Formularinhalte löschen

Universität Rostock IT- und Medienzentrum	**Erweiterungsantrag für einen Zugang zum Verwaltungsnetzwerk** Stand: 20.12.2024	**Universitäts-Nutzerkennzeichen**

Leiter/in (Antragsteller/in)	**Nutzer/in** (Mitantragsteller/in)
✘ Name, Vorname	✘ Name, Vorname
✘ Dezernat / Referat bzw. Einrichtung allg.	✘ Dezernat / Referat bzw. Einrichtung allg.
Telefon	Telefon
✘ ☐ Nein ☒ Ja, bis zum: Befristung des Arbeitsvertrages	✘ E-Mail-Adresse
✘ ☐ Mitarbeiter/in ☐ Wiss./stud. Hilfskraft ☐ Praktikant/in / RIA Status	Ja: ☐ Nein: ☒ Antrag für ein Token zum externen Zugriff

Zugriffsrechte für HIS-Systeme

☐ FSV ☐ SVA

Zugriffsrechte auf das Gruppenlaufwerk K:

Verzeichnis	Leseberechtigung	Schreibberechtigung
	☐	☐
	☐	☐
	☐	☐
	☐	☐
	☐	☐

Ort	✘ Stempel der Einrichtung
✘ Datum 16.01.2025	

✘ Unterschrift Antragsteller/in	✘ Unterschrift Mitantragsteller/in bzw. Nutzer/in

Genehmigungsvermerk IT- und Medienzentrum

Hinweise/Auflagen:

Genehmigt: _____

✘ Bitte unbedingt ausfüllen

Unterschrieben und als Scan per **E-Mail** an: **itservice.zv@uni-rostock.de**

IT-Sicherheitsempfehlungen für die Tätigkeit im „Homeoffice“

Unter dem Begriff „Homeoffice“ werden alle Arbeitsformen (u. a. mobiles Arbeiten, Telearbeit) adressiert, bei denen Mitglieder der Universität Rostock (UR) ihre dienstlichen Tätigkeiten nicht in den Gebäuden der UR, sondern bspw. in ihren privaten Räumlichkeiten verrichten.

Mit dem Homeoffice-Arbeitsplatz kann über das Internet ein Zugang zur internen IT-Infrastruktur der UR hergestellt werden.

Um einen gesicherten Informationsfluss zu gewährleisten und um vor Informationssicherheitsrisiken (Verlust der Vertraulichkeit, Verfügbarkeit und Integrität) bestmöglich geschützt zu sein, müssen die nachfolgenden Regelungen eingehalten werden:

1. Halten Sie die Soft- und Hardware (bspw. Betriebssystem oder Office-Anwendungen) Ihres dienstlichen bzw. privaten Endgerätes (Notebook, PC, Tablet o. ä.) immer auf dem neusten Stand.
2. Verwenden Sie ein Antivirenprogramm und eine Firewall.
3. Benutzen Sie zur Authentifizierung bzw. Anmeldung am Endgerät immer einen Benutzernamen und ein Passwort.
4. Die Ihnen zugewiesenen Anmeldedaten für die technische IT-Infrastruktur der UR (bestehend aus Nutzerkennzeichen und Passwort) sind auf Sie personalisiert und dürfen nicht an andere Personen weitergeben werden.
5. Nutzen Sie unterschiedliche Passwörter und verwenden Sie private Passwörter nicht im dienstlichen Zusammenhang
6. Stellen Sie den Bildschirm bzw. das Endgerät so auf, dass nur Sie die Inhalte auf dem Bildschirm lesen können.
7. Während Sie das Endgerät nicht benutzen, verhindern Sie durch eine Sperrung bzw. eine Abmeldung, dass unbefugte Personen auf Ihr Endgerät und somit auf Informationen widerrechtlich zugreifen können.
8. Schützen Sie Ihr Endgerät vor Beschädigung, Verlust und Diebstahl. Lassen sie insbesondere mobile Geräte nicht unbeobachtet liegen – auch nicht kurzzeitig.
9. Speichern Sie Ihre Daten regelmäßig und nur auf den dafür vorgesehenen Netzlaufwerken (bspw. Home-Laufwerk). Speichen Sie keine Daten lokal bzw. direkt auf ihrem privaten Endgerät.
10. Erstellen Sie regelmäßig eine Datensicherung. Für das Home-Laufwerk und Netzlaufwerke, die vom ITMZ eingerichtet wurden, erfolgt dies automatisch.
11. Öffnen Sie eingehende E-Mails und ggf. darin enthaltene Dateianhänge oder Links niemals unbedacht. Das Risiko einer Infizierung mittels Schadsoftware oder das Ausspähen von Anmeldedaten wird hierdurch minimiert. Antivirenprogramme können nicht in jedem Fall vor einem Schaden durch boshafte E-Mails o. ä. schützen. Hier ist Ihre besondere Achtsamkeit sehr wichtig.
12. Nutzen Sie elektronische Zertifikate für einen sicheren (verschlüsselten) E-Mailtransport bei der Übertragung von vertraulichen bzw. personenbezogenen Daten.
13. Laden Sie dienstliche Dateien bei Bedarf nicht in frei verfügbare Cloud-Systeme (wie bspw. Google Drive od. Dropbox), sondern nutzen Sie das durch die UR bereitgestellte SharePoint oder alternativ die Unibox.
14. Wählen Sie bei Telefonaten oder Videokonferenzen mit vertraulichem Inhalt Ihren Aufenthaltsort so aus, dass Unbefugte das Gespräch nicht mithören können.
15. Betreiben Sie Ihr Endgerät nur mittels mitgeliefertem Stromversorgungsadapter.
16. Bewahren Sie Ihr Endgerät, Ihre Akten und Ihre mobilen Datenträger stets an einem sicheren (verschlossenen) Ort auf.
17. Nutzen Sie, wenn erforderlich, nur verschlüsselte mobile Datenträger (bspw. Festplatten, USB-Sticks).
18. Melden Sie IT-Probleme oder IT-Vorkommnisse in jedem Fall und schnellstmöglich an den für Sie zuständigen IT-Verantwortlichen oder alternativ an die Stabsstelle für Datenschutz und Informationssicherheit.
19. Halten Sie stets die Lizenzbestimmungen bei der durch Sie genutzten Software ein.
20. Beachten Sie die universitär gültigen Bestimmungen zum Datenschutz und zur IT-Sicherheit.

✘ Datum und Unterschrift Nutzer/in zur Kenntisnahme

IT- und Medienzentrum, A. Zeitz