und Gesundheitsschutz im Hinblick auf mobile Arbeit.

C2 Antrags- und Genehmigungsverfahren für die mobile Arbeit

(1) Die Beschäftigten beantragen mit dem als Anlage 4 dieser Dienstvereinbarung angefügten Vordruck mobile Arbeit bei der oder dem unmittelbaren Vorgesetzten. Die oder der unmittelbare Vorgesetzte kann den Antrag schriftlich genehmigen. Die Genehmigung erfolgt grundsätzlich für einen Zeitraum von drei Jahren, die konkrete Inanspruchnahme muss jeweils mit den Vorgesetzten abgestimmt werden. Den genehmigten Antrag auf mobile Arbeit leiten die Vorgesetzten an die Personalverwaltung weiter. Die Beschäftigten erhalten von den Vorgesetzten eine Kopie des genehmigten Antrags. Die Personalverwaltung informiert quartalsweise den Personalrat in geeigneter Form über die genehmigten Anträge.

(2) Eine geplante Ablehnung des Antrags oder der Widerruf eines genehmigten Antrags ist mit entsprechender Begründung der Personalverwaltung mitzuteilen, die diese dem Personalrat als Maßnahme vorlegt. Falls die antragstellende Person schwerbehindert oder gleichgestellt ist, hört die Personalverwaltung die Schwerbehindertenvertretung zum geplanten Widerruf oder die geplante Ablehnung vor Beteiligung des Personalrats an. Sollte nach der Durchführung des Mitbestimmungsverfahrens die Dienststelle an der Ablehnung festhalten, hat sie dies schriftlich der oder dem Beschäftigten unter Angabe der Gründe mitzuteilen.

C3 Arbeits- und Verbrauchsmittel, Kosten

(1) Die notwendigen Arbeits- und Verbrauchsmittel für den Ort der mobilen Arbeit, wie z. B. Schreibgeräte oder Laptops, werden in der Regel nach Absprache mit den Vorgesetzten von der jeweiligen Einrichtung gestellt. Die Nutzung privater IT-Geräte kann nicht angeordnet werden und unterliegt den im Vademecum der Leibniz Universität Hannover veröffentlichten geltenden Regelungen für den dienstlichen Einsatz mobiler und privater Geräte.

(2) Die Leibniz Universität Hannover wird für den Ort der mobilen Arbeit weder einen Anteil an Miete noch an Nebenkosten, beispielsweise auch nicht für Telefon und Datenverbindung erstatten.

C4 Ort der mobilen Arbeit

(1) Der Ort der mobilen Arbeit kann jeder Ort außerhalb der Dienststelle sein. Es gibt keinen spezifisch für die mobile Arbeit vorgesehenen Ort.

(2) Der Ort der mobilen Arbeit ist von den Beschäftigten so zu wählen, dass Dritte keine Einsicht in vertrauliche Daten und Informationen erlangen können. Öffentliche Orte wie z. B. Zugabteile, Cafés und öffentliche Grünanlagen sind daher für die Arbeit mit vertraulichen Daten und Informationen nur bedingt geeignet und erfordern geeignete Schutzmaßnahmen. Personenbezogene Daten und der Geheimhaltung unterliegende Daten dürfen an diesen Orten nur bearbeitet werden, wenn die erforderlichen Schutzmaßnahmen mit der mit der Dienstanweisung zum Datenschutz und zur Informationssicherheit (Anlage 6) und dem Sicherheits- und Technikkonzept (Anlage 7) übereinstimmen.

(3) Mobile Arbeit aus dem Ausland ist unzulässig.

(4) Unfälle während der mobilen Arbeit am Ort der mobilen Arbeit können je nach Einzelfallgestaltung Arbeitsunfälle sein.

C5 Datenschutz

Die Beschäftigten sind verpflichtet, die Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit (Anlage 6) einzuhalten.

Teil D - Schlussbestimmungen

D1 Inkrafttreten / Geltungsdauer / Kündigung

(1) Diese Vereinbarung tritt mit Wirkung vom 01.04.2024 in Kraft. Sie kann einseitig unter Einhaltung einer Kündigungsfrist von vier Monaten gekündigt werden. Mit Inkrafttreten dieser Dienstvereinbarung tritt die befristete Dienstvereinbarung über Homeoffice und mobile Arbeit an der Leibniz Universität Hannover vom 01.04.2022 außer Kraft.

(2) Die einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform. Im Übrigen gilt § 78 Abs. 4 NPersVG.

(3) Nach Beendigung der Dienstvereinbarung ist die änderungslose weitere Anwendung dieser Regelungen unter den hier vereinbarten Bedingungen möglich. Die Dienststelle und der Personalrat verpflichten sich, im Falle der Kündigung unverzüglich Verhandlungen über eine Nachfolgeregelung aufzunehmen.

(4) Sollten einzelne Bestimmungen dieser Vereinbarung insbesondere wegen Verstoßes gegen § 82 NPersVG, nichtig sein oder werden, so berührt dies nicht die Gültigkeit der übrigen Bestimmungen. Anstelle der unwirksamen Bestimmungen, oder zur Ausfüllung eventueller Lücken der Vereinbarung soll eine angemessene Regelung treten, die dem am Nächsten kommt, was die Parteien nach ihrer Zwecksetzung gewollt haben.

Hannover, den 27.03.2024	Hannover, den 27.03.2024
gez. Prof. Dr. iur. Volker Epping	gez. Elvira Grube
Präsident	Vorsitzende des Personalrats

Anlagen:

Anlage 1 – Antragsformular Homeoffice Erstantrag
Anlage 2 – Antragsformular Verlängerung Homeoffice
Anlage 3 – Zusatzvereinbarung zum Homeoffice
Anlage 4 – Antragsformular Mobile Arbeit
Anlage 5 – Hinweise zur Arbeitszeit
Anlage 6 – Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit
Anlage 7 – Sicherheits- und Technikkonzept für Homeoffice und mobiles Arbeiten

Anlage 1:

Vertrauliche Personalsache

Präsident der
Leibniz Universität Hannover
Sachgebiet 21
-21.25-

hier

Einrichtung eines Arbeitsplatzes im Homeoffice – Antrag

A. Angaben der antragstellenden Person

1. Allgemeine Angaben	
Name, Vorname:	
Einrichtung:	
Dienstttelefon:	
dienstliche E-Mail-Adresse:	
Anschrift des Homeoffice-Arbeitsplatzes:	

2. Angaben zum Beschäftigungsverhältnis			
Ich bin	☐ tarifbeschäftigt	☐ verbeamtet	
Umfang der Beschäftigung:		Stunden/Woche	
(mind. 50 %, sonst Einzelfallprüfung)		Prozent (%)	
Ich habe einen Schwerbehindertenstatus gemäß § 2 Absatz 2 SGB IX oder einen Gleichgestelltenstatus gemäß § 2 Absatz 3 SGB IX.		☐ ja	☐ nein

3. Angaben zum Datenschutz und zur Informationssicherheit		
Im Rahmen meiner dienstlichen Aufgaben/Tätigkeiten verarbeite ich personenbezogene oder -beziehbare Daten:	☐ ja	☐ nein
Ich versichere, dass ich im Homeoffice nur Tätigkeiten erledigen werde, die gemäß der Dienstanweisung zum Datenschutz und zur Informationssicherheit (Anlage **6**) mit der mir zur Verfügung gestellten Technik die datenschutzrechtlichen Voraussetzungen zur Teilnahme am Homeoffice erfüllen. Das heißt insbesondere, dass ich im Homeoffice keine besonders sensiblen oder schutzwürdigen Daten nach Schutzstufe E verarbeiten werde. Ferner werden keine Daten verarbeitet, an deren Verarbeitung Dritte Anforderungen bzgl. Vertraulichkeit stellen.		
Die personenbezogenen Daten, die im Homeoffice verarbeitet werden sollen, entsprechen <u>maximal</u> dem folgenden Schutzbedarf: (**Hinweis**: Die Festlegung der Schutzstufen muss anhand der Dienstanweisung zum Datenschutz und zur Informationssicherheit (Anlage 6) vorgenommen werden.)	☐ Schutzstufe A - B ☐ Schutzstufe C ☐ Schutzstufe D	

4. Angaben zu Umfang und Aufteilung des Homeoffices

Mein gewünschter Beginn des Homeoffices ist:	_____
Meine gewünschte Dauer des Homeoffices beträgt: (**Hinweis:** Homeoffice wird zunächst i. d. R. für eine Dauer von drei Jahren genehmigt, um danach die Bedingungen, Voraussetzungen, etc. erneut zu überprüfen. Spätestens drei Monate vor Ablauf des Bewilligungszeitraumes muss Homeoffice neu beantragt werden.)	☐ 3 Jahre ☐ weniger als 3 Jahre, nämlich: _____
Mein gewünschter Umfang des Homeoffices beträgt: (**Hinweis**: mindestens 1/5 der individuellen Arbeitszeit ist in der Dienststelle/im Homeoffice abzuleisten. Auch in Kombination mit dem mobilen Arbeiten dürfen maximal 4/5 der wöchentlichen Arbeitszeit außerhalb der Dienststelle erbracht werden.)	_____ Stunden/Woche bzw. _____ % der wöchentl. Arbeitszeit

☐ Homeoffice soll mit Festlegung der Wochentage wie folgt vereinbart werden:

Wochentag	**Arbeitsplatz an der Universität**	**Homeoffice**	**Bemerkung zur Aufteilung (z. B. vormittags-nachmittags)**
Montag	☐	☐	
Dienstag	☐	☐	
Mittwoch	☐	☐	
Donnerstag	☐	☐	
Freitag	☐	☐	

☐ Homeoffice soll ohne Festlegung der Wochentage vereinbart werden und wird in Absprache mit der vorgesetzten Person individuell verabredet.

5. Angaben zu den technischen Voraussetzungen	
Ich versichere, dass ich im Homeoffice Folgendes zur Verfügung stelle:	
☐	Internetanschluss mit für Büroarbeit üblicher Leistung (z.B. DSL ab 10 MBit, Internetflatrate).
☐	Ein Telefonanschluss (nach Möglichkeit mit separater Telefonnummer)
Aus Gründen der Verbindungsstabilität wird empfohlen, den Arbeitsplatz im Homeoffice kabelgebunden an das Datennetz anzuschließen.	

6. Angaben zum Arbeitsplatz innerhalb der privaten Räumlichkeiten		
Mir steht ein Arbeitsplatz zur Verfügung, an dem ich ungestört arbeiten kann:	☐ ja	☐ nein
Ein Rauchmelder…	☐ ist im Zimmer des Arbeitsplatzes bzw. in einem dem Arbeitsplatz nahe gelegenen Bereich (z. B. Flur) vorhanden.	

7. Technische Ausstattung, die für den Arbeitsplatz im Homeoffice zusätzlich benötigt wird
☐ Telefon ☐ Drucker ☐ Scanner ☐ Aktenvernichter

Zwei Fotos des Zimmers, in dem das Homeoffice ausgeübt werden soll, **sind diesem Antrag beizufügen, sofern der Wohnort außerhalb der Region Hannover liegt** (Anhang D). Daraus gehen auch die bereits

vorhandenen Arbeitsmittel bzw. die Büroeinrichtung hervor, die vorbehaltlich der Empfehlung der Stabstelle für Arbeitssicherheit mitbenutzt werden können. Auf Grundlage dieser Unterlagen wird die Stabstelle für Arbeitssicherheit prüfen, ob der Arbeitsplatz für die zu erledigenden Aufgaben unter Einhaltung der Arbeitsschutzgesetze geeignet ist und den Anforderungen der Verordnungen über Arbeitsstätten entspricht.

8. Erklärung

Ich versichere, dass die erforderlichen Kriterien zur Eignung meiner Aufgaben und Tätigkeiten sowie meines Arbeitsplatzes erfüllt sind und ich die Grundkompetenz für den selbständigen Umgang mit der IT-Technik erworben habe und die benötigten Kenntnisse besitze. Ich kann für einen fachgerechten Anschluss des Rechners am Arbeitsplatz sorgen.

Ich versichere, dass ich alle Angaben nach bestem Wissen und Gewissen gemacht habe. Die **Dienstvereinbarung über Homeoffice und mobile Arbeit an der Leibniz Universität Hannover** habe ich zur Kenntnis genommen.

Mir ist bekannt, dass die Betriebskosten, die im Homeoffice anfallen (Strom, anteilige Miete, Heizung usw.), zu meinen Lasten gehen.

Aus wichtigem Anlass nach vorheriger Terminabsprache räume ich der Stabstelle für Arbeitssicherheit sowie beauftragten Personen Zugang zur Arbeitsstätte in den privaten Räumlichkeiten zwecks Einrichtung, Wartung und Reparatur des Arbeitsplatzes im Homeoffice ein. Mir ist bekannt, dass die Personalvertretung, die/der Datenschutzbeauftragte sowie ggf. die Schwerbehindertenvertretung der Leibniz Universität Hannover die Möglichkeit haben, an der Begehung teilzunehmen. Auch ihnen räume ich ein Zugangsrecht ein.

Ort, Datum	Unterschrift antragstellende Person

B. Stellungnahme der Systemadministration	
Name, Vorname:	
Dienststelle/Institut:	
Diensttelefon:	
dienstliche E-Mail-Adresse:	

Zum Antrag auf Einrichtung eines Arbeitsplatzes im Homeoffice von	
Name, Vorname:	

Technikszenario			
☐	Thinclient	☐	Managed Device
☐	Road-Warrior	☐	Fortrex
☐	Einrichtungs-Laptop mit VPN-Zugang in die Einrichtung		

Angaben zum Zielsystem beim Einsatz eines Thinclients		
Typ	☐ Arbeitsplatz-PC	☐ Server
System	☐ Windows	☐ Linux
Protokoll	☐ RDP	☐ SSH/X2Go
IP-Adresse	. . . (zwingend anzugeben)	

Angaben zur Verbindung bei einem anderen Technikszenario als dem Thinclient			
☐	LUH-VPN	☐	Einrichtungs-VPN

Raum für zusätzliche Angaben

☐ Ich versichere, dass ich das Sicherheits- und Technikkonzept zur Kenntnis genommen habe.

Ort, Datum

Unterschrift Systemadministration

C. Stellungnahme der vorgesetzten Person

Name, Vorname: _____

Einrichtung: _____

Diensttelefon: _____

dienstlicheE-Mail-Adresse: _____

Zum Antrag auf Einrichtung eines Arbeitsplatzes im Homeoffice von

Name, Vorname: _____

☐ Die **Dienstvereinbarung über Homeoffice und mobile Arbeit an der Leibniz Universität Hannover** habe ich zur Kenntnis genommen.

☐ Ich befürworte die Einrichtung eines Arbeitsplatzes im Homeoffice. Dienstliche Gründe stehen nicht entgegen.

Die zu verrichtenden Tätigkeiten sind für Homeoffice geeignet und entsprechen gem. Sicherheits- und Technikkonzept der aggregierten Risikoklasse

☐ unkritisch ☐ moderat ☐ kritisch.

☐ Es wurde entsprechend dem Sicherheits- und Technikkonzept ein geeignetes Technikszenario ausgewählt.

☐ Die antragstellende Person wird durch eine Systemadministration betreut.

☐ Ich befürworte die Einrichtung eines Arbeitsplatzes im Homeoffice nicht. Die Personalverwaltung wird hierüber informiert und entscheidet über den Antrag. Im Falle der Ablehnung wird der Personalrat beteiligt. Folgende dienstliche Gründe stehen entgegen:

Bemerkungen:

Ort, Datum

Unterschrift vorgesetzte Person

D. Anhang (Fotos des im Homeoffice genutzten Zimmers)

Vertrauliche Personalsache

Präsident der
Leibniz Universität Hannover
Sachgebiet 21
-21.25-

hier

Anlage 2:

Homeoffice – Verlängerungsantrag

Hiermit beantrage ich die Verlängerung meines bestehenden Arbeitsplatzes im Homeoffice	
ab dem	
☐	um weitere drei Jahre.
☐	um weniger als drei Jahre, bis zum:

1. Allgemeine Angaben	
Name, Vorname:	
Einrichtung:	
Diensttelefon:	
dienstliche E-Mail-Adresse:	
Anschrift des Homeoffice-Arbeitsplatzes:	

2. Angaben zum Beschäftigungsverhältnis	
☐	Unverändert zum Erstantrag / zum zuletzt vorliegenden Verlängerungsantrag
☐	Folgende Veränderung ist eingetreten:

3. Angaben zum Datenschutz und zur Informationssicherheit	
☐	Unverändert zum Erstantrag / zum zuletzt vorliegenden Verlängerungsantrag
☐	Folgende Veränderung ist eingetreten:

4. Angaben zu den technischen Voraussetzungen und zum Arbeitsplatz innerhalb der privaten Räumlichkeiten	
	Unverändert zum Erstantrag / zum zuletzt vorliegenden Verlängerungsantrag
	Folgende Veränderung ist eingetreten:

5. Angaben zu Umfang und Aufteilung des Homeoffices	
Mein gewünschter Umfang des Homeoffices beträgt: (**Hinweis**: mindestens 1/5 der individuellen Arbeitszeit ist in der Dienststelle/im Homeoffice abzuleisten. Auch in Kombination mit dem mobilen Arbeiten dürfen maximal 4/5 der wöchentlichen Arbeitszeit außerhalb der Dienststelle erbracht werden.)	_____ Stunden/Woche bzw. _____ % meiner wöchentl. Arbeitszeit

☐ Homeoffice soll mit Festlegung der Wochentage wie folgt vereinbart werden:

Wochentag	Arbeitsplatz an der Universität	Homeoffice	Bemerkung zur Aufteilung (z. B. vormittags-nachmittags)
Montag			
Dienstag			
Mittwoch			
Donnerstag			
Freitag			

☐ Homeoffice soll ohne Festlegung der Wochentage vereinbart werden und wird in Absprache mit der vorgesetzten Person individuell verabredet.

6. Angaben zum verwendeten Technikszenario				
Derzeit verwendetes Technikszenario:				
	☐	Thinclient	☐	Managed Device
	☐	Road-Warrior	☐	Fortrex
	☐	Einrichtungs-Laptop mit VPN-Zugang in die Einrichtung		
Zukünftig verwendetes Technikszenario:				
	☐	Thinclient	☐	Managed Device
	☐	Road-Warrior	☐	Fortrex
	☐	Einrichtungs-Laptop mit VPN-Zugang in die Einrichtung		
Hinweis: Bei Änderungen des Technikszenarios bitte eine neue Stellungnahme der Systemadministration beifügen.				

7. Erklärung

Ich versichere, dass die erforderlichen Kriterien zur Eignung meiner Aufgaben und Tätigkeiten sowie meines Arbeitsplatzes weiterhin erfüllt sind. Die **Dienstvereinbarung über Homeoffice und mobile Arbeit an der Leibniz Universität Hannover** habe ich zur Kenntnis genommen.
Ich versichere, bei Änderung die Dienststelle unverzüglich zu informieren.

Aus wichtigem Anlass nach vorheriger Terminabsprache räume ich beauftragten Personen erneut Zugang zum Arbeitsplatz im Homeoffice ein. Mir ist bekannt, dass die Personalvertretung, und ggf. die Schwerbehindertenvertretung der Leibniz Universität Hannover die Möglichkeit haben, an der Begehung teilzunehmen. Auch ihnen räume ich ein Zugangsrecht ein.

_____ _____
Ort, Datum Unterschrift antragstellende Person

8. Stellungnahme der vorgesetzten Person

Name, Vorname: _____

Einrichtung: _____

Diensttelefon: _____

dienstliche E-Mail-Adresse: _____

Zum Homeoffice-Verlängerungsantrag von

Name, Vorname: _____

☐ Die **Dienstvereinbarung über Homeoffice und mobile Arbeit an der Leibniz Universität Hannover** habe ich zur Kenntnis genommen.

☐ Ich befürworte die Verlängerung des Homeoffices. Dienstliche Gründe stehen nicht entgegen.

Darüber hinaus versichere ich, dass die erforderlichen Kriterien zur Eignung der antragstellenden Person weiterhin erfüllt und die Aufgaben und Tätigkeiten, sowie das eingesetzte Technikszenario für Homeoffice weiterhin geeignet sind. Die antragstellende Person wird weiterhin durch eine Systemadministration betreut.

☐ Ich befürworte die Verlängerung des Homeoffices nicht. Die Personalverwaltung wird hierüber informiert und entscheidet über den Antrag. Im Falle der Ablehnung wird der Personalrat beteiligt. Folgende dienstliche Gründe stehen entgegen:

Bemerkungen:

_____ _____

Ort, Datum Unterschrift vorgesetzte Person

Anlage 3:

Vereinbarung zur Durchführung von Homeoffice

Mit

Vor- und Nachname des/der Beschäftigten

Straße- und Hausnummer des Homeoffice-Arbeitsplatzes

PLZ und Wohnort des Homeoffice-Arbeitsplatzes

wird die Einrichtung eines Homeoffice-Arbeitsplatzes im Privatbereich vom _____ bis _____ vereinbart.

1. Grundlage

   Grundlage dieser Vereinbarung ist **Dienstvereinbarung über Homeoffice und mobile Arbeit an der Leibniz Universität Hannover** vom 1. April 2024. Soweit erforderlich, ist der Zutritt zur häuslichen Arbeitsstätte durch den unter B1 Buchstabe e) der Dienstvereinbarung genannten Personenkreis nach Absprache zu gestatten.

2. Arbeitszeit/ Zeiterfassung

2.1 Die zu leistende Arbeitszeit ist die arbeits- oder tarifvertraglich bzw. beamtenrechtlich festgelegte individuelle wöchentliche Arbeitszeit.

2.2 Bei einer regelmäßigen wöchentlichen Arbeitszeit von Stunden können bis zu Stunden pro Woche (entspricht %) im Homeoffice gearbeitet werden. Mindestens Stunden in der Woche sind demnach in der Dienststelle zu arbeiten.

☐ Homeoffice wird mit Festlegung von Wochentagen vereinbart. Die Aufteilung ist in der Regel:

Wochentag	Arbeitsplatz an der Universität	Homeoffice	Bemerkung zur Aufteilung (z. B. vormittags - nachmittags)
Montag	☐	☐	
Dienstag	☐	☐	
Mittwoch	☐	☐	
Donnerstag	☐	☐	
Freitag	☐	☐	

☐ Homeoffice wird ohne Festlegung von Wochentagen vereinbart und in Absprache mit der vorgesetzten Person individuell vereinbart.

2.3 Die Erfassung der Arbeitszeiten erfolgt nach den in der Dienststelle geltenden Regelungen.

2.4 Bei dringenden dienstlichen Erfordernissen ist eine Anwesenheit in der Dienststelle auch an vereinbarten Homeoffice-Tagen möglich. Bei Vorliegen eines wichtigen Grundes kann die Beschäftigte / der Beschäftigte die zusätzliche Anwesenheit ablehnen.

3. Datenschutz- und Informationssicherheit

   Auf den Datenschutz und die Informationssichert gegenüber Dritten, hierzu zählen auch Familienangehörige und sonstige im Haushalt lebende Personen, ist im Privatbereich der Beschäftigten besonders zu achten.

   Die zu ergreifenden Schutzmaßnahmen sind gemessen am Schutzbedarf der zu bearbeitenden Daten dem Sicherheits- und Technikkonzept und der Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und beim mobilen Arbeiten vom **1. April 2022** zu entnehmen.

4. Arbeits- und Gesundheitsschutz

   Für die Dauer der Arbeitszeit sind am Arbeitsplatz die gesetzlichen Bestimmungen des Arbeitsschutzes sowie die allgemein anerkannten Regeln der Ergonomie zu beachten.

Die Dienstvereinbarung gemäß § 78 NPersVG über „Homeoffice und mobile Arbeit an der Leibniz Universität Hannover“ vom 1. April 2024 und die Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und beim mobilen Arbeiten vom 1. April 2022 wurden ausgehändigt.

Datum / Unterschrift

_____	_____
Dienststelle	antragstellende Person

Anlage 4:

Mobiles Arbeiten – Antrag

A Angaben der antragstellenden Person
Hiermit beantrage ich mobiles Arbeiten gemäß der **Dienstvereinbarung über Homeoffice und mobile Arbeit an der Leibniz Universität Hannover**.

Name, Vorname:			
Einrichtung:			
Diensttelefon:			
dienstliche E-Mail-Adresse:			
Zeitraum	3 Jahre ab:		
Ich habe einen Schwerbehindertenstatus gemäß § 2 Absatz 2 SGB IX oder einen Gleichgestelltenstatus gemäß § 2 Absatz 3 SGB IX.		Ja	Nein
Ich bin	☐ tarifbeschäftigt	☐ verbeamtet	

Ich bestätige, die Bestimmungen der **Dienstvereinbarung über Homeoffice und mobile Arbeit an der Leibniz Universität Hannover** zur Kenntnis genommen zu haben.

Insbesondere

- überschreite ich nicht die Obergrenze von 30 Prozent meiner Arbeitszeit im Kalenderhalbjahr und stimme die konkrete Inanspruchnahme des mobilen Arbeitens mit meiner/meinem Vorgesetzten ab,
- halte ich die Dienstanweisung zum Datenschutz und zur Informationssicherheit ein,
- halte ich die Hinweise zur Arbeitszeit und die Vorgaben der Arbeitssicherheit ein.

_____ _____

Ort, Datum Unterschrift der antragstellenden Person

B Stellungnahme der vorgesetzten Person

☐	Ich stimme dem Antrag auf mobiles Arbeiten zu. Die beschäftigte Person hat eine Kopie dieses genehmigten Antrags erhalten. Das Original wird an die für die Einrichtung zuständige Personalsachbearbeitung im Dezernat 2 weitergeleitet.
☐	Die notwendigen Arbeits- und Verbrauchsmittel für die mobile Arbeit, wie z. B. Schreibgeräte oder Laptops, werden bei Bedarf gestellt.
☐	Die zu verrichtenden Tätigkeiten sind für mobiles Arbeiten geeignet und entsprechen gem. Sicherheits- und Technikkonzept der aggregierten Risikoklasse ☐ unkritisch ☐ moderat ☐ kritisch. ☐ Es wurde entsprechend dem Sicherheits- und Technikkonzept ein geeignetes Technikszenario ausgewählt.
☐	Eine Unterweisung zu Arbeitssicherheit sowie Arbeits- und Gesundheitsschutz wird vor der Aufnahme der mobilen Arbeit stattfinden.

☐	Ich stimme dem Antrag auf mobiles Arbeiten aus folgenden Gründen nicht zu. Die Personalverwaltung wird hierüber informiert und entscheidet über den Antrag. Im Falle der Ablehnung wird der Personalrat beteiligt.

Bemerkungen:

_____
Ort, Datum

_____
Unterschrift der vorgesetzten Person

Anlage 5:

Hinweise zur Arbeitszeit im Rahmen von Homeoffice und mobilem Arbeiten

Auch im Rahmen von Homeoffice und mobilem Arbeiten gilt das Arbeitszeitgesetz (ArbZG). Beschäftigte sind mangels der Möglichkeit der Kontrolle durch die Vorgesetzten selbst verantwortlich für die Einhaltung des Arbeitszeitgesetzes.

Folgende Rahmenbedingungen sind dabei in der Regel zu beachten:

- Arbeitszeit ist die Zeit vom Beginn bis zum Ende der Arbeit ohne Ruhepausen, wobei sich Beginn und Ende nach den allgemeinen und individuellen Vorgaben innerhalb der Universität richten. Die jeweilige, für die Beschäftigte oder den Beschäftigten geltende Arbeitszeitregelung kann im Dezernat 2 erfragt werden.
- Die Höchstarbeitszeit gemäß § 3 ArbZG beträgt in der Regel 8 Stunden werktäglich (Montag bis Samstag), sie kann bis zu 10 Stunden betragen, wenn innerhalb von sechs Kalendermonaten oder innerhalb von 24 Wochen im Durchschnitt acht Stunden werktäglich nicht überschritten werden.
- Ruhepausen müssen eingehalten werden.
- Die Dauer der Ruhepausen beträgt nach 6 Stunden Arbeitszeit 30 Minuten und bei mehr als 9 Stunden weitere 15 Minuten.
- Es müssen Ruhezeiten, also Zeiten zwischen der Beendigung und Wiederaufnahme der Arbeit, in denen nicht gearbeitet werden darf, eingehalten werden.
- Die Ruhezeit beträgt mindestens 11 ununterbrochene Stunden.

Anlage 6:

Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit

vom 01.04.2022

§ 1 - Anwendungsbereich

Diese Dienstanweisung definiert spezielle Regelungen und Verhaltensmaßnahmen zur Einhaltung des Datenschutzes und der Informationssicherheit im Homeoffice und während der mobilen Arbeit.

§ 2 – Grundsätzliche Vorgaben

(1) Werden im Homeoffice oder während der mobilen Arbeit personenbezogene Daten verarbeitet, ist die dortige Arbeitsorganisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die geeignet sind:
   1. Unbefugten den Zutritt zu dienstlichen Geräten, an dem personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle),
   2. Zu verhindern, dass der häusliche oder mobile Arbeitsplatz von Unbefugten genutzt wird (Zugangskontrolle),
   3. Zu gewährleisten, dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (Zugriffskontrolle),
   4. Zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten erfolgt (Weitergabekontrolle).

(2) Bei Datenschutzverstößen oder Sicherheitsvorfällen ist unverzüglich der Datenschutzbeauftragte und/oder der/die Informationssicherheitsbeauftragte zu informieren. Die an der Leibniz Universität Hannover (LUH) etablierten Prozesse gelten auch im Rahmen des Arbeitens aus dem Homeoffice und während mobiler Arbeit.

§ 3 – Schutzbedarfsfeststellung

(1) Vor Aufnahme der Tätigkeit ist mit dem/der Vorgesetzten der Schutzbedarf der zu bearbeitenden personenbezogenen Daten nach dem Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen zu bestimmen, eine erste Orientierung der Einordnung bietet Tabelle 1. Etwaige Geheimhaltungsvereinbarungen sind in die Schutzbedarfsfeststellung einzubeziehen.
(2) Je höher der Schutzbedarf der zu bearbeitenden Daten eingestuft wird, desto höher sind die zu ergreifenden Datensicherheitsmaßnahmen.
(3) Daten der Schutzstufe E des Schutzstufenkonzepts der Landesbeauftragten für den Datenschutz Niedersachsen dürfen weder im Homeoffice noch während mobiler Arbeit verarbeitet werden.
(4) Beispiele von Datenkategorien und deren Schutzbedarf sind in Tabelle 1 aufgeführt.

§ 4 – Arbeitsplatzumgebung

(1) Die Arbeitsplatzumgebung ist gemessen an den auszuführenden Tätigkeiten so auszugestalten, dass vom Grundsatz her die Vertraulichkeit und Verfügbarkeit der Daten wie im Büro sichergestellt ist.
(2) Dies bedeutet insbesondere:
   - Der Arbeitsplatz ist so gewählt, dass unbefugte Dritte keinen Blick auf den Bildschirm und in die Papierunterlagen werfen können.
   - Es werden Sichtschutzfolien angeboten, wenn dies erforderlich ist.
   - Es gilt eine Clean-Desk-Policy, das bedeutet, dass beim Verlassen des Arbeitsplatzes alle Unterlagen sicher verschlossen werden und vor unberechtigten Zugriff geschützt werden müssen.

- Papierunterlagen können in Dokumentenmappen oder Schränken verschlossen werden.
- Fenster werden in Erdgeschosswohnungen bei Verlassen des Arbeitsplatzes immer geschlossen.
- Beim Verlassen des Arbeitsplatzes sind die Endgeräte zu sperren.
- Es wird darauf geachtet, dass vertrauliche Gespräche (z.B. Telefongespräche, Videokonferenzen) nicht von unbefugten Personen oder Sprachassistenten (z.B. Alexa, Siri) mitgehört werden

§ 5 – Genutzte Hardware

(1) Die genutzte Hardware ist durch angemessene Zugangsdaten zu schützen. Passwörter und Zugangsdaten dürfen unter keinen Umständen an Dritte (hierzu gehören auch Haushaltsangehörige) weitergegeben werden.
(2) Beim Transport der Hardware oder Nutzung dieser im öffentlichen Raum ist diese angemessen gegen Diebstahl und unbefugte Einsichtnahme zu schützen.
(3) Mobile Speichermedien und Festplatten sind gemäß Rundschreiben 20/2019 zu verschlüsseln.
(4) Bei der Verwendung privater Telefone, sind deren Anruflisten regelmäßig zu löschen. Bei Verwendung fremder IT-Systeme muss sichergestellt werden, dass alle Informationen, inklusiver temporärer Daten, nach Beendigung der jeweiligen Tätigkeit von den Geräten gelöscht werden.
(5) Das eingesetzte Technikszenario aus dem Sicherheits- und Technikkonzept zum Homeoffice und zur mobilen Arbeit ist zwingend einzuhalten.

