Formular drucken | Dieses Formular ist am Bildschirm ausfüllbar | Formular zurücksetzen

Ticket-Nummer:

UNIVERSITÄTS KLINIKUM FREIBURG
Klinikrechenzentrum
Kommunikation/Netzwerk

Antrag auf Telearbeit

☐ **Erstantrag** ☐ **Folgeantrag ohne Änderung** ☐ **Folgeantrag mit Änderung**

☐ Telearbeitsplatz zuhause ☐ wechselnder Einsatzort

Antrag des/der Arbeitnehmers/-in

Nachname: _____ Vorname: _____

E-Mail (dienstlich): _____

Telefon (privat): _____ Telefon (dienstlich): _____

Wohnort: _____

Abteilung: _____

Arbeitsvertrag: ☐ unbefristet ☐ befristet bis _____

derzeitige Arbeitszeit: ☐ vollbeschäftigt ☐ _____ % teilzeitbeschäftigt

Beginn der Telearbeit: _____ Dauer der Telearbeit: _____ (mind. 6 Monate, max. 3 Jahre)

Umfang der gewünschten Telearbeitszeiten: _____ Stunden/Woche

Begründung und Beschreibung der beabsichtigten Telearbeit (ggf. auf Beiblatt fortsetzen)

☐ Support IT ☐ zur Vereinbarkeit von Beruf und Familie ☐ Gesundheit

☐ med. Hintergrunddienst ☐ gelegentlicher Zugriff ☐ anderer Wohnort

_____

_____

_____

_____

_____

Benötigte Dienste (ggf. in Abstimmung mit dem/der IT-Koordinator/-in)

☐ Das Formular "Anwendungen für Telearbeitsplatz" habe ich ausgefüllt

Fernzugriff mit (Erläuterungen siehe Anhang)**:**

☐ Terminalserver (SSL-VPN)
mit beliebigen PCs/Notebooks über Terminalserver mit definiertem Anwendungsspektrum
Hinweis: Beim Terminalserver ist kein Ausdruck auf den eigenen Drucker möglich!)

Reicht die privat vorhandene Ausstattung zur Erledigung der von Ihnen zu erbringenden Arbeiten?

☐ ja, Betriebssystem Privat-PC: _____

☐ nein, ich benötige ein(en) konfiguriertes/-n PC/ Notebook vom Klinikum

☐ Neubeschaffung eines PCs/Notebooks notwendig

☐ vorhandenes/-r dienstliches/-r PC/Notebook wird verwendet

Computername: _____

☐ Vollzugriff (IPSec-VPN)
mit klinikumseigenem PC/Notebook, das einem definierten Mindeststandard entspricht
(Vollzugriff auf Klinikumsnetzwerk mit erweiterten Datenschutzanforderungen)

☐ Neubeschaffung eines PCs/Notebooks notwendig

☐ vorhandenes/-r dienstliches/-r PC/Notebook wird verwendet

Computername: _____

60126625 ForManFR / 20.03.2015

Formular drucken | Formular zurücksetzen

Antrag auf Telearbeit

Ich verfüge an meinem Wohnort über folgende Netzverbindung:

☐ DSL (Geschwindigkeit: _____)

☐ Kabel ☐ LTE/UMTS ☐ andere: _____

Flatrate vorhanden (Telefon- und Internetkosten müssen selbst getragen werden):

► für Internetzugang: ☐ nein ☐ ja

► für Telefon: ☐ nein ☐ ja

Datenschutz – Zusatzfragen des Datenschutzbeauftragten zu Ihrem Antrag auf Telearbeit

Im Rahmen der Prüfung und Bearbeitung des Antrages bitte ich Sie, mir noch einige Informationen mitzuteilen:

1. Welche Aufgaben und Tätigkeiten werden Sie über den Telearbeitsplatz ausführen?

_____

_____

_____

_____

Ein vorzeitiger Wegfall der Zugangsnotwendigkeit wird dem KRZ mitgeteilt durch:

_____

2. Welche personenbezogenen Daten werden verarbeitet (Mitarbeiterdaten, Patientendaten, bitte hierzu nähere Angaben)?

☐ Patientendaten ☐ Mitarbeiterdaten ☐ sonstige personenbezogene Daten

☐ keine personenbezogene Daten

_____

_____

_____

3. Werden Unterlagen zuhause aufbewahrt?

☐ nein ☐ ja

Falls ja, besteht die Möglichkeit diese sicher zu verschließen (Arbeitszimmer, abschließbarer Schrank, etc.)?

☐ nein ☐ ja

4. Ist es erforderlich, dass Unterlagen zuhause ausgedruckt werden?

☐ nein ☐ ja

Falls ja, wie werden nicht mehr benötigte Unterlagen sicher entsorgt?

_____

5. Werden Unterlagen zwischen der Dienststelle und der Wohnung ausgetauscht? Falls ja, wie? (verschließbare Aktentasche, eigener Pkw, öffentliche Verkehrsmittel, etc.)

