Hochschule für Schauspielkunst
Ernst Busch

Busch – Blatt
9 / 2024

vom 01. August 2024

Herausgegeben

im Auftrag der Rektorin
der Hochschule für Schauspielkunst Ernst Busch Berlin

Zinnowitzer Straße 11
10115 Berlin
Telefon: 030/75 54 17 - 0
Telefax: 030/75 54 17 - 175

Inhalt:

Hochschule für Schauspielkunst Ernst Busch

Merkblatt zum Arbeits- und Gesundheitsschutz im Mobilen Arbeiten

Mobiles Arbeiten ermöglicht es, dienstliche Aufgaben ortsungebunden auszuüben. Die Beschäftigten wählen eigenverantwortlich Orte aus, die unter Berücksichtigung der notwendigen technischen und ergonomischen Voraussetzungen geeignet sind. Die Prinzipien der ergonomischen Gerätegestaltung und Arbeitsweise behalten auch im Mobilen Arbeiten ihre Gültigkeit. Aufgrund der räumlichen Distanz und der wechselnden Einsatzorte sind die betrieblichen Gestaltungsmöglichkeiten jedoch begrenzt. Daher steigt die persönliche Verantwortung der mobil arbeitenden Beschäftigten. Das Arbeitsschutzgesetz findet auch beim Mobilen Arbeiten uneingeschränkt Anwendung. In diesem Merkblatt sind Arbeits- und Gesundheitsschutzbedingungen beschrieben, die zu beachten und bestmöglich umzusetzen sind. Mit der Unterschrift des Antrags auf Mobile Arbeit wird dies durch den/die Beschäftigte*n bestätigt.

Nutzen Sie Ihre mobilen Endgeräte mit Bedacht.

- Wenn Sie länger als zwei Stunden an Ihrem Laptop arbeiten, sollte der Bildschirm eine angemessene Größe haben.
- Verwenden Sie bei längerem Arbeiten außerdem eine externe Maus und eine externe Tastatur. Ergonomisch gestaltete Eingabegeräte (Mäuse, Tastaturen) sind bei Personen, die sehr viel oder mit dem 10-Finger-System tippen oder bei Personen sinnvoll, denen herkömmliche Eingabegeräte gesundheitliche Beschwerden bereiten.
- Betreiben Sie Ihren Laptop auf einem Laptopständer stehend, um die Belastung der Halswirbelsäule zu verringern. Bei besonders langen Arbeitsphasen oder Arbeiten, die mit besonderen Anforderungen an das Sehen verbunden sind, empfiehlt sich der Anschluss eines externen PC-Monitors.
- Sorgen Sie für gutes Licht – bestenfalls Tageslicht plus Zimmerbeleuchtung – und eine angenehme Temperatur im Raum. Möglicherweise ist bei Spiegelungen oder zu heller Umgebung das Platzwechseln sinnvoll.
- Positionieren Sie den Bildschirm parallel zum Fenster, um Spiegelungen darauf zu vermeiden. Der Bildschirm sollte frontal vor Ihnen stehen und leicht nach hinten geneigt sein.
- Idealerweise liegt die oberste Bildschirmzeile höchstens auf Augenhöhe. Eine Blickdistanz von 50 bis 80 Zentimetern (ca. 2 DIN A4 Seiten lang) ist ideal.
- Ausreichend große Schriftzeichen (≥ 3,2 mm) in Positivdarstellung (dunkle Zeichen auf hellem Grund) erleichtern das Lesen.
- Von der Nutzung von Notebooks auf dem Schoß oder im Auto ist abzuraten.
- Schreibtisch und Arbeitsstuhl sollten rückengerecht eingestellt sein: Die Füße sollten ganzflächig Bodenkontakt haben, Knie und Hüfte sind im 90-Grad-Winkel, ebenso Ellenbogen. Hände und Unterarme liegen auf, die Schulterhaltung bleibt entspannt.
- Lässt sich die Tischhöhe nicht variieren, passen Sie die Stuhlhöhe an. Es gibt verschiedenste höhenverstellbare Stühle, Sitzbälle oder Hocker. Gegen stundenlanges Verharren in einer Position nützt es, hin und wieder aufzustehen und ein paar Schritte herumzulaufen.
- Sitzen Sie dynamisch und wechseln sie häufiger die Position. Auch ein Meditationskissen und Ähnliches kann mal zum Einsatz kommen, zum Beispiel bei einer Videokonferenz. Stehen Sie zwischendurch auf und telefonieren Sie auch im Stehen.
- Schaffen Sie sich eine ruhige Arbeitsatmosphäre. Bei lauten Umgebungsbedingungen (≥ 50 dB, z.B. Kantinenlärm) kann ein Gehörschutz, z.B. in Form von Ohropax, helfen.
- Nutzen Sie die Mittagspause für Bewegung: ein Spaziergang oder eine Runde joggen hält gesund, lädt die Batterien wieder auf – und steigert sogar die Laune, weil Endorphine ausgeschüttet werden.
- Lüften Sie regelmäßig und bauen Sie währenddessen kleine Bewegungspausen ein – das hilft auch, neue Konzentration zu schöpfen.
- Essen Sie bewusst und nicht nebenbei während der Arbeit. Nehmen Sie sich Zeit für gesunde Mahlzeiten. Gerade im Homeoffice neigen viele dazu, sich nicht ausreichend um gute Ernährung zu kümmern.