§ 6 Umgang mit Papierdokumenten

(1) Beim Umgang und insbesondere während des Transportes von Papierdokumenten besteht ein erhöhtes Verlustrisiko und damit verbunden das Risiko eines meldepflichtigen Datenschutzvorfalls. Es dürfen daher nur die zwingend für die dienstliche Aufgabenerfüllung erforderlichen Dokumente außerhalb der Dienststelle transportiert werden. Diese werden in geeigneten Behältnissen (z.B. Mappen u.a. mit Name der Dienststelle im Falle eines Verlustes) transportiert.
(2) Beim Transport dürfen Papierdokumente nicht unbeaufsichtigt im öffentlichen Raum bleiben und sind so zu schützen, dass Dritte keine Einsicht nehmen können.
(3) Daten der Schutzstufe D sollen grundsätzlich nicht in Papierform im Homeoffice und während der mobilen Arbeit verarbeitet werden. Dies gilt insbesondere für Personalaktendaten oder Dokumente mit einer Vielzahl von Daten der Schutzstufe D.
(4) Soweit möglich, soll nicht mit den Originaldokumenten, sondern mit Kopien gearbeitet werden.
(5) Eine Entsorgung erfolgt nur über geeignete Aktenvernichter, die mindestens der Sicherheitsstufe 3 entsprechen.

§ 7 – Datenverarbeitung

(1) Die Speicherung von Daten hat grundsätzlich auf den üblichen Netzlaufwerken oder den von der LUH zentral zugelassenen Cloud-Speicherdiensten zu erfolgen. Nur so ist gewährleistet, dass die Daten regelmäßig gesichert werden und Datenverlust vermieden wird.
(2) Ausnahmen hiervon dürfen nur gemacht werden, wenn eine Verbindung zu den Netzlaufwerken oder Cloud-Speicherdiensten der LUH nicht möglich ist. Die Speicherung auf den Netzlaufwerken oder Cloud-Speicherdiensten der LUH ist unverzüglich nach Wiederherstellung einer Verbindung nachzuholen. Lokale Kopien von Daten sind anschließend zu löschen.
(3) Aufbewahrungs- und Löschfristen gelten auch für die im Homeoffice gelagerten Daten und Dokumente.

§ 8 – Inkrafttreten

Diese Dienstanweisung tritt mit ihrer Verkündung in Kraft.

Tabelle 1
Orientierungshilfe zur Einordnung der Schutzstufen nach Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen (LfD)

Schutzstufe	Erläuterung der jeweiligen Schutzstufe und welche personenbezogenen Informationen dieser Stufe im Regelfall zugeordnet werden können.	Typische Tätigkeiten an der LUH, bei denen im Regelfall Daten der jeweiligen Schutzstufe verarbeitet werden
A	Schutzstufe A betrifft Daten, die von den Betroffenen frei zugänglich gemacht wurden („Öffentlich zugängliche Daten“). Ebenfalls können dieser Gruppe auch Daten zugeordnet werden, die gar keine personenbezogenen Daten mehr enthalten („Anonyme Daten): • Angaben zu Personen, die zur Veröffentlichung freigegeben sind: ○ Kontaktangaben ○ Tätigkeitsbereiche ○ Publikationen • Weitere Personeninformationen, die aufgrund einer Einwilligung veröffentlicht werden dürfen: ○ Fotos, Video- und Audioaufnahmen ○ Lebensläufe, Profilinformationen ○ Persönliche Angaben • Lehrveranstaltungsbezogene Inhalte, die maximal Angaben zu den Urhebern enthalten: ○ Vorlesungsverzeichnis ○ Vorlesungsmaterialien/Skripte (ggfs. Urheberrechte beachten) ○ Übungsmaterialen (ggfs. Urheberrechte beachten)	- Gestaltung und Pflege von Webseiten - Erstellung universitätsbezogener Dokumente, die keine personenbezogenen Daten (bis auf evtl. Ansprechpersonen) enthalten: - Ordnungen, Satzungen, Dienstvereinbarungen, Vertragsmuster - Rundschreiben, Formulare, Merkblätter - Informationsmaterial - Konzepte - Entwicklung von Lehr- und Lernkonzepten und Lehrveranstaltungsmaterialen - Erstellung von Informationsmaterial für die Öffentlichkeitsarbeit (Flyer, Broschüren, Berichte)

B	Schutzstufe B betrifft Daten, deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden („Intern verfügbare Daten“). Hierbei handelt es sich zumeist um Daten, die nur einem bestimmten Personenkreis verfügbar gemacht werden sollen:
	
	• Dienstliche Daten der Beschäftigten, die die interne Organisation betreffen:
	  • Geschäftsverteilungspläne
	  • Organigramme, Arbeitsanweisungen,
	  • Post- und E-Mailverteiler
	  • Zuständigkeiten
	
	• Interne Kommunikationsdaten:
	  • Adressen
	  • Durchwahl
	  • LUH-ID
	
	• Tätigkeitsbezogene Angaben in Protokollen von hochschulöffentlichen Gremiensitzungen
	
	• Kontaktinformationen Dritter (Vertragspartner, Drittmittelgeber, Behörden und ähnlich verbundenen Einrichtungen)
		- Organisation und Abstimmung von Terminen mit internen und externen Einrichtungen
		- Fachberatung und Ticketsupport von Nutzenden der internen Systeme und Softwarelösungen, wenn dabei auf keine weiteren Daten der Schutzstufen C, D und E zugegriffen wird
		- Entwicklung und Pflege von internen Systemen und Software, wenn dabei auch Daten der Kategorie B verarbeitet werden
		- Verwaltung von Gebäuden und Koordinierung von Neu, Umbau- und Sanierungsarbeiten
		- Bekanntmachung von Wahlergebnissen
		- Einholung von Angeboten
		- Bestellvorgänge und Beschaffungen
		- Administration des Modulkatalogs

C	Schutzstufe C betrifft Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen") („Eingeschränkte Daten)": • Persönliche Daten von Mitarbeitenden/ Studierenden, soweit die Informationen nicht dem Schutzbedarf D oder E zuzuordnen sind: 1. Private Kontaktinformationen 2. Kontoinformationen 3. Stellenbewertung 4. Tätigkeitsbezogene Informationen (Teilnahme an Sitzungen, Gremien) • Veranstaltungsbezogene Teilnehmendeninformationen, wie etwa Anwesenheitslisten oder Kontaktlisten • Vertragsunterlagen (zu Dritten) ○ Rechnungen ○ Reise- und Lohnabrechnungen ○ Drittmittelverträge • Benutzernamen und Passwörter • Forschungsdaten, die noch persönliche Informationen der Teilnehmenden enthalten, die nicht den Schutzstufen D und E zuzuordnen sind. • Studien- und Prüfungsleistungen einzelner Veranstaltungen • Prüfungsergebnisse/Ergebnislisten einzelner Prüfungsleistungen • Individuelle Schließberechtigungen • Persönliche Angaben in Protokollen von nicht hochschulöffentlichen Gremiensitzungen • E-Mail und telefonische Kommunikationsinhalte, sofern keine Daten der Schutzstufe D und E ausgetauscht werden	- Zulassungsverfahren - Beratung von Studieninteressierten - Einschreibungsangelegenheiten (Nachweise, Zahlungseingänge) - Korrektur von Studien- und Prüfungsleistungen - Betreuung von Veranstaltungen in Stud.IP - Verwaltung und Kontrolle von Drittmittelprojekten - Personalkostenverwaltung - Veranstaltungsorganisation - Allgemeine Sekretariatsaufgaben, sofern keine sensiblen Daten (beispielsweise besondere Datenkategorien nach Art. 9 DSGVO) betroffen sind - Nutzung von lesendem SAP-Zugriff, sofern dabei kein Zugriff auf Daten der Schutzstufe D erfolgt - Betreuung rechtlicher Verfahren (Arbeitnehmererfindungen, BAföG-Angelegenheiten, Zulassungsverfahren), soweit keine Angelegenheiten der Schutzstufe D oder E betroffen sind - Organisation innerhalb der Einrichtung (Abstimmungen, Zugang zu Dokumenten, Terminkoordination, Fristenüberwachung) - Beratung und Betreuung von Studierenden zu lehrveranstaltungsbezogenen Themen - Informationsmanagement und Datenlieferung für Personalkostenbudgetierung, -bewirtschaftung und -planung - Organisation und Durchführung von Vergabeverfahren - Organisation und Verwaltung der Schließberechtigungen - Organisation und Abwicklung von Dienstreisen - Rechnungswesen - Systemadministration von Systemen soweit auf den Systemen keine Daten der Schutzstufe D verarbeitet werden - Ticketbearbeitung im User Help Desk

D	Schutzstufe D betrifft Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz") („Sensible Daten"): • Personalunterlagen und Personalakteninhalte (zu Beschäftigten) o Arbeitszeugnisse o Gesundheitsdaten o Krankmeldungen o Sozialdaten o Abwesenheitszeiten (Urlaub, Krankheit) o Leistungsbewertung o Bewerbungsunterlagen, o Gutachten im Berufungsverfahren • E-Mail und telefonische Kommunikationsinhalte, sofern auch Daten der Schutzstufe D ausgetauscht werden • Leistungsinformationen über Studierende (z.B. Prüfungsakte, Leistungsübersicht, Abschluss) • Daten besonderer Kategorien nach Art. 9 DSGVO • Forschungsergebnisse, sofern sensible Daten betroffen sind • Daten die der Geheimhaltung unterliegen	- Personalangelegenheiten - Nutzung von SAP, soweit dabei auch auf Personalaktendaten zugegriffen wird - Betreuung rechtlicher Verfahren im Personalwesen oder in Härtefall-Angelegenheiten - Untersuchungen der Innenrevision - Berufungs- und Bewerbungsverfahren - Beratung und Betreuung von Studierenden und Beschäftigten zu physischen und psychischen Belastungen, Härtefällen, usw). - Strafrechtliche Ermittlungsmaßnahmen - Systemadministration von Systemen soweit auf den Systemen Daten der Schutzstufe D verarbeitet werden.
E	Schutzstufe E betrifft Daten, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte („Hochsensible Daten") • Forschungsdaten, sofern hochsensible Daten betroffen sind • Bspw. Strafakten, Zeugenschutzprogramme	- Forschungsarbeiten mit Daten aus hochsensiblen Bereichen

Anlage 7:

Leibniz Universität IT Services (LUIS)

Sicherheits- und Technikkonzept für Homeoffice und mobiles Arbeiten

Stand: 17.03.2022

1. Einleitung

Dieses Konzept definiert die technischen Rahmenbedingungen für Arbeitsformen abseits des dienstlichen Arbeitsplatzes und außerhalb der Räume der Leibniz Universität Hannover (LUH). Die beiden betrachteten grundsätzlichen Modelle sind Homeoffice und mobiles Arbeiten, die sich sowohl aus technischer als auch organisatorischer Sicht zum Teil erheblich unterscheiden.

Die Einführung eines Konzepts zur Telearbeit (jetzt Homeoffice) wurde bereits 2011 vorgelegt und wird seitdem erfolgreich angewendet. Das Konzept zum mobilen Arbeiten ist durch die Einführung dieses Modells an der LUH durch das Präsidium der LUH in 2019 als zusätzlicher Baustein zur Flexibilisierung der Arbeit erforderlich geworden.

Homeoffice und mobiles Arbeiten werden neben diesem Konzept auch durch die „Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte an der Leibniz Universität Hannover“ („Mobilrichtlinie“)[2] reguliert.

2. Zielsetzung

Das Ziel dieses Konzepts ist der Schutz von Informationen, die während des Homeoffices bzw. der mobilen Arbeit gespeichert, verarbeitet und übertragen werden. Dazu werden typische Gefährdungen aufgezeigt und spezielle Anforderungen an die sichere Durchführung der gewählten Arbeitsform definiert.

Dieses Konzept legt für die technische und operative Modellierung von Homeoffice und mobilem Arbeiten das BSI Grundschutzkompendium (Bundesamt für Sicherheit in der Informationstechnik) Edition 2021 zugrunde[3]. Für die Ausformulierung der infrastrukturellen Maßnahmen unter Berücksichtigung der spezifischen Gefährdungslagen im Kontext der LUH werden im Kapitel 6 für den Arbeitsplatz im Privatbereich[4] sowie für den mobilen Arbeitsplatz[5] in Kapitel 7 behandelt.

In Ergänzung zum in der LUH etablierten Konzept mit stationären Endgeräten wird in diesem Konzept auch Homeoffice mit mobilen Endgeräten im Privatbereich betrachtet. Bei der Sicherheitsbeurteilung des mobilen Arbeitens hingegen wird das Augenmerk auf eine Vergleichbarkeit mit den Arbeitsformen Büroarbeit und Homeoffice gelegt. Diese kann nur durch ein koordiniertes Zusammenwirken technischer und organisatorischer Maßnahmen angenähert werden und ist insbesondere von zwei abhängigen Faktoren gekennzeichnet. Zum einen spielt der Ort der Datenverarbeitung eine wesentliche Rolle; das entstehende Risiko wird in diesem Konzept als Umgebungsrisiko beschrieben. Andererseits wird das Risiko wesentlich von der verwendeten Anwendung bestimmt. Dies wird als Sicherheitsdomänenrisiko bezeichnet. Die Sicherheitsaspekte der unterschiedlichen technischen Konzepte für bestimmte Endgerätekonstellationen werden gemäß der BSI Standard-Anforderung OPS.1.2.4.A6 „Erstellen eines Sicherheitskonzeptes“ betrachtet.

3. Abgrenzung und Modellierung

Dieses Konzept[6] konzentriert sich zunächst auf Homeoffice und mobile Arbeit, die im Privatbereich durchgeführt wird[7]. Es wird davon ausgegangen, dass zwischen dem Homeoffice-Arbeitsplatz bzw. der mobilen Arbeitsstätte und der jeweiligen Einrichtung eine sichere Telekommunikationsverbindung

---

[2] Verkündungsblatt 10/2021 der Gottfried Wilhelm Leibniz Universität Hannover vom 25.06.2021

[3] Konkret wird der Prozessbaustein OPS.1.2.4 für beide Arbeitsformen herangezogen.

[4] vgl. BSI Infrastrukturbaustein INF.8

[5] vgl. BSI Infrastrukturbaustein INF.9

[6] Der diesem Konzept zugrundeliegende BSI Baustein OPS.1.2.4 ist für jeden Tele- und Mobilarbeitsplatz anzuwenden.

[7] lt. BSI „heimbasierte Telearbeit“

besteht, die es ermöglicht, geeignet Informationen auszutauschen und auf Daten auf dem Server der Einrichtungen zuzugreifen. Die Anforderungen dieses Bausteins umfassen die folgenden drei Bereiche:

• die Organisation von Homeoffice und mobiler Arbeit,

• das Endgerät der beschäftigten Person und

• die Kommunikationsverbindung zwischen Endgerät und Einrichtung.

Sicherheitsanforderungen an die Infrastruktur des Homeoffice-Arbeitsplatzes werden in diesem Kapitel nicht berücksichtigt, sondern sind im Abschnitt 0 beschrieben. Anforderungen an einen nichtdauerhaft eingerichteten (mobilen) Arbeitsplatz sind im Abschnitt 0 dieses Konzepts zu finden. Detaillierte Empfehlungen, wie die IT-Systeme konkret konfiguriert und abgesichert werden können, werden nicht im Rahmen dieses Konzepts behandelt, Kapitel 6 soll dazu Handlungsempfehlungen geben[8].

4. Zuständigkeiten

Die vorgesetzte Person, die dem Homeoffice oder der mobilen Arbeit der Beschäftigten zustimmt, ist für die Auswahl und Einhaltung eines angemessenen Technikszenarios verantwortlich. Die vorgesetzte Person nimmt für die verwendeten Sicherheitsdomänen (z. B. einrichtungsspezifische Anwendungen und Daten) der Beschäftigten eine Schutzbedarfsfeststellung vor und nimmt das festgestellte Restrisiko in Kauf.

Grundsätzlich ist die mit Informationssicherheit beauftragte Person (ISB) der Einrichtung oder Fakultät dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Technikszenario erfüllbar sind und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben.

Beschäftigte in Homeoffice oder mobiler Arbeit sind grundsätzlich für die Erfüllung des festgelegten Technikszenarios am jeweiligen Arbeitsplatz verantwortlich, soweit dies in ihrer Gewalt liegt.

Gemäß der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" der LUH sind Beschäftigte, die private Geräte für dienstliche Zwecke nutzen, für die Einhaltung der festgelegten Sicherheitsmaßnahmen in Bezug auf Endgerät, Arbeitsort und verwendeter Infrastruktur persönlich verantwortlich.

5. Handhabung des Technikkonzepts

Die vorgesetzten Personen können anhand der Kapitel 6 bis 8, die als Checkliste dienen sollen, mit den Beschäftigten die Risiken für die Tätigkeiten einschätzen, die in Homeoffice oder mobiler Arbeit entstehen können und sie damit für die Gefährdungslage sensibilisieren, und anschließend ein geeignetes Technikszenario auswählen. Bei Bedarf können die Informationssicherheitsbeauftragten beratend hinzugezogen werden. Hierzu ist der Schutzbedarf der konkreten Tätigkeiten im Homeoffice oder mobilem Arbeiten (Kap. 0), mit den organisatorischen Risiken (Kap. 0), den Risiken der Arbeitsumgebung (Kap. 0) und der Sicherheitsumgebung (Kap. 0) sowie mit der Arbeitsform fester Arbeitsplatz im Privatbereich (Kap. 0) oder mobiler Arbeitsplatz (Kap. 0) in Einklang zu bringen mit der ausgewählten technischen Ausstattung (Kap. 0), um die Risiken bestmöglich zu minimieren. IT-Beauftragte oder Systemadministratoren der Einrichtung können beratend hinzugezogen werden.

Die im BSI formulierten Risiken sind jeweils in grau hinterlegt dargestellt, bereits ergriffene Maßnahmen seitens der LUH werden als blau gerahmte Hinweise aufgeführt.

[8] Empfehlungen sind in SYS.2.1 „Allgemeiner Client“ sowie in den betriebssystemspezifischen Systembausteinen zu finden. Weitere für die Telearbeit relevante Sicherheitsaspekte, wie z. B. für WLAN, werden in den Bausteinen der Teilschichten NET.2 „Funknetze“ oder NET.4 „Telekommunikation“ betrachtet. Sofern Daten, die bei der Telearbeit verändert wurden, nicht unmittelbar auf IT-Systemen der Einrichtung gespeichert werden, muss geregelt werden, wie eine Datensicherung durchgeführt wird. Anforderungen dazu sind im Baustein CON.3 „Datensicherungskonzept“ zu finden.

6. Gefährdungslage

6.1 Datenschutzstufenkonzept der Landesbeauftragten für den Datenschutz (LfD) Niedersachsen

Im Rahmen der Risikobetrachtung ist eine Klassifizierung der zugreifbaren Daten und der Arbeitsorte notwendig. Dazu wird auf das Schutzstufenkonzept der LfD Niedersachsen zurückgegriffen. In der Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit wurden die Schutzstufenvorgaben der LfD um Beispiele aus dem universitären Arbeitsumfeld ergänzt:

Tabelle 1

Orientierungshilfe zur Einordnung der Schutzstufen nach Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen (LfD)

Schutzstufe	Erläuterung der jeweiligen Schutzstufe und welche personenbezogenen Informationen dieser Stufe im Regelfall zugeordnet werden können.	Typische Tätigkeiten an der LUH, bei denen im Regelfall Daten der jeweiligen Schutzstufe verarbeitet werden
A	Schutzstufe A betrifft Daten, die von den Betroffenen frei zugänglich gemacht wurden („Öffentlich zugängliche Daten“). Ebenfalls können dieser Gruppe auch Daten zugeordnet werden, die gar keine personenbezogenen Daten mehr enthalten („Anonyme Daten): • Angaben zu Personen, die zur Veröffentlichung freigegeben sind: ○ Kontaktangaben ○ Tätigkeitsbereiche ○ Publikationen • Weitere Personeninformationen, die aufgrund einer Einwilligung veröffentlicht werden dürfen: ○ Fotos, Video- und Audioaufnahmen ○ Lebensläufe, Profilinformationen ○ Persönliche Angaben • Lehrveranstaltungsbezogene Inhalte, die maximal Angaben zu den Urhebern enthalten: ○ Vorlesungsverzeichnis ○ Vorlesungsmaterialien/Skripte (ggfs. Urheberrechte beachten) ○ Übungsmaterialen (ggfs. Urheberrechte beachten)	- Gestaltung und Pflege von Webseiten - Erstellung universitätsbezogener Dokumente, die keine personenbezogenen Daten (bis auf evtl. Ansprechpersonen) enthalten: - Ordnungen, Satzungen, Dienstvereinbarungen, Vertragsmuster - Rundschreiben, Formulare, Merkblätter - Informationsmaterial - Konzepte - Entwicklung von Lehr- und Lernkonzepten und Lehrveranstaltungsmaterialen - Erstellung von Informationsmaterial für die Öffentlichkeitsarbeit (Flyer, Broschüren, Berichte)

B	Schutzstufe B betrifft Daten, deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden („Intern verfügbare Daten“). Hierbei handelt es sich zumeist um Daten, die nur einem bestimmten Personenkreis verfügbar gemacht werden sollen:
	• Dienstliche Daten der Beschäftigten, die die interne Organisation betreffen:
	  • Geschäftsverteilungspläne
	  • Organigramme, Arbeitsanweisungen,
	  • Post- und E-Mailverteiler
	  • Zuständigkeiten
	• Interne Kommunikationsdaten:
	  • Adressen
	  • Durchwahl
	  • LUH-ID
	• Tätigkeitsbezogene Angaben in Protokollen von hochschulöffentlichen Gremiensitzungen
	• Kontaktinformationen Dritter (Vertragspartner, Drittmittelgeber, Behörden und ähnlich verbundenen Einrichtungen)
		- Organisation und Abstimmung von Terminen mit internen und externen Einrichtungen
		- Fachberatung und Ticketsupport von Nutzenden der internen Systeme und Softwarelösungen, wenn dabei auf keine weiteren Daten der Schutzstufen C, D und E zugegriffen wird
		- Entwicklung und Pflege von internen Systemen und Software, wenn dabei auch Daten der Kategorie B verarbeitet werden
		- Verwaltung von Gebäuden und Koordinierung von Neu, Umbau- und Sanierungsarbeiten
		- Bekanntmachung von Wahlergebnissen
		- Einholung von Angeboten
		- Bestellvorgänge und Beschaffungen
		- Administration des Modulkatalogs

C	Schutzstufe C betrifft Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen”) („Eingeschränkte Daten)“:
	• Persönliche Daten von Mitarbeitenden/ Studierenden, soweit die Informationen nicht dem Schutzbedarf D oder E zuzuordnen sind:
	  5. Private Kontaktinformationen
	  6. Kontoinformationen
	  7. Stellenbewertung
	  8. Tätigkeitsbezogene Informationen (Teilnahme an Sitzungen, Gremien)
	• Veranstaltungsbezogene Teilnehmendeninformationen, wie etwa Anwesenheitslisten oder Kontaktlisten
		- Zulassungsverfahren
		- Beratung von Studieninteressierten
		- Einschreibungsangelegenheiten (Nachweise, Zahlungseingänge)
		- Korrektur von Studien- und Prüfungsleistungen
		- Betreuung von Veranstaltungen in Stud.IP
		- Verwaltung und Kontrolle von Drittmittelprojekten
		- Personalkostenverwaltung
		- Veranstaltungsorganisation
		- Allgemeine Sekretariatsaufgaben, sofern keine sensiblen Daten (beispielsweise besondere Datenkategorien nach Art. 9 DSGVO) betroffen sind
		- Nutzung von lesendem SAP-Zugriff, sofern dabei kein Zugriff auf Daten der Schutzstufe D erfolgt
		- Betreuung rechtlicher Verfahren (Arbeitnehmererfindungen, BA-

	• Vertragsunterlagen (zu Dritten)
	  ○ Rechnungen
	  ○ Reise- und Lohnabrechnungen
	  ○ Drittmittelverträge
	• Benutzernamen und Passwörter
	• Forschungsdaten, die noch persönliche Informationen der Teilnehmenden enthalten, die nicht den Schutzstufen D und E zuzuordnen sind.
	• Studien- und Prüfungsleistungen einzelner Veranstaltungen
	• Prüfungsergebnisse/Ergebnislisten einzelner Prüfungsleistungen
	• Individuelle Schließberechtigungen
	• Persönliche Angaben in Protokollen von nicht hochschulöffentlichen Gremiensitzungen
	• E-Mail und telefonische Kommunikationsinhalte, sofern keine Daten der Schutzstufe D und E ausgetauscht werden
		föG-Angelegenheiten, Zulassungsverfahren), soweit keine Angelegenheiten der Schutzstufe D oder E betroffen sind
		- Organisation innerhalb der Einrichtung (Abstimmungen, Zugang zu Dokumenten, Terminkoordination, Fristenüberwachung)
		- Beratung und Betreuung von Studierenden zu lehrveranstaltungsbezogenen Themen
		- Informationsmanagement und Datenlieferung für Personalkostenbudgetierung, -bewirtschaftung und -planung
		- Organisation und Durchführung von Vergabeverfahren
		- Organisation und Verwaltung der Schließberechtigungen
		- Organisation und Abwicklung von Dienstreisen
		- Rechnungswesen
		- Systemadministration von Systemen soweit auf den Systemen keine Daten der Schutzstufe D verarbeitet werden
		- Ticketbearbeitung im User Help Desk

D	Schutzstufe D betrifft Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz") („Sensible Daten"):
	• Personalunterlagen und Personalakteninhalte (zu Beschäftigten)
	  ○ Arbeitszeugnisse
	  ○ Gesundheitsdaten
	  ○ Krankmeldungen
	  ○ Sozialdaten
	  ○ Abwesenheitszeiten (Urlaub, Krankheit)
	  ○ Leistungsbewertung
	  ○ Bewerbungsunterlagen,
	  ○ Gutachten im Berufungsverfahren
	• E-Mail und telefonische Kommunikationsinhalte, sofern auch Daten der Schutzstufe D ausgetauscht werden
		- Personalangelegenheiten
		- Nutzung von SAP, soweit dabei auch auf Personalaktendaten zugegriffen wird
		- Betreuung rechtlicher Verfahren im Personalwesen oder in Härtefall-Angelegenheiten
		- Untersuchungen der Innenrevision
		- Berufungs- und Bewerbungsverfahren
		- Beratung und Betreuung von Studierenden und Beschäftigten zu physischen und psychischen Belastungen, Härtefällen, usw).
		- Strafrechtliche Ermittlungsmaßnahmen
		- Systemadministration von Systemen soweit auf den Systemen Daten der Schutzstufe D verarbeitet werden.

	• Leistungsinformationen über Studierende (z.B. Prüfungsakte, Leistungsübersicht, Abschluss) • Daten besonderer Kategorien nach Art. 9 DSGVO • Forschungsergebnisse, sofern sensible Daten betroffen sind • Daten die der Geheimhaltung unterliegen	
E	Schutzstufe E betrifft Daten, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte („Hochsensible Daten“) • Forschungsdaten, sofern hochsensible Daten betroffen sind • Bspw. Strafakten, Zeugenschutzprogramme	- Forschungsarbeiten mit Daten aus hochsensiblen Bereichen

Tabelle 1: Datenschutzstufen

6.2 Konkrete Gefährdungen für Homeoffice und mobile Arbeit

Folgende organisatorische Bedrohungen und Schwachstellen sind für Homeoffice und mobile Arbeit von besonderer Bedeutung. Dieser und die Abschnitte 6 und 7 können als Checkliste verwendet werden, um Beschäftigte in Homeoffice oder mobiler Arbeit für die Gefährdungslage zu sensibilisieren und bestehende Maßnahmen und Regelungen näher zu bringen[9].

Fehlende oder unzureichende Regelungen für den Telearbeitsplatz

Die Nutzung eines Telearbeitsplatzes erfordert ergänzende organisatorische Absprachen zwischen Beschäftigten und Vorgesetzten. Zudem brauchen sie Handlungsanweisungen für den Fall, dass sicherheitsrelevante Vorkommnisse am Telearbeitsplatz eintreten. Gelangen beispielsweise vertrauliche Informationen in die Hände Unbefugter, können schwerwiegende Folgen für die Einrichtung entstehen.

Regelungen zum Homeoffice-Arbeitsplatz wurden zentral für alle Einrichtungen der LUH erlassen und sind somit sichergestellt über die

- „Dienstvereinbarung über Homeoffice und Mobile Arbeit“
- „Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit“

Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners

Im Privatbereich kann leichter nicht geprüfte und nicht freigegebene Hard- oder Software eingesetzt werden und so durch unbedachtes Handeln beispielsweise Schadsoftware auf den Telearbeitsrechner gelangen. Dadurch könnten vertrauliche Informationen kompromittiert werden.

Es könnte z. B. der fehlende Zugriff auf die gewohnte Büro-Arbeitsumgebung Beschäftigte dazu verleiten, bestimmte Problemstellungen durch einen „Workaround“ zu lösen.

[9] Die Formulierungen der Schwachstellen sind aus dem BSI-Baustein OPS.1.2.4 entnommen. Bereits ergriffene Maßnahmen seitens der LUH werden als gerahmte Hinweise aufgeführt.

Nutzende arbeiten gemäß der „Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte“ nicht mit administrativen Rechten.

Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Beschäftigten

Haben Beschäftigte keine festen Arbeitszeiten am Telearbeitsplatz und werden keine festen Zeiten vereinbart, an denen er erreichbar sein muss, kann aufgrund dessen der Arbeitsablauf verzögert werden und evtl. bei Sicherheitsvorfällen u. U. eine unverzügliche Kontaktaufnahme nicht erfolgen.

Die Erreichbarkeit ist in der „Dienstvereinbarung über Homeoffice und Mobile Arbeit“ geregelt.

Mangelhafte Einbindung der Beschäftigten in den Informationsfluss

Da Beschäftigte nicht täglich in der Einrichtung sind, haben sie weniger Gelegenheit, am direkten Informationsaustausch mit Vorgesetzten und Arbeitskollegen teilzuhaben. Es ist daher möglich, dass Telearbeiter insbesondere mündlich weitergegebene Informationen nicht oder erst verzögert erhalten. Hierdurch können Arbeitsabläufe und betriebliche Prozesse gestört und die Produktivität der Beschäftigteneingeschränkt werden.

Zur Aufrechterhaltung der Kommunikationsfähigkeit sollten alle zur Verfügung gestellten Mittel ausgeschöpft werden. Neben dem Telefon stehen auch von der LUH zentral betriebene Chat und Videokonferenzsysteme bereit.

Nichtbeachtung von Sicherheitsmaßnahmen

Am Telearbeitsplatz können beispielsweise fehlende Kontrollmöglichkeiten dazu führen, dass Beschäftigte empfohlene oder angeordnete Sicherheitsmaßnahmen nicht oder nicht in vollem Umfang umsetzen. So können z. B. vertrauliche Informationen in die Hände Dritter geraten.

Folgende technische Bedrohungen treten darüber hinaus im Kontext der LUH auf:

Einsichtnahme auf das Gerät durch Nichtberechtigte Personen

Als nichtberechtigte Personen sind alle LUH internen und externen Personen zu verstehen, die keinen Zugriff auf die schützenswerten Daten erhalten dürfen. Dies können im Rahmen der Telearbeit insb. neben Fremden auch Personen desselben Haushaltes der oder des Beschäftigten sein.

Neben der Umsetzung der „Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte“ in Bezug auf Bildschirmsperren können auch Sichtschutzfolien für Bildschirme in Erwägung gezogen werden.

Umfeld des Endgerätes

Einbindung des Endgerätes in eine potenziell als unsicher und kompromittiert anzunehmende Arbeitsumgebung wie z.B. ein privates Netzwerk.

Beachtung der „Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit“ in Bezug auf die Arbeitsumgebung (z.B. Sprachassistenten)

Fehlendes Monitoring

Fehlende netzwerktechnische Überwachung (Monitoring) und Absicherung (Firewall) beim Arbeiten außerhalb des universitären Netzwerkes.

Regelungen in der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" (Endgerätemaßnahmen zur Reduktion des Risikos), Always-on-VPN

Kompromittierende Zugriffe

Gefahr der kompromittierten Datenübertragung/Datenzugriff auf das universitäre Netzwerk, durch das Gewähren von für das mobile Arbeiten, notwendiger Zugriffe.

Insbesondere der Zugriff auf die „Instituts-VPNs“ birgt ein Risiko für das gesamte Netzsegment der betreffenden Einrichtung, da hier meist nicht mit Koppelnetzen gearbeitet wird. Ein vermeintlich

sicherer VPN-Zugang sichert zwar den Kanal gegen Abhören, stellt – einmal etabliert - jedoch einen direkten Zugang zu weiteren Ressourcen dar.