☐ nein ☐ ja

Falls ja, wie (verschließbare Aktentasche, eigener Pkw, öffentliche Verkehrsmittel, etc.)?

_____

Antrag auf Telearbeit

UNIVERSITÄTS KLINIKUM FREIBURG

6. Haben Sie in den vergangenen zwei Jahren eine Datenschutzschulung besucht?

☐ nein ☐ ja

7. Falls Sie einen Vollzugriff beantragt haben, warum ist dieser im Rahmen der Antragstellung erforderlich?

_____

_____

_____

Können Sie Ihre Tätigkeit auch mit einem auf Ihren Bedarf eingeschränkten Anwendungsspektrum erfüllen?

☐ nein, weil: _____

☐ ja

8. Die Allgemeinen Anforderungen des Datenschutzes an Tele-/Heimarbeit wurde von mir zur Kenntnis genommen.

☐ nein ☐ ja

Die in diesem Dokument geforderten Maßnahmen können und werden von mir umgesetzt bzw. eingehalten.

☐ nein ☐ ja

Wenn nein, weil: _____

_____

_____

Einverständnis

Der Benutzer/Die Benutzerin verpflichtet sich, die Kommunikationsdienste ausschließlich dienstlich bzw. für wissenschaftliche Zwecke zu nutzen. Die Speicherung von personenbezogenen Daten außerhalb des Klinikums ist verboten, da die Vertraulichkeit nicht gewährleistet werden kann. Ich erkläre hiermit, dass ich die Bestimmungen des Landesdatenschutzgesetzes (LDSG), die Datenschutzbestimmungen des Landeskrankenhausgesetzes (LKHG), die betrieblichen Bestimmungen zum Datenschutz, insbesondere die Datenschutz-Regelung Nr. 7 (Datenschutz Handbuch des Klinikums) bei der Nutzung der Internet-Dienste gewissenhaft beachte. Ich wurde auf das Datengeheimnis nach § 6 LDSG verpflichtet.

Der Benutzer/Die Benutzerin nimmt ausdrücklich zur Kenntnis:

Sie werden ein Token zur Passworterzeugung für den Zugriff auf das Klinikumsnetzwerk erhalten, welches Sie unbedingt und immer vertraulich behandeln müssen. Geben Sie dieses nicht an Dritte weiter. Sie sollten dieses getrennt vom PC aufbewahren. Einen Verlust oder der Verdacht eines Fremdzugriffs melden Sie bitte unverzüglich dem Klinikrechenzentrum.
Durch Ihre Unterschrift bestätigen Sie neben der Einhaltung der oben genannten Anforderungen auch den Erhalt des Merkblattes ***für Klinikumsmitarbeiter zum VPN-Zugang*** sowie der „Allgemeinen Anforderungen des Datenschutzes an Tele-/Heimarbeitsplätze" (vgl. Anlagen und Intranet - IT Service - Dokumentationen - Remote-/Fernzugang).

Datum	Name Antragsteller/-in, Benutzer/-in	✕ Unterschrift Antragsteller/-in, Benutzer/-in

UNIVERSITÄTS KLINIKUM FREIBURG

Antrag auf Telearbeit

Stellungnahme des/der Abteilungsleiter/-in

☐ Der Antrag wird befürwortet

☐ Die Finanzierung (derzeit 1.500,-- € / 3 Jahre) erfolgt über die Kostenstelle: _____

☐ Der Antrag wird nicht bzw. mit folgenden Änderungen befürwortet:

_____

_____

_____

Datum	Name Abteilungsleiter/-in, Institutsleiter/-in	✕ Unterschrift Abteilungsleiter/-in, Institutsleiter/-in

Stellungnahme des/der IT-Koordinators/-in (Zustimmung auch per Ticket möglich)

☐ Der Antrag wird befürwortet

☐ Der Antrag wird nicht bzw. mit folgenden Änderungen befürwortet:

_____

_____

_____

Datum	Name IT-Koordinator/-in	✕ Unterschrift IT-Koordinator/-in

Bitte nach Unterschrift an das KRZ weiterleiten, gerne über das Ticketsystem (it.support@uniklinik-freiburg.de).

Die Zustimmung des Datenschutzbeauftragten, des KRZ, des Personalrats und der Beauftragten für Chancengleichheit erfolgen über das Ticketsystem.

Zustimmung ist erfolgt

☐ IT-Koordination ☐ per Ticket

☐ Datenschutzbeauftragter

☐ KRZ

☐ Personalrat

☐ Beauftragte für Chancengleichheit

☐ G4

Datum	Name KRZ-Mitarbeiter/-in	✕ Unterschrift KRZ-Mitarbeiter/-in

Seite verbleibt beim Nutzer!

