

Wenn vollständig ausgefüllt:

per E-Mail: vpn-antrag@charite.de

Nur von einer Charité-Absenderadresse aus!

VPN-Antrag (Mitarbeitende, Studierende)

Achtung: Für E-Mail-Abruf ist VPN nicht erforderlich, <https://email.charite.de> ist auch ohne VPN erreichbar!

Standard-Berechtigungen

Beschreibung: Zugriff auf die Standard-Berechtigungen **Internet-Proxy** (Zugriff auf Online-Zeitschriften und e-Books) und **Intranet** (ausgewählte Systeme im Intranet, z.B. E-Mail, intranet.charite.de, info.charite.de, Laborbuch, QM-Handbuch, FACT, Drittmittelanzeige, lizenzierte Software, z.B. **SPSS** u.a.).

Die Freigabe dieser Berechtigungen bedarf **keiner** Zustimmung.

Erweiterte Berechtigungen

Erweiterte Berechtigungen können für Mitarbeitende und Studierende (nur mit Arbeitsvertrag der Charité!) eingerichtet werden. Erweiterte Berechtigungen sind mit gesondertem Formular zu beantragen. Die Freigabe der erweiterten Berechtigungen bedarf der Zustimmung der Leitung der Einrichtung oder der Charité-Leitung; siehe Intranet, https://intranet.charite.de/it/it_serviceueberblick/vpn/vpn_antrag

Verpflichtungserklärung und Unterschrift

Die Nutzung der Berechtigung darf nur durch den*die Antragsteller*in selbst erfolgen; ein Zugriff durch Dritte darf nicht möglich sein. Die einschlägigen rechtlichen Bestimmungen zum Datenschutz sind einzuhalten. Insbesondere werden die aus dem Bereich der Charité erlangten Informationen - gleich welcher Art - streng vertraulich behandelt, nicht an Dritte weitergegeben oder in sonstiger Weise verwertet. Die Verwendung, Verwertung, Weitergabe oder unbefugte Aufzeichnung von Geschäfts- und Betriebsgeheimnissen der Charité ist untersagt.

Es darf ausschließlich auf die oben beantragten IT-Systeme zugegriffen werden. Verbindungsversuche zu anderen als den freigegebenen IT-Systemen sind zu unterlassen. Der Charité behält sich vor, alle Zugriffe zu protokollieren und diese Protokolle regelmäßig auszuwerten.

Es wird zugesichert, dass die für den VPN-Zugriff verwendeten Geräte dem aktuellen Stand der Technik (Betriebssystemversion) entsprechen und durch geeignete Mittel (Schutzprogramme) frei von Schadsoftware (Viren, Trojaner etc.) sind. Passwort und Zertifikat sind sicher zu verwahren und nicht an Dritte weiterzugeben. Verlust von Passwort oder Zertifikat sind unverzüglich dem GB IT zu melden.

Die Nutzung des VPN-Zugriffs in öffentlicher und damit nicht sicherer Umgebung (z.B. Gaststätten, Wartebereiche, Verkehrsmittel) ist wegen der Möglichkeit der Kenntnisnahme von Daten durch unbefugte Dritte untersagt.

Der*Die Antragsteller*in ist einverstanden, dass seine*ihre persönlichen Daten zur Verwaltung des Zugangs zweckgebunden gespeichert werden.

☐ Ich akzeptiere die aufgeführten Regelungen und verpflichte mich, den VPN-Zugang nur gemäß den Regelungen zu verwenden.

Datum, Unterschrift Antragsteller*in: