Freistaat Thüringen
Landesamt für Finanzen

Telearbeit in den Thüringer Finanzämtern

Sicherheitskonzept für den Einsatz von IT-Geräten und den Umgang mit dienstlichen Informationen am häuslichen Telearbeitsplatz

(kurz: SiKo Telearbeit FÄ)

Vers. 0.3 (23.03.2021)

Version:	0.4
Stand vom:	23.03.2021
Ablageort:	Intranet (**A**llgemeines **I**nformations**S**ystem - AIS)
Dokumententyp:	Dienstanweisung
Status:	Entwurf - Zuarbeit an TFM
Vertraulichkeitsstufe:	Nur für den Dienstgebrauch

		Einrichtung/Rolle Datum	Name
Autoren-übersicht	von: am:	TFM Autor 23.03.2021	Daniel Faulwetter
Review	von: am:	TFM Rolle __.__2021	
Review	von: am:	TFM Rolle __.__2021	
Freigegeben:	von: am:	TFM Rolle __.__2021	

Inhaltsverzeichnis

Geschlechterspezifische Formulierungen

1 Die Regelungen dieser Dienstanweisung und alle Funktions-, Status- und sonstigen Bezeichnungen meinen jeweils alle Geschlechter.

Geltungsbereich

2 Die Risiken bzw. Gefährdungen bei der Verarbeitung von personenbezogenen Daten oder dem Steuergeheimnis unterliegenden Daten sind vielfältig. Die derzeit möglichen technischen Maßnahmen reichen nicht immer aus, um Datenverluste und unberechtigte Zugriffe auf schutzbedürftige Daten zu verhindern.

3 Dieses Sicherheitskonzept stellt die zur Gewährleistung der Informationssicherheit notwendigen organisatorischen und technischen Regelungen (organisatorische Regelungen: OR; technische Regelungen: TR) – insbesondere beim Umgang mit IT-Geräten und dienstlichen Informationen am häuslichen Telearbeitsplatz dar.

4 Es ist von allen Bediensteten beim Umgang mit Informationstechnik zum Einsatz im Rahmen von Telearbeit in den Thüringer Finanzämtern zu beachten.

5 Über dieses Sicherheitskonzept hinausgehende Regelungen sind durch die Fachreferate des TFM eigenständig zu veranlassen.

Sensibilisierung der Nutzer

6 Der Nutzer eines häuslichen Telearbeitsplatzes muss entsprechend seiner vereinbarten Verpflichtungen mitwirken und sensibilisiert sein, die Gesamtheit der getroffenen Maßnahmen einzuhalten.

7 Der Nutzer kann sich bei Fragen zur Umsetzung der durch ihn zu treffenden technischen und organisatorischen Maßnahmen zur Einhaltung der datenschutzrechtlichen Anforderungen direkt an

- den Datenschutzbeauftragten seiner Behörde oder
- an das für Datenschutz zuständige Referat des TFM wenden.

8 Der Nutzer kann sich bei Fragen zur Umsetzung der durch ihn zu treffenden technischen und organisatorischen Maßnahmen zur Einhaltung der Informationssicherheit Anforderungen direkt an

- an die für Informationssicherheit zuständige Stelle seiner Dienststelle oder
- an den Systembetreuer seiner Dienststelle

wenden.

OR 01. Vor der Übergabe der Geräte ist dem Nutzer dieses Sicherheitskonzept bekannt zu geben.

OR 02. Lizenzbestimmungen und datenschutzrechtliche Belange sind in die regelmäßig durchzuführenden Belehrungen einzubeziehen.

Verantwortlichkeit des Bediensteten

9 Der Bedienstete handelt beim Umgang mit dienstlichen Informationen im besonderen Maße eigenverantwortlich. Es obliegt insbesondere auch dem Bediensteten, dass bei häuslicher Telearbeit die Bestimmungen zum Datenschutz und zur Informationssicherheit eingehalten werden.

Verantwortlichkeiten der Dienststelle

10 Durch den Bediensteten ist die Einhaltung der notwendigen Maßnahmen zur Gewährleistung des Datenschutzes, des Steuergeheimnisses und der Informationssicherheit am Telearbeitsplatz zu erklären.

11 Vor der Genehmigung eines häuslichen Telearbeitsplatzes kann durch die Dienststelle – soweit möglich – geprüft werden, ob alle in dieser Dienstanweisung und in der mit dem Bediensteten abzuschließenden individuellen Vereinbarung vorgesehenen Maßnahmen zur Gewährleistung des Datenschutzes und zur Einhaltung der Vorschriften der Abgabenordnung zum Steuergeheimnis auch am häuslichen Telearbeitsplatz eingehalten werden können. Über die tatsächlichen Gegebenheiten vor Ort ist hierzu ein Protokoll der Inaugenscheinnahme zu fertigen.

Nutzung der dienstlich bereitgestellten Informationstechnik

12 Der Einsatz von IT-Technik richtet sich nach den fachlichen Notwendigkeiten.

13 Die am häuslichen Telearbeitsplatz notwendige technische Ausstattung wird durch das TLF in Abstimmung mit dem TFM festgelegt. Die notwendige Hardware (z. B. PC-Technik/ Notebook, Monitor, Drucker, Eingabegeräte und Sicherheitsausstattung [z. B. OTP-Token]) sowie die zur Erfüllung der Fachaufgaben notwendige Software werden durch das TLF zur Verfügung gestellt.

14 Der Bereich der Nutzung der dienstlich bereitgestellten Informationstechnik ist einzuschränken, um missbräuchliche Nutzungen zu verhindern.

OR 03. Dienstlich bereitgestellte Informationstechnik darf nur für dienstliche Zwecke und aufgabengebunden verwendet werden.

OR 04. Für dienstliche Zwecke darf – mit Ausnahme der zur Herstellung der Internetverbindung notwendigen Komponenten – nur dienstlich bereitgestellte Informationstechnik genutzt werden.

OR 05. Der Einsatz sonstiger, insbesondere privater oder nicht lizenzierter Software ist untersagt.

OR 06. Änderungen an der bereitgestellten Hard- und Software sind – sofern nicht ausdrücklich zugelassen ist oder der bestimmungsgemäßen Nutzung entspricht – untersagt. Ausnahmen bedürfen der Zustimmung des für IT- Grundsatzangelegenheiten zuständigen Referats des TLF.

OR 07. Die Nutzung von E-Mail und des Internets für private Zwecke ist nicht gestattet.

OR 08. Eine private Nutzung durch den Bediensteten oder durch Dritte (insbesondere am Telearbeitsplatz) ist untersagt.

Verwaltung der Geräte

15 Es muss nachvollziehbar sein, wer und welche Dienststelle welches Notebook innehat.

OR 09. Sämtliche Übergaben sind in geeigneter Weise zu dokumentieren (Übergabeprotokolle).

OR 10. Die einzelnen Geräte sind bestandsmäßig in der jeweiligen Dienststelle zu führen. Hierbei sind die Bestimmungen über den Nachweis von Vermögen zu beachten.

OR 11. Änderungen am Gerätebestand erfolgen nur auf Weisung des TLF, Referat IT-Grundsatzangelegenheiten oder auf Weisung des TFM; dies gilt insbesondere für Umsetzungen, Aussonderungen sowie Rückgaben an das TLF.[i]

OR 12. Bei Beendigung der häuslichen Telearbeit sind sämtliche IT-Technik, welche im Zusammenhang mit dem Telearbeitsplatz übergeben wurden, zurückzuführen.

16 Um einen Missbrauch der bereitgestellten Geräte zu vermeiden, ist die Berechtigung zur Installation von Software zu beschränken. Darüber hinaus darf nur durch das TFM, das TLRZ oder das TLF freigegebene Software zum Einsatz kommen.

OR 13. Das TLF stellt sicher, dass nur freigegebene Software bereitgestellt wird.

OR 14. Die Installation der erforderlichen Software erfolgt durch das TLF.

Dienstlich bereitgestellte IT-Geräte

17 Die dienstlich bereitgestellten IT-Geräte, insbesondere PC/ Notebooks werden durch die Dienststelle gebrauchsfertig übergeben. Mit der Bereitstellung der Informationstechnik für den häuslichen Telearbeitsplatz ist in jedem Fall durch die Dienststelle eine Einweisung vorzunehmen. Diese kann auch als schriftliche Anleitung erfolgen. Die erstmalige Inbetriebnahme der dienstlichen Technik am Telearbeitsplatz wird bei Bedarf durch die für die Betreuung der Systeme in den Dienststellen zuständigen Stellen unterstützt.

18 Hinsichtlich des Betriebs und der Verwaltung der dienstlich bereitgestellten Informationstechnik (insbesondere Bestandsverwaltung, Umsetzung, Aussonderung, Reparatur, Verlust, Datenlöschung) gelten die für die Dienststelle getroffenen Regelungen für Arbeitsplatztechnik analog am häuslichen Telearbeitsplatz. Auf die entsprechenden Regelungen u.a. in der „Rahmenrichtlinie zur Informationssicherheit - Katalog organisatorischer Maßnahmen“ und im Umlaufordner der Dienststelle in der jeweils aktuellen Fassung wird verwiesen.

OR 15. Die dienstlich bereitgestellten IT-Geräte sind durch den Bediensteten vor Beschädigung, unsachgemäßem Gebrauch und unbefugter Nutzung zu schützen.

19 Die PCs / Notebooks verfügen und Antiviren-Software; Notebooks verfügen über eine zusätzliche Verschlüsselung.

OR 16. Die standardmäßig bei Ausgabe der Geräte vorinstallierten Schutzmechanismen dürfen weder deaktiviert noch deinstalliert werden.

Durch den Bediensteten bereitzustellende Technik

20 Soweit zur netztechnischen Anbindung des häuslichen Telearbeitsplatzes zusätzliche IT-Komponenten durch den Bediensteten bereitzustellen sind (u.a. ausreichend performanter Internetzugang, Router mit Firewall), werden Art und Umfang der zu stellenden Technik durch das TFM in Abstimmung mit dem TLF vorgegeben.

21 Die nachfolgend aufgeführten Vorgaben leiten sich aus aktuellen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Konfiguration des Routers (Internetzugangspunkt) und dem Einsatz von WLAN bei Verbindung zum Router ab.

OR 17. Grundsätzlich hat der Bedienstete für die durch ihn bereitzustellende Technik die Betriebssicherheit (insb. Verfügbarkeit, Wiederherstellung im Havariefall) eigenverantwortlich zu gewährleisten.

OR 18. Insbesondere ist der Bedienstete verpflichtet, nur dem Stand der Technik entsprechende Hard- und Software zu nutzen. Stehen für die Hard- und Software, die für den Internetzugang genutzt wird, Sicherheits- oder Firmwareupdates bereit, sind diese unverzüglich zu installieren.

22 Die Verbindung der von der Dienststelle bereitgestellten IT-Geräte mit den durch den Bediensteten gestellten IT-Komponenten kann kabelgestützt (Netzwerkkabel/ RJ45, üblicherweise CAT 5E) oder drahtlos (insb. WLAN) erfolgen. Bei Nutzung von WLAN sind die unter OR 20 dargestellten Anforderungen zu beachten.

Router Konfiguration

OR 19. Unabhängig von der Art des Aufbaus der Internetverbindung muss die Routerkonfiguration mindestens folgenden Anforderungen entsprechen:

a. Die Administration des Routers ist nur nach Eingabe eines hinreichend komplexen Passworts möglich. (Das Werks-Passwort des Routers muss geändert sein.)
b. Um Router zu administrieren bzw. zu überwachen, sind ausreichend verschlüsselte Protokolle einzusetzen (z. B. Zugang zur Administrationsschnittstelle nur über https).
c. Das Netzwerk ist durch eine aktive, hardwaregestützte Firewall (z. B. eine in den Router integrierte Firewall) geschützt.
d. Der Router besitzt eine integrierte und aktivierte automatische IP-Adressen-Vergabe.
e. Kein Zugangspunkt zum Drahtlosnetzwerk darf unverschlüsselte Verbindungen zulassen. Sie dürfen nicht als öffentliche Internetzugangspunkte (Hotspot) dienen.
f. Der Router darf keine sog. „Exposed Host"-Konfiguration aufweisen, die es ermöglicht, dass Geräte auf allen Ports direkt über das Internet erreichbar sind.
g. Die Punkte a und b gelten für sämtliche aktive Netzkomponenten zur Herstellung oder Erweiterung des drahtlosen Heimnetzwerks.