Zeitmanagement

- Planen Sie morgens den Arbeitstag und priorisieren Sie die wichtigsten Arbeitsziele.
- Versuchen Sie, klare Absprachen mit Familienmitgliedern oder Mitbewohnenden zu treffen, wie sie Störungen und Unterbrechungen möglichst minimieren können.
- Vereinbaren Sie feste Zeiten, wer wann für die Kinderbetreuung zuständig ist. Kleine Kinder zu beaufsichtigen und gleichzeitig konzentriert zu arbeiten ist in der Regel utopisch.
- Tauschen Sie sich mit anderen aus, die in einer vergleichbaren Belastungssituation arbeiten. Eventuell bringt Sie das zu neuen Lösungsideen, wie Sie besser mit den Stressfaktoren umgehen können.
- Legen Sie Auszeiten und Denkpausen ein: Wenn Konzentration und Energie verbraucht sind, brauchen Sie Regeneration.
- Vereinbaren Sie Zeitfenster für die Erreichbarkeit mit Vorgesetzten und Kolleg*innen.

Halten Sie Pausen- und Ruhephasen ein.

- Bitte achten Sie darauf, Ihre Tätigkeit so zu organisieren, dass Sie regelmäßig eine Bildschirmpause machen können. Pausen sind unverzichtbar. Seien Sie streng mit sich selbst: Starten Sie zu festen Zeiten und machen Sie regelmäßige Pausen. Ansonsten schaden Sie nicht nur Ihrer Gesundheit, sondern auch Ihrer Produktivität. Verbringen Sie Pausen am besten fernab vom Arbeitsplatz, ohne Blick auf Bildschirm oder Handy – draußen an der Luft bei Tageslicht.
- Trennen Sie dienstliche und private Belange und beantworten Sie beispielsweise dienstliche Emails und Telefonate während Ihrer Arbeitszeit aber trotz technischer Möglichkeiten nicht außerhalb Ihrer Arbeitszeit (z.B. am Wochenende oder im Urlaub).
- Halten Sie die gesetzlich vorgeschriebenen Pausenzeiten ein.
- Nach Beendigung der täglichen Arbeitszeit müssen Beschäftigte grundsätzlich eine ununterbrochene Ruhezeit von mind. 11 Stunden haben.