UNIVERSITÄTS KLINIKUM FREIBURG

Antrag auf Telearbeit - Anhang

Informationen des Klinikrechenzentrums zum Antrag auf VPN-Zugang

Zugang über **Terminalserver** (**SSL**-VPN)

Bei Zugang über einen Terminalserver wird in einem Windowsfenster eine vollständige „Windows Umgebung“ zur Verfügung gestellt. Es können hier die Standard Anwendungen verwendet werden, wie Office, SAP, Medoc (siehe Anwendungsliste). Sie können auf Serververzeichnisse und Dateien des Klinikums zugreifen und über Netzwerkdrucker im Klinikumsnetzwerk drucken. Nicht möglich ist ein lokales speichern, Zugriff auf USB-Sticks/ externe Festplatten, lokale Drucker usw. Dadurch ist ein hohes Maß an Sicherheit der Daten gewährleistet. Eigene Programme können nicht installiert werden. Diese Verbindung stellt keine hohen Anforderungen an die Bandbreite des Internet-Anschlusses.

Zugang über dienstliches **Notebook - Vollzugriff** (**IPSec**-VPN)

Beim Vollzugriff, der nur mit einem dienstlichen Notebook/PC möglich ist, wird nach einer Verbindung mit dem Internet (ob von zu Hause, Hotel, …) über eine spezielle Anwendung (EndPointSecurity Client) eine gesicherte Verbindung ins Klinkumsnetzwerk hergestellt. Ist diese Verbindung hergestellt, können Sie nach dem Starten des Anmeldeskriptes mit dem Notebook arbeiten, als wenn Sie an Ihrem Arbeitsplatz am Klinikum wären. Lokales speichern und drucken ist unter Beachtung der Datenschutzvorgaben möglich. Spezielle Programme können auf dem Notebook installiert und von Ihnen genutzt werden. Diese Verbindung benötigt eine hohe Bandbreite Ihres Internet-Anschlusses.

In beiden Fällen ist ein Kennwort erforderlich, welches über ein Kennwortgenerator (Mini Token) jeweils zur Anmeldung von Ihnen erzeugt wird.

Was ist VPN?

Die Kommunikationstechnik VPN (Virtual Private Network) dient zur Anbindung von PCs im mobilen Einsatz an das Unternehmensnetzwerk. Kernstück jeder VPN-Lösung ist die Möglichkeit, geschützte, private Kommunikation über unsichere Netze (Internet, WLAN) betreiben zu können.

Deshalb werden die Informationen in einem VPN mit Hilfe von verschlüsselten Datenpaketen in einem Tunnel übertragen. Durch das sog. "Tunneling" können sich beispielsweise Ärzte in Hintergrundbereitschaft in das zentrale Klinikumsnetzwerk einwählen und innerhalb des schützenden Tunnels entsprechend definierter Zugriffsberechtigungen auf Patientendaten zugreifen.

Die Einwahl über VPN erfolgt meistens in zwei Schritten:

► Im ersten Schritt wird eine Verbindung (Modem, ISDN, DSL, WLAN, etc.) zu einem Provider hergestellt.

► Im zweiten Schritt erfolgt der Aufbau des VPN-Tunnels zum Klinikumsnetzwerk.

Wie sicher ist eine Verbindung mit VPN?

Die Sicherheitsanforderungen des Klinikums werden durch den Aufbau eines Tunnels und das Verschlüsseln der Daten gewährleistet. Das Transportprotokoll IPSec bzw. SSL verhindert das Ausspionieren oder Manipulieren der Daten während der Verbindung über das Internet.
Als zusätzlicher Schutz wird zur Anmeldung neben den persönlichen Windows Anmeldedaten ein persönlicher Schlüssel (Token) für die Authentifizierung am Klinikumsnetz verwendet.

Erst nach erfolgreicher Authentisierung wird ein VPN Tunnel aufgebaut. Sie erhalten in diesem Zusammenhang eine persönliche PIN. **Bitte beachten Sie, dass Sie diese PIN zukünftig für jeden VPN-Verbindungsaufbau benötigen. Daher sollten Sie sich diese gut merken.**

Nach erfolgreicher Authentifizierung ist der so genannte VPN Tunnel aktiv und Sie können auf die Ihnen zugeteilten Ressourcen am Klinikum zugreifen.

Bei einer ungültigen Eingabe findet keine Authentifikation statt und der Zugriff auf die Ressourcen des Klinikums wird verweigert

Besondere Verantwortung des Anwenders

Die Sicherheit der einzelnen Kommunikationsverbindung, wie auch die Sicherheit innerhalb des gesamten Netzwerkes hängen von einem sorgfältigen und verantwortungsbewussten Umgang mit dem Token und der dazugehörenden PIN ab.

Achten Sie bitte auf den Token so, als wenn es sich dabei um Bargeld handeln würde und schützen Sie Ihre PIN in gleicher Weise, wie Sie die PIN Ihrer EC-Karte schützen. Mit beiden können unberechtigte Personen erheblichen Schaden verursachen und die Vertraulichkeit der uns von Patienten überlassenen Informationen gefährden.

Jeder Anwender muss sich daher der besonderen Bedeutung und seiner persönlichen Verantwortung bei der Nutzung dieses Verfahrens bewusst sein und besondere Sorgfalt walten lassen.