Nutzung von WLAN

OR 20. Sofern die Verbindung zum Internetzugangspunkt drahtlos (WLAN) statt über Kabelverbindung aufgebaut wird, müssen während der Dauer der dienstlichen Nutzung zusätzlich folgende Anforderungen erfüllt sein[1]:

a. Die Drahtlosverbindung sowie der Zugang zur Drahtlosverbindung müssen entsprechend dem Stand der Technik verschlüsselt sein - maßgeblich sind hier die Empfehlungen des BSI zu Verschlüsselung und Passwortschutz der Drahtlosverbindung[2].
b. Das WPS-PIN-Verfahren muss am Router deaktiviert sein.

1 Aus Sicherheitsgründen werden diese Konfigurationseinstellungen für die Drahtlosverbindung auch bei ausschließlich privater Nutzung empfohlen.
2 Zurzeit empfiehlt das BSI mindestens die Verschlüsselung per WPA2 und einen mindestens 20 Zeichen langen, komplexen Netzwerkschlüssel. Der Netzwerkschlüssel darf nicht dem Netzwerkschlüssel im Auslieferungszustand entsprechen.

Anbindung an die Informationstechnik der Dienststelle

23 Datenübertragungen und Datenaustausche zwischen dem häuslichen Telearbeitsplatz und der Dienststelle erfolgen ausschließlich über den bereitgestellten VPN-Zugang. Die darüber übertragenen Daten werden dabei über eine verschlüsselte Verbindung übertragen. Mithilfe des VPN-Zugangs können somit schutzbedürftige Daten über Datennetze wie das Internet übertragen werden, ohne die Vertraulichkeit dieser Daten zu gefährden. Für häusliche Telearbeitsplätze wird dem Bediensteten ein Zugriff über eine sichere VPN-Verbindung zwischen dem dienstlichen Endgerät und dem CN der Thüringer Landesverwaltung bereitgestellt.

24 Die Verbindung des häuslichen Telearbeitsplatzes zum CN wird über den privaten Internetanschluss und Router des Bediensteten hergestellt.

OR 21. Der Zugang zum Landesdatennetz ist nur über eine gesicherte VPN-Verbindung möglich und zulässig. Diese ist mit den bereitgestellten Mitteln zur Zwei-Faktor-Authentifizierung (z. B. OTP-Generator, OTP-SMS, Yubikey) herzustellen.

TR 01. Hierfür ist auf dem dienstlichen Endgerät eine spezielle Verschlüsselungs- und Zugangssoftware installiert.

25 Nach erfolgter Einwahl erhält der Bedienstete Zugriff auf die für die Erledigung der Aufgaben notwendigen Fachverfahren, Ressourcen sowie Kommunikationsmittel (z. B. E-Mail).

26 Darüber hinaus wird für die Anbindung des häuslichen Telearbeitsplatzes an die Informationstechnik der Dienststelle auf das „Sicherheitskonzept für die Anbindung von außerhalb der Dienststelle eingesetzter Informationstechnik an das Netz der Steuerverwaltung“ in der jeweils aktuellen Fassung verwiesen.

Zugang zu und Umgang mit dienstlich bereitgestellter Informationstechnik sowie dienstlichen Unterlagen und Informationen einschließlich deren Aufbewahrung

OR 22. Der Umgang mit Informationstechnik hat so zu erfolgen, dass ein Verlust oder eine Beschädigung des Notebooks sowie der Verlust von Daten ausgeschlossen sind.

OR 23. Eine Aufbewahrung des Notebooks, von Datenträgern und aller Unterlagen mit personenbezogenen Daten außerhalb der Diensträume ist nur mit Genehmigung (z. B. Dienstreiseantrag oder genehmigter Heimarbeitsplatz) zulässig.

OR 24. Die Medien zur Zwei-Faktor-Authentifizierung (z. B. PIN und Passwortgenerator) sind unbedingt getrennt voneinander zu verwahren. Eine unbeaufsichtigte Aufbewahrung (z. B. im Hotelzimmer, in Tagungsräumen) ist nicht zulässig.