Hochschule für Schauspielkunst Ernst Busch

Merkblatt zu Datenschutz und IT-Sicherheit

1. Die für die HfS geltenden Bestimmungen zum Datenschutz/zur Datensicherheit, zur IT-Nutzung und zur Informationssicherheit gelten gleichermaßen auch für die Mobile Arbeit und sind einzuhalten.
2. In Bezug auf den Datenschutz und die Datensicherheit haben die Beschäftigten im Mobilen Arbeiten eine besondere Sorgfaltspflicht. Die Beschäftigten haben dafür zu sorgen, dass personenbezogene und vertrauliche Daten und Passwörter geschützt, ein unbefugter Zugang sowie unberechtigte Zugriffe auf Daten und Unterlagen wirksam verhindert werden. Die Nutzung offener WLAN-Hotspots ist ausdrücklich untersagt. Personenbezogene und/oder vertrauliche Daten dürfen nicht mittels SMS oder Messenger-Diensten (z. B. WhatsApp) übermittelt werden.
3. Mobile Endgeräte sind zwingend mit einem Passwort/Sperrcode vor unbefugtem Zugriff zu schützen. Es ist eine passwortgeschützte Bildschirmsperre mit kurzer Intervallzeit einzurichten.
4. Bei einem Verlust von dienstlichen Unterlagen oder einer Datenpanne, einem Datenleck oder bei einer möglichen Ausspähung von Daten muss umgehend das ServiceCenter IT (SC-IT), die/der Fachvorgesetzte und die/der Datenschutzbeauftragte der HfS benachrichtigt werden, um ggf. unverzüglich eine Änderung/Sperrung der Zugangsdaten zu veranlassen. Vorstehendes gilt entsprechend auch für alle anderen Störungen oder etwa die Beseitigung von Schadsoftware.
5. Verlust oder Beschädigung von dienstlichen Arbeitsmitteln ist der Dienststelle (Fachvorgesetzte*r) und dem SC-IT unverzüglich unter Darlegung der Umstände und des Hergangs anzuzeigen.
6. Tätigkeiten mit dem Schutzbedarf „Normal“ können in Mobiler Arbeit erledigt werden. Daten, vor allem solche mit Personenbezug oder sonstigen schützenswerten Inhalten, müssen bei Mobiler Arbeit mit besonderer Sorgfalt vor dem Zugriff durch unberechtigte Dritte und mindestens im gleichen Umfang wie am Büroarbeitsplatz geschützt werden. Die Prüfung, ob sich Tätigkeiten mit höherem Schutzbedarf unter Berücksichtigung datenschutzrechtlicher Anforderungen für die Mobile Arbeit eignen, liegt bei der HfS. Im Zweifel ist die/der Datenschutzbeauftragte zu Rate zu ziehen.
7. Für die Speicherung der Daten dürfen ausschließlich die durch die Dienststelle bereitgestellten Netzwerke und das dienstliche Dokumentenmanagementsystem genutzt werden. Papierakten sollen nicht bei der Mobilen Arbeit bearbeitet werden. Die HfS kann unter Berücksichtigung datenschutzrechtlicher Vorkehrungen abweichende Regelungen treffen.
8. Bei Vorhandensein von Fachverfahren darf die Verarbeitung von personenbezogenen Daten bei der Mobilen Arbeit nur im Rahmen dieser entsprechenden Fachverfahren erfolgen. Die vorhandenen Datenschutzkonzepte sind einzuhalten. Beschäftigten- und Sozialdaten dürfen nur an nicht öffentlich zugänglichen Bereichen bearbeitet werden.
9. Leistungs- und Verhaltenskontrollen der Beschäftigten durch Auswertung von Daten und Kenntnissen sind verboten; dennoch erlangte Erkenntnisse hieraus dürfen nicht zu Lasten der betroffenen Beschäftigten verwendet werden.

Entnehmen Sie nur erforderliche Daten: Entnehmen Sie nur die dienstlichen Daten aus der Beschäftigungsstelle, die unbedingt erforderlich sind. Personenbezogene und vertrauliche Daten sollen nicht entnommen werden. Bei dienstlicher Notwendigkeit können analoge Ressourcen vorab digitalisiert werden und auf sicheren Serverbereichen abgelegt werden.

Über VPN kann dann auf die Daten auch von außerhalb der HfS zugegriffen werden. Ist dies nicht möglich, sind dienstliche Clouds zu nutzen.