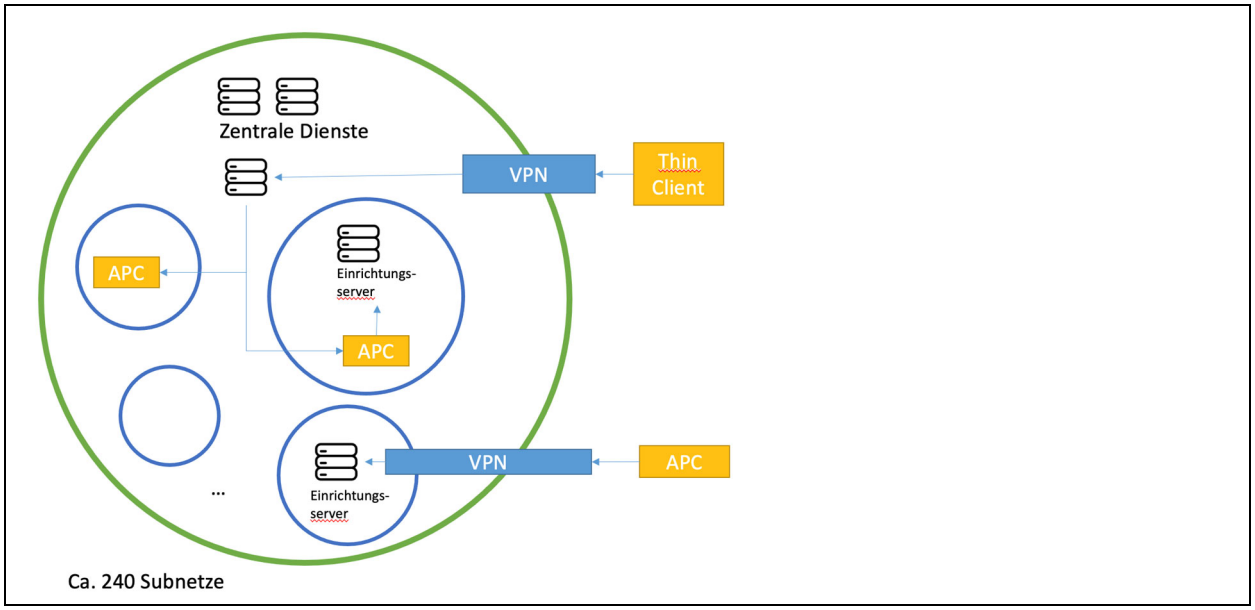

Abbildung 1: Zentral- und Einrichtungs-VPN

Physischer Zugriff

Höhere Gefahr, des Zugriffs fremder Personen auf das Endgerät. Manipulation der Endgeräte, z.B. durch anschließen von USB-Sticks mit Mal- oder Spyware.

Geregelt durch "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" und "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit".

Verlust Endgeräte / Manipulation

Bei der Verwendung von mobilen Geräten besteht die Gefahr des Verlustes oder des Zugriffs auf das Endgerät beim Wechsel des Arbeitsortes zwischen dem universitären Arbeitsplatz und dem externen Arbeitsort.

Fehlende Updates

Gefahr der Kompromittierung durch Schadsoftware, wenn längere Zeit keine Updates eingespielt werden können.

Mögliche Maßnahmen können sein: Always-on-VPN, organisatorische Regelungen: VPN durch Beschäftigte manuell mindestens alle 2-Tage aufbauen.

Einbringen kompromittierter Systeme

Gefahr der Einbringung von Viren und Schadsoftware, wenn ein extern kompromittiertes Endgerät wieder in das universitäre Datennetz eingebracht wird.

Alle Endgeräte, die mit dem Netz der LUH intern oder über VPN verbunden werden, müssen der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" genügen. Dies umfasst z. B. stets aktuelle Betriebssystem- und Antivirensoftware.

6.3 Umgebungsrisiko

Ohne weitreichende technische Maßnahmen auf dem Endgerät sind die vorgenannten Risiken im Rahmen des mobilen Arbeitens, ohne fest definierte Arbeitsumgebung signifikant höher als beim Homeoffice mit festgelegtem und definiertem Arbeitsort.

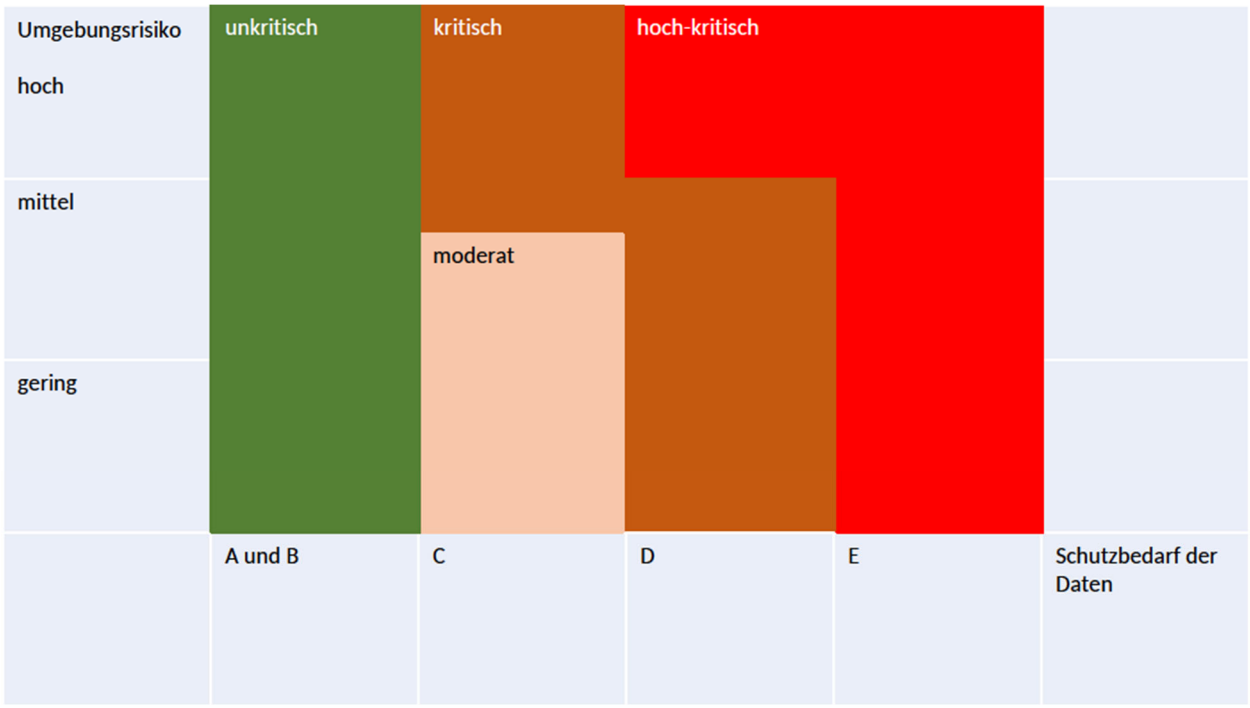

Abbildung 2: Umgebungsrisiko

In diesem Konzept wird von der gut zu begründenden Annahme ausgegangen, dass das Arbeiten am dienstlichen Arbeitsplatz aufgrund der dort getroffenen baulichen und organisatorischen Maßnahmen „kein“ erhöhtes Risiko hinsichtlich der Ortswahl bedeutet. Im Gegensatz dazu ist davon auszugehen, dass der Arbeitsplatz im Privatbereich regelmäßig eine geringfügig erhöhte Gefährdung von Daten und Zugängen mit sich bringt, sofern die für Homeoffice definierten technischen Randbedingungen stationär installierter Endgeräte ohne lokale Datenhaltung eingehalten werden. Das Risiko wird hier als „gering“ bezeichnet. Wird am Arbeitsplatz im Privatbereich ein mobiles Endgerät verwendet, so steigt das Risiko in den Bereich „mittel“, da zusätzlich zum Ort das Endgerät mit lokal gespeicherten Betriebs- und Zugangsdaten wegen Diebstahls oder Verlusts gefährdet ist. Das Risiko mobiler Endgeräte ohne weitere technisch-organisatorische Schutzmaßnahmen im öffentlichen Raum (Park, Café, Bahn) schließlich ist mit „hoch“ zu bewerten, da hier sowohl die Gefährdung durch Diebstahl oder Verlust signifikant erhöht ist, die Gefährdung durch Einsichtnahme Dritter (direkt oder z.B. durch Videokameras) auf das Gerät erhöht ist und zusätzlich potenziell mobile/unsichere Netzwerkverbindungen genutzt werden.

Unter dem Gesichtspunkt des Umgebungsrisikos ergeben sich in Verbindung mit den Datenschutzstufen unterschiedliche technische Voraussetzungen, die für eine Verarbeitung spezifisch schutzbedürftiger Daten in der gewählten Umgebung erforderlich sind. Unter Punkt 0 werden verschiedene Konzepte aufgezeigt, um die Umgebungsrisiken abzumildern. Dabei entsprechen die hier verwendeten Schutzstufen denen der LfD in Tabelle 1für personenbezogene Daten oder werden von der verantwortlichen Einrichtung, die dem Homeoffice oder der mobilen Arbeit der Beschäftigten zustimmt, im Rahmen einer Schutzbedarfsfeststellung auf die verwendeten Stufen A-E abgebildet.

6.4 Sicherheitsdomänenrisiko

Neben dem Umgebungsrisiko hängt die Gefahr für verarbeitete Daten auch von der Sicherheitsdomäne ab, auf die ein Zugriff beabsichtigt wird. Eine Sicherheitsdomäne kann ein Netzwerksegment, ein Anwendungskontext oder eine auf geeignete Weise logisch abgrenzbare Ressource oder Ressourcensammlung sein. Durch die Öffnung eines Netzsegmentes durch VPN nach außen ergibt sich eine höhere Gefährdung für das interne Netz. Die höchste Schutzstufe verarbeiteter Daten im selben Netzsegment bestimmt das Domänenrisiko für das entsprechende Teilnetz.

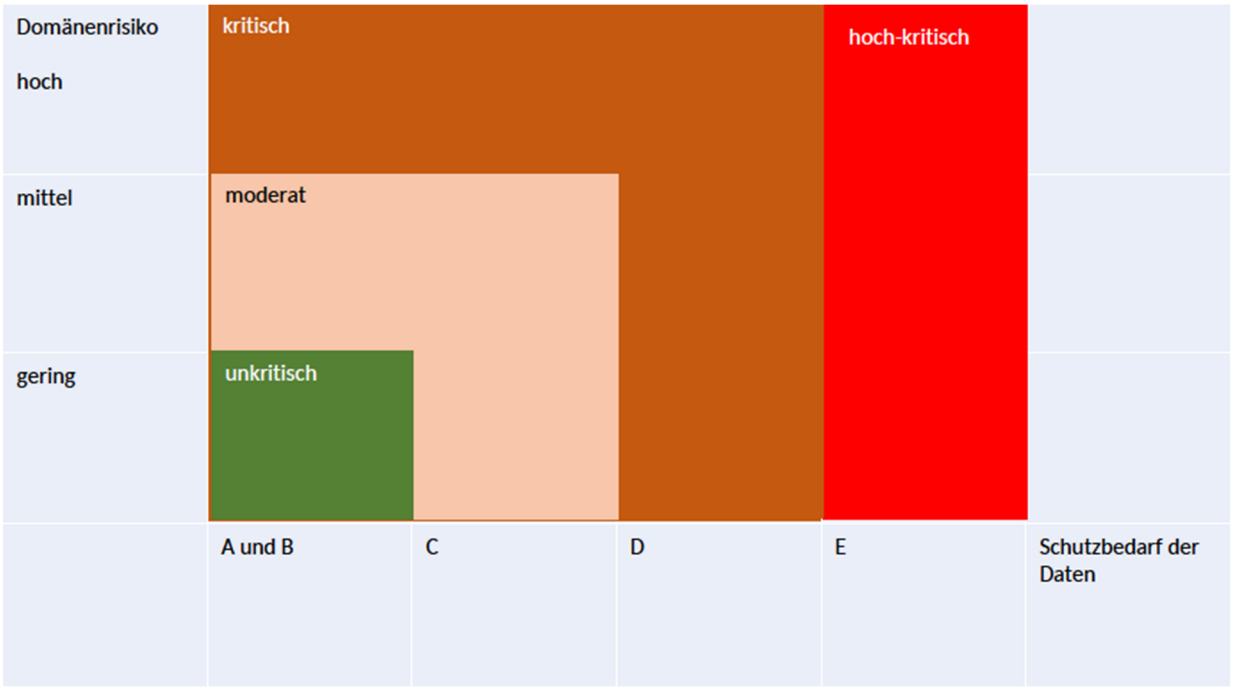

Abbildung 3: Sicherheitsdomänenrisiko

Das Risiko wird hier in der Form auf den Schutzbedarf von Daten abgebildet, sodass die Stufen A und B ein geringes Risiko bedeuten. Der Zugriff auf Sicherheitsdomänen der Schutzstufe C wird mittleres Risiko gedeutet, wohingegen der Zugriff auf Domänen der Stufe D als kritisch eingestuft werden. Eine Verarbeitung von Daten der Schutzstufe E wird als hoch-kritisch klassifiziert und ist im Kontext von Homeoffice und mobilem Arbeiten ausgeschlossen.

7. Arbeitsplatz im Privatbereich

Der Einsatz eines Arbeitsplatzes im Privatbereich[10] wird im BSI Grundschutz im Infrastrukturbaustein INF.8 beschrieben. Die dort aufgeführten Modellierungen und Maßnahmen gelten im Grundsatz und werden hier im Kontext der LUH ausformuliert.

7.1 Begriffsbestimmung

Im Gegensatz zum Arbeitsplatz im Büro nutzen Beschäftigte in Homeoffice einen Arbeitsplatz im Privatbereich. Dabei muss ermöglicht werden, dass die berufliche Umgebung hinreichend von der privaten getrennt ist. Wenn Mitarbeitende Arbeitsplätze im Privatbereich dauerhaft benutzen, müssen zudem diverse rechtliche Anforderungen erfüllt sein, die durch die entsprechende Dienstvereinbarung spezifiziert werden.

Für die LUH mit der "Dienstvereinbarung über Homeoffice und Mobile Arbeit" geregelt.

Bei einem Arbeitsplatz im Privatbereich kann nicht die gleiche infrastrukturelle Sicherheit vorausgesetzt werden, wie sie in den Büroräumen einer Einrichtung anzutreffen ist. So ist z. B. der Arbeitsplatz oft auch für Besucher oder Familienangehörige zugänglich. Deshalb müssen Maßnahmen ergriffen werden, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum in Annäherung vergleichbar ist.

In diesem Abschnitt wird aufgezeigt, wie sich die Infrastruktur eines Arbeitsplatzes im Privatbereich sicher aufbauen und betreiben lässt. Kernziel des Abschnitts ist der Schutz der Informationen der Einrichtung am Arbeitsplatz im Privatbereich.

Dieses Kapitel enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, um den Gefährdungen für einen Arbeitsplatz im Privatbereich entgegenwirken zu können[11]. Dabei werden

[10] In anderem Zusammenhang auch „häuslicher Arbeitsplatz“

[11] Der BSI-Baustein INF.8 „Häuslicher Arbeitsplatz“ ist für alle Räume anzuwenden, die als Homeoffice-Arbeitsplatz genutzt werden.

jedoch nur spezifische Anforderungen an die Infrastruktur für einen ortsfesten Arbeitsplatz mit Zugang durch Dritte definiert. Sicherheitsanforderungen für die eingesetzten IT-Systeme, z. B. Clients und Multifunktionsgeräte und insbesondere für die technischen Anteile des Homeoffices, z. B. Kommunikationsverbindungen, sind dagegen nicht Gegenstand des vorliegenden Bausteins[12].

7.2 Spezifische Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind von besonderer Bedeutung[13].

Fehlende oder unzureichende Regelungen für den Arbeitsplatz im Privatbereich

Da ein Arbeitsplatz im Privatbereich außerhalb der Einrichtung liegt, sind die Beschäftigten dort weitgehend auf sich allein gestellt. Dadurch können durch fehlende oder unzureichende Regelungen für das Arbeitsplatzumfeld im Privatbereich IT-Probleme mit höheren Ausfallzeiten entstehen. Wenn IT-Probleme nicht per Fernadministration geklärt werden können, muss beispielsweise ein Ersatzgerät zur Verfügung gestellt werden. Im schlechtesten Fall kann in dieser Zeit nicht gearbeitet werden. Wenn der Umgang mit internen und vertraulichen Informationen am Arbeitsplatz im Privatbereich nicht nachvollziehbar geregelt ist, könnten Beschäftigte solche Informationen falsch aufbewahren. Wenn nicht verhindert werden kann, dass Informationen ausgespäht oder modifiziert werden, kann die Vertraulichkeit und Integrität der Informationen gefährdet sein.

Die Aufbewahrung vertraulicher Informationen am häuslichen Arbeitsplatz sind in der "Dienstvereinbarung über Homeoffice und Mobile Arbeit" geregelt.

Als zusätzliche Maßnahme kann z.B. der Fernwartungsdienst ISLonline des LUIS .

Unbefugter Zutritt zu schutzbedürftigen Räumen des Arbeitsplatzes im Privatbereich

Räume eines Arbeitsplatzes im Privatbereich, in denen schutzbedürftige Informationen aufbewahrt und weiterverarbeitet werden oder in denen schutzbedürftige Geräte aufbewahrt oder betrieben werden, werden dadurch zu schutzbedürftigen Räumen. Wenn unbefugte Personen diese Räume unbeaufsichtigt betreten können, ist die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten und Informationen erheblich gefährdet. Beispiele:

• Ein Beschäftigter hatte Zuhause zwar ein separates Arbeitszimmer eingerichtet, aber es nicht konsequent abgeschlossen. Als seine kleinen Kinder kurz unbeaufsichtigt waren, spielten sie in dem nicht verschlossenen Arbeitszimmer. Dabei wurden wichtige Dokumente als Malgrundlage verwendet.