OR 25. In jedem Fall ist darauf zu achten, dass die Aufbewahrung verschlossen erfolgt. Notebooks sind nach Gebrauch (nach dem Ende der Tätigkeit) immer auszuschalten.

OR 26. Am häuslichen Telearbeitsplatz ist der PC/ das Notebook, alle Datenträger und sämtliche Unterlagen mit personenbezogenen Daten nach Beendigung der Tätigkeit und bei absehbar längeren Arbeitsunterbrechungen in einem verschließbaren Behältnis oder in einem verschließbaren Schrank aufzubewahren. Dabei muss sichergestellt sein, dass die dienstlichen Unterlagen vor dem Zugriff Dritter geschützt sind, d. h. der Schlüssel ist für Dritte unzugänglich aufzubewahren.

OR 27. Der Transport des Notebooks, der Datenträger und dienstlicher Unterlagen ist nur im nicht einsehbaren Kofferraumbereich des PKW zulässig. Bei zwingend erforderlicher Fahrtunterbrechung hat sich der Bedienstete vom ordnungsgemäßen Verschluss des PKW, insbesondere des Kofferraums, zu überzeugen.

OR 28. Bei vorhersehbarer Nichtbenutzung eines Notebooks und dienstlicher Unterlagen mit personenbezogenen Daten über einen längeren Zeitraum (Urlaub oder sonstige Abwesenheit, die länger als 5 Arbeitstage dauert) sind die Geräte, die Datenträger und Unterlagen grundsätzlich in der Dienststelle an geeigneter Stelle abzugeben (z. B. in den Finanzämtern beim Sachgebietsleiter, Innendienst oder in der Geschäftsstelle), wo sie einbruchsicher und verschlossen aufzubewahren sind.

OR 29. Das Verbringen von Verschlusssachen mit der Einstufung höher als VS-VERTRAULICH im Sinne der Verschlusssachenanweisung für den Freistaat Thüringen an den Telearbeitsplatz ist grundsätzlich im Vorfeld mit dem Geheimschutzbeauftragten der Dienststelle abzustimmen und zu dokumentieren.

Arbeitsunterbrechungen

27 Begibt sich der Bedienstete nach Inbetriebnahme des Notebooks auch nur kurzzeitig an einen anderen Ort, von dem aus er nicht in der Lage ist, die Bedienung des Gerätes bzw. die Einsichtnahme in Unterlagen durch eine andere Person einzusehen, sind Maßnahmen erforderlich, die eine unbefugten Zugriff auf die Daten verhindern.

28 Dies gilt in besonderer Weise auch für die Nutzung am häuslichen Telearbeitsplatz, soweit sich weitere Personen in der Wohnung aufhalten. Dabei ist es unerheblich, ob es sich ausschließlich um Familienangehörige oder Kinder handelt.

OR 30. Die dienstliche Informationstechnik und die dienstlichen Unterlagen sind nicht unbeaufsichtigt zu lassen.

OR 31. Verlässt der Bedienstete nach Inbetriebnahme des APC auch nur kurzzeitig den häuslichen Telearbeitsplatz, hat er seinen Arbeitsraum so zu verschließen, dass kein Dritter Zugang zum APC und zu den Unterlagen hat. Ist dies nicht möglich, hat er:

a. Die Bildschirmsperre zu aktivieren. Die Bildschirmsperre darf sich nur durch Eingabe eines Passworts, nicht aber durch einfachen Druck auf eine beliebige Taste wieder aufheben lassen.
b. Es ist sich als Nutzer aus einer Mehrnutzerumgebung abzumelden.
c. Die Unterlagen und Datenträger sind unter Verschluss zu nehmen.

29 Passwörter sind geeignete Maßnahmen, um den Zugriff auf IT-Systeme und Daten zu beschränken und nur Nutzer nur den Zugriff auf Daten und Software erhalten, den sie zur Aufgabenerfüllung benötigen. Dies gilt insbesondere für Anmeldekennwörter.

OR 32. Das TLF stellt sicher, dass der direkte Zugriff auf Daten sowie auf Programme, mit denen auf Datenbanken zugegriffen werden kann, durch Benutzerkennungen und das Login-Passwort geschützt. Zugriffskennungen und Passwörter sind vor der Einsichtnahme Dritter zu sichern.