Geben Sie keine Daten an Unbefugte weiter: Schützen Sie alle Daten und Unterlagen, insbesondere die personenbezogenen und vertraulichen so, dass ein unberechtigter Zugang oder Zugriff wirksam verhindert wird (z.B. abschließbare Räumlichkeiten, abschließbare Schränke, Einsatz der Bildschirmsperre bei jedem Verlassen des Arbeitsplatzes, in Windows: Windowstaste + L). Sie dürfen weder an Dritte weitergegeben noch zur Einsicht zur Verfügung gestellt werden. Im Mobilen Arbeiten sind die Daten auch vor der Einsicht durch Angehörige oder Mitbewohner*innen zu schützen). Login-Daten dürfen nicht weitergegeben werden. Das Abspeichern persönlicher Zugangsdaten auf privaten und dienstlichen Geräten ist -mit Ausnahme der Terminalserver- untersagt. Sollte ein Gerät gehackt werden, ist das umgehend der HfS und dem SC-IT zu melden, so dass neue Passwörter vergeben werden können. Der Transport von Endgeräten und Datenträgern hat in dafür geeigneten Behältnissen zu erfolgen.
Daten/Informationen sind so zu schützen, dass Dritte, einschließlich der Familienmitglieder, keine Einsichts- und Zugriffsmöglichkeit haben.

Schützen Sie Ihre Geräte: Der mobile Arbeitsplatz darf nicht unbeaufsichtigt sein. Sperren Sie die von Ihnen genutzten Geräte bei Inaktivität und bewahren Sie sie sicher auf. Eine Weitergabe dienstlicher Geräte an Dritte ist untersagt. Nutzen Sie auf privaten Geräten ein separates Nutzerprofil für den dienstlichen Gebrauch und schützen Sie dieses mit einem Passwort. Halten Sie Passwörter geheim. Verwenden Sie bei Bedarf eine Blickschutzfolie für Ihren Laptop.

Nutzen Sie geeignete Software-Produkte: Verwenden Sie auf Ihren privaten Geräten, wenn Sie diese dienstlich nutzen, möglichst die gleichen Software-Produkte wie am dienstlichen Arbeitsplatz. Insoweit Dienstrechner zur Verfügung gestellt wurden, sind ausschließlich diese zu benutzen. Achten Sie darauf, für den dienstlichen Gebrauch auch auf Tablets und Smartphones datenschutzgerechte Apps und Dienste einzusetzen. Löschen Sie Apps und deinstallieren Sie Software, die Sie nicht mehr benötigen. Verwenden Sie nur empfohlene und datenschutzrechtlich zugelassene Produkte. Externe Cloud-Dienste wie Skype, DropBox, GoogleDrive und iCloud dürfen nicht genutzt werden.

Halten Sie die Technik Ihrer Geräte sicher: Stimmen Sie sich bei dienstlichen Geräten regelmäßig mit dem SC-IT ab, damit dieses erforderliche Systemeinstellungen und Aktualisierungen vornehmen kann. Konfigurieren Sie Ihre privaten Geräte datenschutzkonform. Nutzen Sie für diese Aufgaben ein separat einzurichtendes Administrations-Profil. Arbeiten Sie auf Ihrem privaten Gerät mit einem einfachen Benutzeraccount und nutzen für PC-Konfigurations- und -Installationsaufgaben einen extra Administratorenaccount. Aktualisieren Sie regelmäßig das Betriebssystem und alle installierten Programme/Apps. Installieren Sie eine Virenschutzsoftware und aktivieren Sie die Firewall auf Ihren Geräten. Deaktivieren Sie die Rufnummernanzeige auf Ihren privaten Telefonen, wenn Sie diese den Gesprächspartnern nicht anzeigen möchten.

Bleiben Sie auf dem aktuellen Stand:

Informationen zum Datenschutz. Zahlreiche Hinweise und ausführliche Anleitungen finden Sie auch im Datenschutz-Blog der Technischen Universität Berlin (TUB): https://blogs.tu-berlin.de/datenschutz_notizen/category/anleitungen

Berliner Datenschutzgesetz BlnDSG: https://www.datenschutz-berlin.de/datenschutz/rechtliche-grundlagen/berliner-datenschutzgesetz/