• Als eine Beschäftigte am Arbeitsplatz im Privatbereich in eine Projektarbeit vertieft war, bekam sie überraschend Besuch. Während sie in der Küche Kaffee kochte, wollte der Besuch am nicht gesperrten Computer schnell etwas im Internet recherchieren und hat diesen dabei versehentlich mit Schadsoftware infiziert.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" geregelt (Endgeräte sperren).

Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen am Arbeitsplatz im Privatbereich

Ein nicht nach ergonomischen Gesichtspunkten eingerichteter Arbeitsplatz im Privatbereich oder ein ungünstiges Arbeitsumfeld können dazu führen, dass dort nicht ungestört gearbeitet werden kann. Auch die verwendete IT kann möglicherweise nicht oder nicht optimal benutzt werden. Ungünstig auswirken können sich etwa Lärm, Störungen durch Familienmitglieder sowie eine schlechte Beleuchtung oder Belüftung. Dadurch werden Arbeitsabläufe und Beschäftigtenpotenziale eingeschränkt. Es könnten sich bei der Arbeit auch Fehler einschleichen. Außerdem kann der Schutz der Integrität von Daten vermindert werden.

Mit der Unterweisung zu Arbeitssicherheit und mit zur Verfügung gestellter Technik zu gewährleisten.

[12] Sie werden im BSI-Baustein OPS.1.2.4 „Telearbeit“ bzw. in den jeweiligen systemspezifischen Bausteinen beschrieben.

[13] Gemäß BSI-Baustein INF.8 „Häuslicher Arbeitsplatz“; die Formulierungen zur Gefährdungslage sind diesem BSI-Baustein entnommen und durch gerahmte Hinweise zur Umsetzung in der LUH ergänzt

Im Rahmen der Telearbeit wird der Arbeitsplatz im Rahmen der Arbeitsschutzverordnung bewertet und Empfehlungen ausgesprochen. Ungesicherter Akten- und Datenträgertransport

Wenn Dokumente, Datenträger oder Akten zwischen der Einrichtung und dem Arbeitsplatz im Privatbereich transportiert werden, können diese Daten und Informationen verloren gehen. Auch könnten sie von unbefugten Dritten entwendet, gelesen oder manipuliert werden. Der Akten- und Datenträgertransport kann auf verschiedene Arten unzureichend gesichert sein:

• Werden Unikate transportiert und fehlt ein entsprechendes Backup, können Ziele und Aufgaben nicht wie geplant erreicht werden, wenn das Unikat verlorengeht.

• Fallen unverschlüsselte Datenträger in falsche Hände, kann das zu einem schwerwiegenden Verlust der Vertraulichkeit führen.

• Wenn unterwegs kein ausreichender Zugriffsschutz vorhanden ist, können Akten oder Datenträger unbemerkt kopiert oder manipuliert werden.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" geregelt.

Ungeeignete Entsorgung der Datenträger und Dokumente

Ist es Beschäftigten am Arbeitsplatz im Privatbereich nicht möglich, Datenträger und Dokumente in geeigneter Weise zu entsorgen, könnten sie einfach in den Hausmüll geworfen werden. Angreifer können daraus jedoch wertvolle Informationen gewinnen, die sich gezielt für Erpressungsversuche oder zur Wirtschafts- oder Wissenschaftsspionage missbrauchen lassen. Die Folgen reichen vom Wissensverlust bis zur juristischen Folgen der Einrichtung, z. B. wenn dadurch vertrauliche Daten abfließen. Weiterhin können durch den Verlust von Informationen ein meldepflichtiger Datenschutzverstoß vorliegen sowie gemäß DV vom xxx ein Ausschluss von der Telearbeit und mobilen Arbeiten erfolgen.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" und dem Rundschreiben 20/2019 zur „Verschlüsselung mobiler Speicherträger“ geregelt.

Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software am Arbeitsplatz im Privatbereich

IT-Geräte, Zubehör, Informationen und Software, die am Arbeitsplatz im Privatbereich benutzt werden, können unter Umständen einfacher manipuliert oder zerstört werden als in der Einrichtung. Der Arbeitsplatz im Privatbereich ist oft für Angehörige und Besucher der Familie zugänglich. Wenn IT-Geräte, Zubehör, Informationen oder Software manipuliert oder zerstört werden, sind Beschäftigte am Arbeitsplatz im Privatbereich oft nur noch eingeschränkt arbeitsfähig. Des Weiteren müssen womöglich zerstörte IT-Komponenten, Informationen und Softwarelösungen ersetzt werden, was sowohl finanzielle als auch zeitliche Ressourcen erfordert.

Um den Verlust oder die Zerstörung eines Arbeitsgerätes unwahrscheinlicher zu machen, können der Einsatz von Kabelschlössern (sog. Kensington-Locks) und das Einschließen der Geräte bei Nichtbenutzung erwägt werden.

Diebstahlgefahr am Arbeitsplatz im Privatbereich

Einbrecher stehlen meistens vorrangig Gegenstände, die schnell und einfach verkauft werden können. Dabei kann auch dienstliche IT gestohlen werden. Die auf den entwendeten dienstlichen IT-Systemen vorhandenen Informationen besitzen aber oft einen höheren Wert als die IT-Systeme selbst. Einbrecher könnten versuchen, durch Erpressung oder Weitergabe der Daten an Konkurrenzunternehmen einen höheren Gewinn als durch den Verkauf der Hardware zu erzielen.

Um den Verlust oder die Zerstörung eines Arbeitsgerätes unwahrscheinlicher zu machen, können der Einsatz von Kabelschlössern (sog. Kensington-Locks) und das Einschließen der Geräte bei Nichtbenutzung erwägt werden. Mobile Geräte müssen dem Rundschreiben 20/2019 zur „Verschlüsselung mobiler Speicherträger“ verschlüsselt sein.

7.3 Grundlegende Sicherheitsanforderungen

Eine verantwortliche Mitwirkung der beschäftigten Person ist für eine sichere Ausgestaltung und Nutzung des Arbeitsplatz im Privatbereich erforderlich[14]. Der Informationssicherheitsbeauftragte (ISB) der Einrichtung oder Fakultät ist bei strategischen Entscheidungen beratend hinzuzuziehen.

Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig erfüllt werden[15]:

Sichern von dienstlichen Unterlagen am Arbeitsplatz im Privatbereich

Dienstliche Unterlagen und Datenträger MÜSSEN am Arbeitsplatz im Privatbereich so aufbewahrt werden, dass keine Unbefugten darauf zugreifen können. Daher MÜSSEN ausreichend verschließbare Behältnisse (z. B. abschließbare Rollcontainer oder Schränke) vorhanden sein. Alle Beschäftigten MÜSSEN sicherstellen, dass keine schützenswerten Informationen frei zugänglich sind.

Entsprechende organisatorische Regelungen sind in der "Dienstvereinbarung über Homeoffice und Mobile Arbeit" und der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" enthalten.

Transport von Arbeitsmaterial zum Arbeitsplatz im Privatbereich

Es MUSS geregelt werden, welche Datenträger und Unterlagen am Arbeitsplatz im Privatbereich bearbeitet und zwischen der Einrichtung und dem Arbeitsplatz im Privatbereich hin und her transportiert werden dürfen. Generell MÜSSEN Datenträger und andere Unterlagen sicher transportiert werden. Diese Regelungen MÜSSEN den Beschäftigten in geeigneter Weise bekanntgegeben werden.

Mit dem Rundschreiben 20/2019 zur „Verschlüsselung mobiler Speicherträger“ geregelt.

Schutz vor unbefugtem Zutritt am Arbeitsplatz im Privatbereich

Den Beschäftigten MUSS mitgeteilt werden, welche Regelungen und Maßnahmen zum Einbruchs- und Zutrittsschutz zu beachten sind. So MUSS darauf hingewiesen werden, Fenster zu schließen und Türen abzuschließen, wenn der Arbeitsplatz im Privatbereich nicht besetzt ist. Es MUSS sichergestellt werden, dass Unbefugte zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" geregelt.

Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik[16]. Sie SOLLTEN grundsätzlich erfüllt werden.

Geeignete Einrichtung des Arbeitsplatzes im Privatbereich

Der Arbeitsplatz im Privatbereich SOLLTE durch eine geeignete Raumaufteilung von den privaten Bereichen der Wohnung getrennt sein. Der Arbeitsplatz im Privatbereich SOLLTE mit Büromöbeln eingerichtet sein, die ergonomischen Anforderungen entsprechen. Ebenso SOLLTE der Arbeitsplatz im Privatbereich durch geeignete technische Sicherungsmaßnahmen vor Einbrüchen geschützt werden. Die Schutzmaßnahmen SOLLTEN an die örtlichen Gegebenheiten und den vorliegenden Schutzbedarf angepasst sein.

Für das Homeoffice wird der Arbeitsplatz im Rahmen der Arbeitsschutzverordnung bewertet und Empfehlungen ausgesprochen.

[14] Im Folgenden sind die spezifischen Anforderungen des BSI Bausteins INF.8 „Häuslicher Arbeitsplatz“ aufgeführt; die Formulierungen zu den Anforderungen sind diesem BSI-Baustein entnommen und durch gerahmte Hinweise zur Umsetzung in der LUH ergänzt

[15] Gemäß BSI-Baustein INF.8 "Häuslicher Arbeitsplatz"

[16] Gemäß BSI-Baustein INF.8 „Häuslicher Arbeitsplatz“

Entsorgung von vertraulichen Informationen am Arbeitsplatz im Privatbereich

Vertrauliche Informationen SOLLTEN sicher entsorgt werden. In einer speziellen Sicherheitsrichtlinie/Dienstanweisung SOLLTE daher geregelt werden, wie schutzbedürftiges Material zu beseitigen ist. Es SOLLTEN die dafür benötigten Entsorgungsmöglichkeiten verfügbar sein.

Vertrauliche Informationen MÜSSEN gemäß den Regelungen der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" entsorgt werden.

Anforderungen bei erhöhtem Schutzbedarf (D-E)

Im Folgenden sind exemplarische Vorschläge[17] für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am Arbeitsplatz im Privatbereich

Wenn Beschäftigte dienstliche Unterlagen oder Informationen mit erhöhtem Schutzbedarf bearbeiten müssen, SOLLTE überlegt werden, von einem Arbeitsplatz im Privatbereich ganz abzusehen. Anderenfalls SOLLTE der Arbeitsplatz im Privatbereich durch erweiterte, hochwertige technische Sicherungsmaßnahmen geschützt werden.

Eine Verarbeitung von Daten der Schutzstufe E ist nicht zulässig. Daten der Schutzstufe D sollten entsprechend der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" grundsätzlich nicht in Papierform bearbeitet werden.

Bei der elektronischen Verarbeitung der Schutzstufe D SOLLTE ein zusätzlicher Sichtschutz sichergestellt werden.

8. Mobiler Arbeitsplatz

Der Einsatz eines mobilen Arbeitsplatzes wird im BSI Grundschutz im Infrastrukturbaustein INF.9 beschrieben. Die dort aufgeführten Modellierungen und Maßnahmen gelten im Grundsatz und werden hier im Kontext der LUH ausformuliert.

8.1 Begriffsbestimmung

Eine gute Netzabdeckung sowie leistungsfähige IT-Geräte, wie z. B. Laptops, Smartphones oder Tablets, ermöglichen es Beschäftigten, nahezu an jedem Platz bzw. von überall zu arbeiten. Das bedeutet, dass dienstliche Aufgaben häufig nicht mehr nur in den Räumen und Gebäuden der Einrichtung erfüllt werden, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen, z. B. in Hotelzimmern, in Zügen oder auf Konferenzen aber auch im Homeoffice. Die dabei verarbeiteten Informationen müssen angemessen geschützt werden. Das mobile Arbeiten verändert einerseits die Dauer, Lage und Verteilung der Arbeitszeiten. Andererseits erhöht es die Anforderungen an die Informationssicherheit, da in Umgebungen mit mobilen Arbeitsplätzen keine sichere IT-Infrastruktur vorausgesetzt werden kann, so wie sie in einer Büroumgebung anzutreffen ist.

Der Abschnitt beschreibt Sicherheitsanforderungen an mobile Arbeitsplätze. Ziel ist es, für solche Arbeitsplätze eine mit einem Büro oder einem Arbeitsplatz im Privatbereich annähernd vergleichbare Sicherheitssituation zu schaffen.

Dieser Abschnitt des Konzepts ist für alle Räume anzuwenden, die häufig als mobiler Arbeitsplatz genutzt werden. Der Abschnitt enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn Beschäftigte nicht nur innerhalb der Einrichtung arbeiten, sondern auch häufiger an wechselnden Arbeitsplätzen außerhalb. Der Abschnitt bildet vor allem die organisatorischen, technischen und personellen Anforderungen an die teilweise mobile Arbeit ab[18].

[17] Gemäß BSI-Baustein INF.8 „Häuslicher Arbeitsplatz“;

[18] Um IT-Systeme, Datenträger oder Unterlagen, die beim mobilen Arbeiten genutzt werden, abzusichern, müssen alle relevanten BSI-Bausteine wie z. B. SYS.3.1 „Laptops“, SYS.3.2 „Allgemeine Smartphones und Tablets“, SYS.4.5 „Wechseldatenträger“, NET.3.3 „VPN“ sowie SYS.2.1 „Allgemeiner Client“ gesondert berücksichtigt werden.

8.2 Spezifische Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind von besonderer Bedeutung[19].

Fehlende oder unzureichende Regelungen für mobile Arbeitsplätze

Ist das mobile Arbeiten nicht oder nur unzureichend geregelt, können der Einrichtung unter anderem finanzielle Schäden entstehen. Ist beispielsweise nicht geregelt, welche Informationen außerhalb der Einrichtung transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu beachten sind, können vertrauliche Informationen in fremde Hände gelangen. Diese können dann von Unbefugten möglicherweise gegen die Einrichtung verwendet werden.

Handlungsanweisungen werden in der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" ausgeführt.

Beeinträchtigung durch wechselnde Einsatzumgebung

Da mobile Datenträger und Endgeräte in sehr unterschiedlichen Umgebungen eingesetzt werden, sind sie vielen Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie z. B. zu hohe oder zu niedrige Temperaturen, Staub oder Feuchtigkeit. Auch Transportschäden können auftreten. Neben diesen Einflüssen ist auch die Einsatzumgebung mit ihrem unterschiedlichen Sicherheitsniveau zu berücksichtigten. Smartphones, Tablets, Laptops und ähnliche mobile Endgeräte sind nicht nur beweglich, sondern können auch mit anderen IT-Systemen kommunizieren. Dabei können beispielsweise Schadprogramme übertragen oder schützenswerte Informationen kopiert werden. Auch können eventuell Aufgaben nicht mehr erfüllt, Kundentermine nicht wahrgenommen oder IT-Systeme beschädigt werden.

Durch die "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" und das Rundschreiben 20/2019 zur „Verschlüsselung mobiler Speicherträger“ geregelt.

Manipulation oder Zerstörung von IT-Systemen, Zubehör, Informationen und Software am mobilen Arbeitsplatz

IT-Systeme, Zubehör, Informationen und Software, die mobil genutzt werden, können unter Umständen einfacher manipuliert oder zerstört werden als in der Einrichtung. Der mobile Arbeitsplatz ist oft für Dritte zugänglich. Werden IT-Systeme, Zubehör, Informationen oder Software manipuliert oder zerstört, ist der Beschäftigte am mobilen Arbeitsplatz oft nur noch eingeschränkt arbeitsfähig. Des Weiteren müssen womöglich zerstörte IT-Komponenten oder Softwarelösungen ersetzt werden, was sowohl finanzielle als auch zeitliche Ressourcen erfordert.

Die Handhabung mobiler Endgeräte wird in der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" thematisiert.

Um den Verlust oder die Zerstörung eines Arbeitsgerätes unwahrscheinlicher zu machen, kann bei Vorhandensein geeigneter Haltepunkte der Einsatz von Kabelschlössern (sog. Kensington-Locks) erwägt werden.

Verzögerungen durch temporär eingeschränkte Erreichbarkeit

Meist sind Beschäftigte am mobilen Arbeitsplatz schwerer zu erreichen. Dadurch kann sich der Informationsfluss deutlich verzögern. Selbst wenn die Informationen per E-Mail übermittelt werden, verkürzt sich nicht zwingend die Reaktionszeit, da nicht sichergestellt werden kann, dass die mobilen Beschäftigten die E-Mail zeitnah lesen. Die temporär eingeschränkte Erreichbarkeit wirkt sich dabei je nach Situation und Einrichtung unterschiedlich aus, kann aber die Verfügbarkeit von Informationen stark einschränken.

Die Erreichbarkeit ist in der „Dienstvereinbarung über Homeoffice und Mobile Arbeit“ geregelt.

Ungesicherter Akten- und Datenträgertransport

Wenn Dokumente, Datenträger oder Akten zwischen der Einrichtung und den mobilen Arbeitsplätzen transportiert werden, können diese Informationen und Daten verlorengehen oder auch von Unbefugten

[19] gemäß BSI-Baustein INF.9 „Mobiler Arbeitsplatz“; die Formulierungen zur Gefährdungslage sind diesem BSI-Baustein entnommen und durch gerahmte Hinweise zur Umsetzung in der LUH ergänzt

entwendet, gelesen oder manipuliert werden. Dadurch können der Einrichtung größere finanzielle Schäden entstehen. Der Akten- und Datenträgertransport kann auf verschiedene Arten unzureichend gesichert sein:

• Werden Unikate transportiert und fehlt eine entsprechende Datensicherung, können Ziele und Aufgaben nicht wie geplant erreicht werden, wenn das Unikat verloren geht.

• Fallen unverschlüsselte Datenträger in falsche Hände, kann dies zu einem schwerwiegenden Verlust der Vertraulichkeit führen.

• Ist unterwegs kein ausreichender Zugriffsschutz vorhanden, können Akten oder Datenträger unbemerkt kopiert oder manipuliert werden.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" und dem Rundschreiben 20/2019 zur „Verschlüsselung mobiler Speicherträger“ geregelt.

Unterlagen mit schutzbedürftigen Daten sollten in der Regel nicht im mobilen Szenario bearbeitet werden.

Ungeeignete Entsorgung der Datenträger und Dokumente

Ist es am mobilen Arbeitsplatz nicht möglich, Datenträger und Dokumente in geeigneter Weise zu entsorgen, wandern diese meist in den Hausmüll. Auch dort, wo unterwegs gearbeitet wird, werfen Beschäftigte Entwürfe und andere vermeintlich unnütze Dokumente häufig direkt in den nächsten Papierkorb. Oder sie lassen sie einfach liegen, sei es im Hotel oder in der Bahn. Wenn jedoch Datenträger oder Dokumente nicht geeignet entsorgt werden, können Angreifer daraus wertvolle Informationen entnehmen, die sich gezielt für Erpressungsversuche oder zur Wirtschafts- oder Wissenschaftsspionage missbrauchen lassen. Die Folgen reichen vom Wissensverlust bis zu juristischen Folgen für die Einrichtung, z. B. wenn dadurch vertrauliche Informationen abfließen.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" und dem Rundschreiben 20/2019 zur „Verschlüsselung mobiler Speicherträger“ geregelt.

Ordnungsgemäß verschlüsselte Datenträger (z. B. AES128 oder besser20) sollten vorzugsweise über die Einrichtung und ersatzweise über spezielle Elektroschrott-Annahmestellen entsorgt werden.

Vertraulichkeitsverlust schützenswerter Informationen

Am mobilen Arbeitsplatz können Angreifende einfacher auf vertrauliche Informationen zugreifen, die sich auf Festplatten, auf austauschbaren Speichermedien oder auf Papier befinden, besonders dann, wenn sie dabei professionell agieren. Auch können sie Kommunikationsverbindungen abhören. Werden Informationen unberechtigt gelesen oder preisgegeben, hat das jedoch schwerwiegende Folgen für die gesamte Einrichtung. Unter anderem kann der Verlust der Vertraulichkeit dazu führen, dass die Einrichtung gegen Gesetze verstößt oder dass Wettbewerbsnachteile und finanzielle Schäden entstehen.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" und dem Rundschreiben 20/2019 zur „Verschlüsselung mobiler Speicherträger“ geregelt. Zusätzlich sollten verschlüsselte Verbindungen genutzt werden.

Diebstahl oder Verlust von Datenträgern oder Dokumenten

Der mobile Arbeitsplatz ist nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen oder in einer Behörde. Dienstliche IT-Systeme und Dokumente können daher z. B. während einer Bahnfahrt, aus einem Hotelzimmer oder aus externen Konferenzräumen leichter gestohlen werden. Zudem können mobile IT-Systeme oder IT-Komponenten verloren gehen. Neben dem rein materiellen Schaden durch den unmittelbaren Verlust des mobilen IT-Systems kann zudem ein weiterer finanzieller Schaden entstehen, etwa, wenn schützenswerte Daten wie z. B. E-Mails, Notizen von Besprechungen, Adressen oder sonstige Dokumente offengelegt werden. Auch könnte der Ruf der Einrichtung geschädigt werden.

[20] Empfehlungen zur Wahl von Verschlüsselungsverfahren und Schlüssellängen gibt das BSI in der Technischen Richtlinie TR-02102-1

Um den Verlust oder die Zerstörung eines Arbeitsgerätes unwahrscheinlicher zu machen, können der Einsatz von Kabelschlössern (sog. Kensington-Locks) und die Beaufsichtigung der Geräte bei Nichtbenutzung erwägt werden.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" und Maßnahmen in der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" geregelt.

8.3 Grundlegende Sicherheitsanforderungen

Grundsätzlich ist die Einrichtungsleitung dafür verantwortlich, dass alle Anforderungen gemäß dem hier festgelegten Sicherheits- und Technikkonzept erfüllt und überprüft werden[21]. Informationssicherheitsbeauftragte (ISB) der Einrichtung oder Fakultät können beratend hinzugezogen werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben.

Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN[22] vorrangig erfüllt werden:

Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes

Die Einrichtung MUSS ihren Beschäftigten vorschreiben, wie mobile Arbeitsplätze in geeigneter Weise ausgewählt und benutzt werden sollen. Es MÜSSEN Eigenschaften definiert werden, die für einen mobilen Arbeitsplatz wünschenswert sind. Es MÜSSEN aber auch Ausschlusskriterien definiert werden, die gegen einen mobilen Arbeitsplatz sprechen. Mindestens MUSS geregelt werden:

• unter welchen Arbeitsplatzbedingungen schützenswerte Informationen bearbeitet werden dürfen,

• wie sich Beschäftigte am mobilen Arbeitsplatz vor ungewollter Einsichtnahme Dritter schützen,

• ob eine permanente Netz- und Stromversorgung gegeben sein muss sowie

• welche Arbeitsplatzumgebungen komplett verboten sind.

Einstiegspunkte zur Auswahl des geeigneten Endgeräte-Szenarios sind in diesem Konzept die Diagramme zum Umgebungs- und Sicherheitsdomänenrisiko. Hier kann festgestellt werden, welches Risiko sich durch den gewählten Arbeitsplatz in Bezug auf die verarbeiteten Daten ergibt und welche Endgeräte-Szenarien geeignet sind. Andere als die erwähnten Endgeräte-Szenarien sind nicht zulässig.

Weitere Punkte sind in der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" und der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" geregelt.

Regelungen für mobile Arbeitsplätze

Für alle Arbeiten unterwegs MUSS durch die jeweilige Einrichtung geregelt werden, welche Informationen außerhalb der Einrichtung transportiert und bearbeitet werden dürfen. Es MUSS zudem geregelt werden, welche Schutzvorkehrungen dabei zu treffen sind. Dabei MUSS auch geklärt werden, unter welchen Rahmenbedingungen Beschäftigte mit mobilen IT-Systemen auf interne Informationen ihrer Einrichtung zugreifen dürfen. Die Mitnahme von IT-Komponenten und Datenträgern MUSS klar geregelt werden. So MUSS festgelegt werden, welche IT-Systeme und Datenträger mitgenommen werden dürfen, wer diese mitnehmen darf und welche grundlegenden Sicherheitsanforderungen dabei beachtet werden müssen. Es MUSS zudem protokolliert werden, wann und von wem welche mobilen Endgeräte außer Haus eingesetzt wurden. Die Benutzer von mobilen Endgeräten MÜSSEN für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Sie MÜSSEN über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten IT-Systeme aufgeklärt werden. Außerdem MÜSSEN sie darüber informiert werden, welche Art von Informationen auf mobilen IT-Systemen verarbeitet werden darf. Alle Benutzenden MÜSSEN auf die

[21] Im Folgenden sind die spezifischen Anforderungen des BSI Bausteins INF.9 „Mobiler Arbeitsplatz“ aufgeführt.

[22] Gemäß BSI Baustein INF.9 „Mobiler Arbeitsplatz“; die Formulierungen zu den Anforderungen sind diesem BSI-Baustein entnommen und durch gerahmte Hinweise zur Umsetzung in der LUH ergänzt

geltenden Regelungen hingewiesen werden, die von ihnen einzuhalten sind. Sie MÜSSEN entsprechend geschult werden.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit", der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" und dem Rundschreiben 20/2019 zur „Verschlüsselung mobiler Speicherträger“ geregelt.

Zutritts- und Zugriffsschutz

Den Beschäftigten MUSS bekannt gegeben werden, welche Regelungen und Maßnahmen zum Einbruch- und Zutrittsschutz am mobilen Arbeitsplatz zu beachten sind. Wenn der mobile Arbeitsplatz nicht besetzt ist, MÜSSEN Fenster und Türen abgeschlossen werden. Ist dies nicht möglich, z. B. im Zug, MÜSSEN die Beschäftigten alle Unterlagen und IT-Systeme an sicherer Stelle verwahren oder mitführen, wenn sie abwesend sind. Es MUSS sichergestellt werden, dass Unbefugte zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können. Wird der Arbeitsplatz nur kurz verlassen, MÜSSEN die eingesetzten IT-Systeme gesperrt werden, sodass sie nur nach erfolgreicher Authentisierung wieder benutzt werden können.

Arbeiten mit fremden IT-Systemen

Die jeweilige Einrichtung MUSS regeln, wie Beschäftigte mit einrichtungsfremden IT-Systemen arbeiten dürfen. Mobil arbeitende Beschäftigte müssen über die Gefahren fremder IT-Systeme aufgeklärt werden. Die Regelungen MÜSSEN vorgeben, ob und wie schützenswerte Informationen an fremden IT-Systemen bearbeitet werden dürfen. Sie MÜSSEN zudem festlegen, wie verhindert wird, dass nicht autorisierte Personen die Informationen einsehen können. Wenn Beschäftigte mit fremden IT-Systemen arbeiten, MUSS grundsätzlich sichergestellt sein, dass alle währenddessen entstandenen temporären Daten gelöscht werden.

Mit der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" geregelt, Regelungen zur Nutzung privater Endgeräte (Bring Your Own Device, BYOD) sind in der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" enthalten.

Wird z. B. bei Kooperationsprojekten auf fremde Speicherdienste zurückgegriffen, muss von der Einrichtung geklärt werden, wie Speicher- und Löschfristen dort umgesetzt werden.

Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik[23]. Sie SOLLTEN grundsätzlich erfüllt werden.

Zeitnahe Verlustmeldung

Beschäftigte SOLLTEN ihrer Einrichtung umgehend melden, wenn Informationen, IT-Systeme oder Datenträger verlorengegangen sind oder gestohlen wurden. Dafür SOLLTE es klare Meldewege und Ansprechpartner innerhalb der Einrichtung geben.

Ansprechpartner in den Einrichtungen sind die IT-Beauftragten und ggf. die dezentralen Informationssicherheitsbeauftragten. Alternativ kann das Sicherheits-Team des LUIS kontaktiert werden.

Entsorgung von vertraulichen Informationen

Vertrauliche Informationen SOLLTEN auch unterwegs sicher entsorgt werden. Bevor ausgediente oder defekte Datenträger und Dokumente vernichtet werden, MUSS überprüft werden, ob sie sensible Informationen enthalten. Ist dies der Fall, MÜSSEN die Datenträger und Dokumente wieder mit zurücktransportiert werden und auf einrichtungseigenem Wege entsorgt oder vernichtet werden.

Vertrauliche Informationen MÜSSEN gemäß der "Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit" entsorgt werden.

[23] Gemäß BSI Baustein INF.9 „Mobiler Arbeitsplatz“

Rechtliche Rahmenbedingungen für das mobile Arbeiten

Für das mobile Arbeiten SOLLTEN arbeitsrechtliche und arbeitsschutzrechtliche Rahmenbedingungen beachtet und geregelt werden. Alle relevanten Punkte SOLLTEN entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen den mobilen Beschäftigten und der Dienststelle geregelt werden.

Die rechtlichen Rahmenbedingungen werden in der "Dienstvereinbarung über Homeoffice und Mobile Arbeit" geregelt.

Sicherheitsrichtlinie für mobile Arbeitsplätze

Alle relevanten Sicherheitsanforderungen für mobile Arbeitsplätze SOLLTEN in einer für die mobilen Beschäftigten verpflichtenden Sicherheitsrichtlinie dokumentiert werden. Sie SOLLTE zudem mit den bereits vorhandenen Sicherheitsrichtlinien der Einrichtung sowie mit allen relevanten Fachabteilungen abgestimmt werden. Die Sicherheitsrichtlinie für mobile Arbeitsplätze SOLLTE regelmäßig aktualisiert werden. Die Beschäftigten der Einrichtung SOLLTEN hinsichtlich der aktuellen Sicherheitsrichtlinie sensibilisiert und geschult sein.

Die "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" sowie dieses Dokument erfüllen den Zweck der Sicherheitsrichtlinie für mobile Arbeitsplätze.

Verschlüsselung tragbarer IT-Systeme und Datenträger

Bei tragbaren IT-Systemen und Datenträgern SOLLTE sichergestellt werden, dass diese entsprechend den internen Richtlinien abgesichert sind. Mobile IT-Systeme und Datenträger SOLLTEN dabei verschlüsselt werden. Die kryptografischen Schlüssel SOLLTEN getrennt vom verschlüsselten Gerät aufbewahrt werden.

Die Handhabung ist im Rundschreiben 20/2019 zur „Verschlüsselung mobiler Speicherträger“ verpflichtend geregelt.

Nutzung eines Bildschirmschutzes

Wenn IT-Systeme an mobilen Arbeitsplätzen genutzt werden, SOLLTEN die Beschäftigten einen Sichtschutz für die Bildschirme der IT-Systeme verwenden.

Zum Schutz des Bildschirms werden im Handel Schutzfolien angeboten, die eine Einsichtnahme von der Seite deutlich erschweren.

Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein INF.9 "Mobiler Arbeitsplatz" Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse durch die jeweilige Einrichtung.

Einsatz von Diebstahlsicherungen

Bietet das verwendete IT-System eine Diebstahlsicherung, SOLLTE sie benutzt werden. Die Diebstahlsicherungen SOLLTEN stets dort eingesetzt werden, wo ein erhöhter Publikumsverkehr herrscht oder die Fluktuation von Benutzenden sehr hoch ist. Dabei SOLLTEN die Beschäftigten immer beachten, dass der Schutz der auf den IT-Systemen gespeicherten Informationen meist einen höheren Wert besitzt als die Wiederanschaffungskosten des IT-Systems betragen. Die Beschaffungs- und Einsatzkriterien für Diebstahlsicherungen SOLLTEN an die Prozesse der Einrichtung angepasst und dokumentiert werden.

Viele tragbare Geräte sind mit Vorkehrungen für Kabelschlösser (sog. Kensington Locks) versehen. Als zusätzliche Maßnahme können mobile Geräte auch eingeschlossen werden.

Verbot der Nutzung unsicherer Umgebungen

Es SOLLTEN Kriterien für die Arbeitsumgebung festgelegt werden, die mindestens erfüllt sein müssen, damit Informationen mit erhöhtem Schutzbedarf mobil bearbeitet werden dürfen. Die Kriterien SOLLTEN mindestens folgende Themenbereiche abdecken:

• Einsicht und Zugriff durch Dritte,

• geschlossene und, falls nötig, abschließbare oder bewachte Räume,

• gesicherte Kommunikationsmöglichkeiten sowie

• eine ausreichende Stromversorgung.

Die Beurteilung der jeweiligen Arbeitsumgebung muss der oder die Beschäftigte treffen. Abschnitt 0 dient als Orientierungshilfe für das Umgebungsrisiko.

9. Sicherheits- und Technikkonzepte der zulässigen Szenarien für Homeoffice und mobiles Arbeiten

Die Sicherheits- und Technikkonzepte beschreiben grundlegende Systemanordnungen bei Endgeräten, die typischerweise im LUH-Umfeld zu finden sind. Außerdem werden Systeme skizziert, die erweiterten Sicherheitsanforderungen im mobilen Umfeld besser gerecht werden, als die zurzeit am häufigsten eingesetzten mobilen Szenarios.

9.1 Endgerätekonzepte

Hier werden verschiedene Szenarien vorgestellt, die für Homeoffice und mobiles Arbeiten aus sicherheitstechnischer und organisatorischer Sicht geeignet sind. Die Eignung für verschiedene Sicherheitsanforderungen wird separat betrachtet. Andere als die hier aufgezählten Endgeräte-Szenarien sind für Homeoffice und mobile Arbeit nicht zulässig.

Thinclient (bisherige Telearbeit)

Ein Thinclient ist ein Gerät, welches lediglich ein rudimentäres Betriebssystem auf einer reduzierten Hardware-Plattform besitzt. Die Grundidee ist die Verlagerung von administrativem Aufwand und vor allem der eigentlichen Datenverarbeitung und Datenhaltung auf ein zentral im LUIS oder in der Einrichtung vorgehaltenes, verhältnismäßig leistungsfähiges Computersystem. Dabei kann es sich um einen physischen Büro-PC oder um einen virtuellen PC (z. B. per Terminal-Server oder Virtual Desktop Infrastructure) handeln. Durch die fehlende lokale Datenhaltung und eine ausschließliche Datenverarbeitung auf dem Computersystem in den gesicherten Räumen der LUH verlagert sich das Umgebungsrisiko dorthin. Der Thinclient erlaubt es, nur einen spezifischen VPN-Tunnel zum LUIS herzustellen. Über diesen Tunnel werden alle Eingabedaten, Verarbeitungsdaten und Remote-Desktop-Informationen verschlüsselt übertragen.

Auf dem Gerät selbst sind keine weiteren Schutzmaßnahmen notwendig, da die verarbeiteten Daten nicht auf dem Gerät gespeichert werden. Zu beachten sind Thinclients, die neben der Möglichkeit des Remote-Desktop-Betriebes durchaus lokale Anwendungen, wie einen Web-Browser (z. B. für Videokonferenzen) bieten. Hier muss die Notwendigkeit der Bereitstellung solcher lokaler Software durch die jeweilige Einrichtung abgewogen werden.

Die Vorbereitung und Verwaltung des Gerätes erfolgen aus dem LUIS, die notwendigen Updates des Systems werden rechtzeitig vom LUIS initiiert.

Vorteile des Thinclients:

- wird vom LUIS verwaltet
- baut selbständig einen VPN-Tunnel auf
- direkter Zugriff ausschließlich auf einen einzelnen Arbeitsplatzrechner
- besonders sicher, weil Betriebssystem besonders geschützt ist (gehärtet)
- keine lokale Datenhaltung
- das Sicherheitsniveau ist bis auf das Umgebungsrisiko grundsätzlich mit einem Büroarbeitsplatz vergleichbar

Road-Warrior (bisheriges „ungeregeltes“ mobiles Arbeiten) ohne Zugriff auf interne Einrichtungsressourcen

Der Begriff Road Warrior stammt aus einer Zeit, in der es die heute aus dem Arbeits- und Wirtschaftsleben nicht mehr wegzudenkenden Telekommunikationsmittel noch nicht gegeben hat. Schon vor den 1990er Jahren wurden Menschen, die beruflich viel unterwegs waren als Road Warrior bezeichnet. Diese Beschäftigten sind eigentlich nur zur Erledigung ihrer administrativen Verpflichtungen oder für wichtige Besprechungen ins Büro gekommen, oder, wenn sie Kommunikationsmittel wie das Telefax verwenden wollten. Diese technischen Ressourcen waren

damals sehr teuer und nicht im Übermaß vorhanden und standen an einer zentralen Stelle zur gemeinsamen Nutzung zur Verfügung.

Der Begriff kennzeichnet im Kontext der Corona-Pandemie jenes mobile Arbeitsmodell, das ohne aufwändige infrastrukturelle Vorkehrungen seitens des Arbeitgebers mit den zur Verfügung stehenden mobilen Endgeräten kurzfristig unterstützt werden kann.

In der Regel kommen hier dienstliche Stand-Alone Endgeräte zum Einsatz, die gemäß der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" der LUH verschlüsselt und sicherheitstechnisch aktuell gehalten müssen. Im Gegensatz zum Thinclient werden weder ein dediziertes zentrales VPN („LUH-VPN“) vorausgesetzt, noch ein abgeschottetes Institutsnetz („Instituts-VPN“). Gleichwohl muss die Übertragung dienstlicher Daten immer verschlüsselt erfolgen. Als Ersatz für eine VPN-Verbindung kommen hier geeignete TLS-verschlüsselte Verbindungen (z. B. per HTTP/S) in Frage. Dabei soll auf dem Client nach Möglichkeit die Authentizität des verbundenen Servers anhand eines digitalen Zertifikats geprüft werden.

Beim Modell Road-Warrior soll eine Zusammenarbeit mit anderen Beschäftigten z. B. an gemeinsamen Dokumenten ausschließlich über die vom LUIS angebotenen Cloud-Dienste und die LUIS-Projektablage sowie mit zulässigen dezentralen Diensten erfolgen. Eine lokale Datenhaltung und der Versand von bearbeiteten Dokumenten per E-Mail müssen für schutzbedürftige Informationen unbedingt unterbleiben.

Einrichtungs-Laptops mit VPN-Zugang in die Einrichtung

Die Nutzung von durch die Einrichtung administrierten mobilen Endgeräten ist gemäß den Vorgaben der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" gestattet. Insbesondere sollte beachtet werden, dass die Nutzung eines Instituts-/Einrichtungs-VPNs keinen Sicherheitsgewinn gegenüber dem normalen LUH-VPN bedeutet. Es bringt eher eine Erhöhung des Risikos für die Einrichtung mit sich, da dadurch mobile Endgeräte, die sich in potentiell gefährlicher Umgebung befinden direkten Zugriff auf das Instituts-/Einrichtungsnetz erhalten.

Aus Sicherheitssicht ist daher ein Road-Warrior-Szenario, ohne direkten Zugriff auf das Instituts-Netz via Instituts-VPN wie oben beschrieben vorzuziehen.

Eine wirkliche Erhöhung der Sicherheit wäre nur durch Endpoint-Detection and -Response-System auf gemanageten Endgeräten möglich (vgl. Managed Devices oder Fortrex-Szenario, welche derzeit noch nicht zentral angeboten werden können).

Instituts-Laptops unterliegen der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" der LUH.

Bring Your Own Device (BYOD)

Die Nutzung von privaten Geräten (BYOD), die den Vorgaben der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" entsprechen, ist zwar in gewissen Arbeitsbereichen zulässig (zu beachten insb. § 4 Abs. 3 der Richtlinie), sollte jedoch aus der Sicherheitsperspektive weitestgehend vermieden werden. Als Szenario für Homeoffice und mobiles Arbeiten mit schützenswerten dienstlichen Informationen ist BYOD grundsätzlich nicht geeignet.

Managed Device

Unter Managed Device wird grundsätzlich ein Endgerät verstanden, dessen Installation, Wartung und Software-Pflege nicht durch den Besitzenden selbst vorgenommen wird. Vielmehr werden diese Aufgaben durch eine zentrale Stelle für viele Endgeräte mit etablierten Prozessabläufen geplant und erledigt.

Technisch gesehen handelt es sich also um einheitlich und zentral gemanagte mobile Endgeräte (vorwiegend Notebooks) idealerweise mit Zwei-Faktor-Authentifizierung. Die Netzwerkanbindung wird durch ein zentrales Geräte-VPN realisiert, das nicht direkt in der Einrichtung, sondern in einem separiertem Koppelnetz terminiert. Ein Geräte-VPN wird im Gegensatz zu einem benutzerinitiierten VPN vom Endgerät selbständig zu einer fest definierten Gegenstelle in der LUH aufgebaut. Jeglicher Netzwerkverkehr wird über dieses VPN geleitet. Da das VPN nicht im dezentralen VPN einer Einrichtung terminiert, erhält das Endgerät eine IP-Adresse aus dem Koppelnetz und erhält durch

geeignete Firewall-Konfigurationen Zugriff auf definierte Ressourcen der Ziel-Einrichtung. Auch auf einem mobilen Endgerät als Managed Device wird regelmäßig lokale Datenhaltung betrieben, die lokalen Datenträger sind also zwingend zu verschlüsseln.

Bei Managed Devices besteht wie beim Konzept „Thinclient“ die Möglichkeit, eine RDP/SSH-Sitzung auf einen in den gesicherten Räumen der LUH bereitgestellten Server oder Arbeitsplatz-Computer einzuleiten um auf Spezialanwendungen zugreifen zu können. Der Unterschied zum derzeitigen Konzept „Thinclient“ ist die Möglichkeit, im Normalfall auch ohne den zentral bereitgestellten Computer als Gegenstelle auszukommen. Beim Einsatz der Managed Devices als „mobiler Thinclient“ mit lokaler Datenhaltung bestehen immer noch die Risiken durch die Umgebung und Diebstahl.

Das Managed Devices-Szenario kann derzeit nicht zentral durch das LUIS angeboten werden. Der Dienst APC-Vollservice deckt einen Teil der Sicherheitsanforderung ab, jedoch nicht alle erforderlichen Maßnahmen für das beschriebene Szenario.

„Fortrex“

Das Fortrex-Szenario hat das Ziel, ein mobiles Endgerät im Sinne einer „beweglichen Festung“ durch verschiedene technische und organisatorische Maßnahmen sicherheitstechnisch so auszustatten, dass das Sicherheitsniveau des oben beschriebenen Thinclients angenähert wird. Dieses Ziel ist nur durch einen erheblichen Eingriff in das Management eines mobilen Endgerätes zu erreichen, der weit über denjenigen bei Managed Devices hinausgeht. Die Verwendung des Fortrex-Szenarios bedeutet für das Endgerät praktisch, dass im Tausch für den Sicherheitsgewinn die administrative Verfügungsgewalt durch die beschäftigte Person vollständig aufgegeben wird. Außerdem wird für das Fortrex-Szenario eine besonders abgestimmte zentrale Management-Infrastruktur benötigt.

Um bei mobilen Endgeräten ein überwachbares Sicherheitsniveau („Security Supervised Device“) zu erreichen, sind zentral wenigstens die folgenden Infrastrukturmaßnahmen zwingend erforderlich.

MDM - Mobile Device Management

Ein Mobile Device Management ist die Grundvoraussetzung zur Herstellung eines verlässlichen Plattformzustandes bei mobilen Endgeräten. Ein solches System stellt alle erforderlichen Software-Komponenten auf dem mobilen Endgerät zur Verfügung und stellt gleichzeitig sicher, dass nur die für den jeweiligen Kontext benötigte Software und Gerätekonfiguration verwendet werden kann.

ID / Policy Management

Damit auf dem Endgerät zu jedem Zeitpunkt nur die benötigten Software-Komponenten und die die richtige Gerätekonfiguration zur Verfügung stehen, wird ein Rollenmodell benötigt, das Identitäten, Anwendungen, Daten und Arbeitsorte in Beziehung setzt und daraus die erforderlichen Policies ableitet. Diese werden über das MDM auf den Endgeräten umgesetzt.

Zentrales Geräte-VPN

Um einen Abfluss von Informationen zu vermeiden, werden alle Daten über einen zentral gemanagten, vom Gerät selbständig zu einer festen Gegenstelle hergestellten VPN-Tunnel geleitet. Ein sog. Split-Tunnel, bei dem lediglich ausgewählte Datenströme über das VPN geleitet werden, ist ausgeschlossen.

Zusätzlich zu diesen Komponenten sind auf den Endgeräten wenigstens die folgenden Maßnahmen zwingend erforderlich.

MFA - Multifaktor Authentifizierung

Die Multifaktor-Authentifizierung stellt sicher, dass ein gestohlenes oder verloren gegangenes Endgerät nicht ohne einen weiteren Faktor, wie ein Mobiltelefon oder beispielweise ein Sicherheits-Token entsperrt werden kann.

Device Posture Checks (Konformitätsprüfung)

Mit der Herstellung einer VPN-Verbindung wird das Endgerät zunächst auf Plattformaktualität, vorhandene Sicherheitsmerkmale und aufgetretene Sicherheitsvorfälle überprüft. Eine vollständige Netzwerkverbindung wird erst hergestellt, wenn alle Prüfungen des Endgeräts zufriedenstellend gemäß der zentralen Policy verlaufen. Andernfalls hat das Endgerät nur Zugriff auf einen abgeschotteten Netzbereich („Quarantäne“), in dem ggf. eine Behandlung der Verstöße gegen die

Sicherheitsregeln durch zusätzliche Konfigurationsschritte oder Software-Updates eingeleitet werden kann („Remediation“).

EDR - Endpoint Detection & Response

Ein System zur Endpoint Detection & Response überwacht die Sicherheit durch aktive Softwarekomponenten auf dem Endgerät, die über die Funktionalität eines reinen Virenscanners hinausgehen. So werden z. B. typische Prozessketten eines Malware-Befalls erkannt und unterbunden. Gegebenenfalls werden Sperrmaßnahmen auf dem Endgerät zur Schadensbegrenzung durchgesetzt.

Das Fortrex-Szenario kann derzeit nicht zentral durch das LUIS angeboten werden.

9.2 Zuordnung der Konzepte zu Sicherheitsbereichen

Aufgrund der unterschiedlichen Beschaffenheit der vorgenannten technischen Konstellationen im Hinblick auf ein erreichbares Sicherheitsniveau eigenen sich diese nicht gleichermaßen für alle Arbeitssituationen. Um die für die jeweilige Situation angemessene Arbeitsplatzausstattung zu ermitteln, dienen die oben definierten Bewertungsmodelle *Umgebungsrisiko* und *Sicherheitsdomänenrisiko*. Diese bilden typische qualitative Beurteilungseckpunkte der potenziellen Bedrohungslage (gering, mittel, hoch) im Bezug auf den Schutzbedarf der verarbeiteten Informationen (Schutzstufen A - E) auf einen Risikoklasse (unkritisch, moderat, kritisch, hoch-kritisch) ab. Bei Abweichungen der beiden Modelle in der Bewertung derselben Arbeitssituation ist dabei die höhere Risikobewertung zugrunde zu legen.

Gemäß der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" wird privaten, mobilen Endgeräten, die vollständig im Verantwortungsbereich von Beschäftigten liegen, ein erhebliches Sicherheits-Niveau zugerechnet, sofern die definierten Maßnahmen vollständig umgesetzt werden. Dies kann eine im Ausnahmefall zu rechtfertigende Annahme sein. Oft ist diese jedoch einer erhöhten Risikobereitschaft aller Verantwortlichen geschuldet, die im Zuge der zeitlich angespannten Anfangsphase der Corona-Pandemie nicht zu vermeiden war. Es wird empfohlen, mit privaten, mobilen Endgeräten nur in der Risikobewertung „unkritisch“ zu operieren.

aggregierte Risiko-klasse	Technikkonzepte
unkritisch	Thinclient Fortrex[24] Managed Device[23] Road-Warrior Einrichtungs-Laptops mit VPN-Zugang in die Einrichtung alle Geräte, die der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" genügen
moderat	Thinclient Fortrex[23] Managed Device[23] Road-Warrior Einrichtungs-Laptops mit VPN-Zugang in die Einrichtung
kritisch	Thinclient Managed Device[23]

[24] Die Szenarien *Fortrex* und *Managed Device* können Stand März 2022 noch nicht zentral durch das LUIS angeboten werden

	Fortrex[23]
hoch-kritisch	Hier ist weder mobiles Arbeiten, noch Homeoffice zulässig

Tabelle 2: Ausstattungszuordnung

Durch den Einsatz weiterer Maßnahmen kann ein bestimmtes Szenario durchaus für einen höher bewerteten Sicherheitsbereich ertüchtigt werden.

Beispiel: Die Cloud-Dienste des LUIS sind grundsätzlich für Daten der Schutzstufe C konzipiert. Sollen hier etwa Bewerbungsunterlagen verwaltet werden, so sollte als zusätzliche Maßnahme eine verschlüsselte Datei (z.B. eine verschlüsselte ZIP-Datei) angelegt werden, um eine zusätzliche Sicherheitsschicht zu gewährleisten. Hierbei ist ein angemessenes Schlüssel-Management anzuwenden.

Weiterführende Hinweise
Homeoffice und mobile Arbeit unterliegen den jeweils geltenden Dienstanweisungen und Richtlinien. Es sollte sichergestellt werden, dass Beschäftigte in Homeoffice oder mobiler Arbeit insbesondere auf die folgenden Dokumente hingewiesen werden.

- Informationssicherheits- und Datenschutzaspekte beim mobilen Arbeiten, Merkblatt des Informationssicherheitsstabes der LUH
- Richtlinie zur Nutzung von E-Mails an der Leibniz Universität Hannover, Rundschreiben
- Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte an der Leibniz Universität Hannover, Rundschreiben
- Verschlüsselung dienstlich genutzter mobiler Speicherträger, Rundschreiben
- Homeoffice und mobile Arbeit an der Leibniz Universität Hannover, Rundschreiben
- Ordnung zur Informationssicherheit in der Leibniz Universität Hannover, Rundschreiben
- Nutzungsordnung der Leibniz Universität IT Services, Ordnung