TR 02. Notebooks sind mit einem BIOS-Passwort abzusichern.

OR 33. Diese sind nur den Fachsystembetreuern bekannt zu geben.

OR 34. Login-Sperren können nur vom Benutzer zusammen mit dem Fachsystembetreuer aufgehoben werden, indem beim Verfahrensbetreuer des TLF ein neues Passwort anfordert wird (Challenge/Response- Verfahren). Der User-HelpDesk (UHD) ist zu nutzen.

OR 35. Die jeweils standardmäßig bei Ausgabe der Geräte vorinstallierten oder sonstig angebrachten Schutzmechanismen dürfen ohne Genehmigung des TLF weder deaktiviert noch deinstalliert werden.

30 Für die am Telearbeitsplatz eingesetzten APC/ Notebooks gelten die Regelungen der Passwortrichtlinie des Landes in der jeweils geltenden Fassung und sofern vorhanden, weitere für die Dienststellen verbindliche Festlegungen.

Vorkommnisse, Störungen, Verlust

31 Bei sicherheitsrelevanten Vorkommnissen (z.B. Verlust, Einbruch, Diebstahl, unbefugter Gebrauch, Virenbefall) ist über den Systembetreuer des Finanzamtes der UserHelpDesk (UHD) zu informieren. Ebenso ist bei Störungen zu verfahren.

32 Die Einbeziehung des Informationssicherheitsbeauftragten (ISB) und / oder des Informationssicherheitskoordinators (ISK) der Dienststelle ist über den Systembetreuer und UHD sichergestellt. Die jeweiligen Fachvorgesetzten bzw. Datenschutzbeauftragte sind bei Bedarf gesondert zu informieren.

33 Unabhängig davon wird auf die Arbeitsanweisung zur Behandlung von IT-Sicherheitsmeldungen und IT-Sicherheitsvorfällen in der jeweils geltenden Fassung verwiesen.

Inkrafttreten

Die Regelungen des Sicherheitskonzepts sind ab ihrer Bekanntgabe verbindlich zu beachten; sie werden zur verbindlichen Arbeitsgrundlage des Informationsverbundes des Finanzamtes.

Die Bekanntgabe erfolgt im Allgemeinen Informationssystem (AIS) der Thüringer Finanzverwaltung.

Mitgeltende Unterlagen

- Leitlinie zur Informationssicherheit für die Thüringer Landesfinanzdirektion und die Finanzämter
- Arbeitsanweisung zur Behandlung von IT-Sicherheitsmeldungen und IT-Sicherheitsvorfällen
- Rahmenrichtlinie zur Informationssicherheit bzw. bestehende IT-Sicherheitskonzepte (z.B. „Sicherheitskonzept für die Anbindung von außerhalb der Dienststelle eingesetzter IT-Technik an das Netz der Steuerverwaltung“ in der jeweils aktuellen Fassung)
- Passwortrichtlinie in der jeweils aktuellen Fassung

1.1 Abkürzungen

AIS	Allgemeines Informationssystem der Thüringer Finanzverwaltung.
APC	Arbeitsplatz PC (Personal Computer)
BSI	Bundesamt für Sicherheit in der Informationstechnik
OTP-Token	OneTimePass – Einmal-Passwort-Generator
ISB	Informationssicherheitsbeauftragter
ISK	Informationssicherheitskoordinator
IT	Informationstechnik, Bereich der Informations- und Datenverarbeitung
KVP	Kontinuierlicher Verbesserungsprozess
TFM	Thüringer Finanzministerium
TLF	Thüringer Landesamt für Finanzen
UHD	UserHelpDesk (Ticketbasiertes Hilfesystem des TLF – ein Ticket kann über den Systembetreuer des Finanzamtes erstellt werden)
VPN	Virtual Private Network -> deutsch virtuelles privates Netzwerk (Bezeichnet eine spezielle Netzwerkverbindung, die von Unbeteiligten nicht einsehbar ist.)
z.B.	zum Beispiel

1.2 Dokumenthistorie

[i] Die Verfügung vom 11.12.2003, Az. O 2200 A – 04/04 – L 3105 (G) ist auch nach Herstellung der Zweistufigkeit im Geschäftsbereich des TFM zu beachten.