

Nutzung privater Endgeräte am Hochschuldatennetz

Den Antrag bitte **vollständig** auf der Vorder- und **Rückseite** und möglichst in Druckbuchstaben ausfüllen.

1) Informationen zum Nutzer/Gerät

Name, Vorname des Nutzers		
Kontaktdaten	Telefon:	Mail:
Aufstellungsort	Raum:	Dose:
Art und Einsatz des Geräts	<input type="checkbox"/> Laptop <input type="checkbox"/> Standgerät <input type="checkbox"/> Arbeitsplatz/Client	
MAC (TP/Wireless)		
Betriebssystem		
Zweck des Einsatzes/Nutzungsdauer		
Systemverantwortlicher		

Zugewiesene IP	
System durch Netzverantwortlichen überprüft?	Datum, Unterschrift NV
Nutzer über lokale/uniweite Regelungen informiert	Datum, Unterschrift NV

2) Kostenübernahme bei Einsatz kostenpflichtiger Software

Auftraggeber Vorstand/Leiter/Direktor	
Institut/Abteilung	
Finanzstelle	
Straße	
PLZ, Ort	

Datum:

Unterschrift des Auftraggebers / Institutsstempel

3) Bedingungen 1. Vollständigkeit der Angaben

Die unter Punkt 1) und Punkt 2) aufgeführten Angaben müssen vollständig sein. Falls sich Änderungen an den Angaben ergeben, dann ist es Aufgabe des Nutzers dies dem lokalen Netzverantwortlichen mitzuteilen. Es dürfen nur vollständig erfasste Endgeräte ans Datennetz angeschlossen werden.

2. Benutzungsordnungen

Der Benutzer erklärt hiermit, dass er die Benutzungsordnungen für Informationsverarbeitungssysteme der Universität Würzburg und für das Hochschulnetz der Universität Würzburg und die Richtlinien zum Betrieb und Aufbau WWW-basierter Informationssysteme an der Universität Würzburg in der jeweils gültigen Fassung anerkennt. Diese Bedingungen, Benutzungsordnungen und Richtlinien können von den Seiten des Rechenzentrums unter http://www.rz.uni-wuerzburg.de/infos/benutzungsordnung_und_konzepte/ eingesehen werden. Kommerzielle Tätigkeiten sind gemäß diesen Bedingungen untersagt.

Der Benutzer erklärt des weiteren, dass er (falls vorhanden) lokale, weiterführende Regelungen anerkennt. Diese können über den lokalen Netzverantwortlichen bzw. IT-Bereichsmanager bezogen werden.

3. Sicherer Betrieb des Endgeräts

Der Nutzer (bzw. der Systemverantwortliche) ist für den sicheren Betrieb des Endgeräts verantwortlich. Hierzu gehört die Einrichtung automatischer Online-Updates für Betriebssystem und Applikationen, Installation eines geeigneten AntiVirus-Programms mit regelmäßigen Updates und je nach Bedarf einer persönlichen Firewall. Die getroffenen Einstellungen sind periodisch vom Nutzer (bzw. Systemverantwortlichen) zu überprüfen um eventuelle Fehlerzustände in diesen kritischen Bereichen zu erkennen.

Unnötige Netzdienste sind zu deaktivieren, nicht benötigte Netzprotokolle (insbesondere IPv6, Netzwerkbrücken zwischen verschiedenen Netzschnittstellen) sind zu deaktivieren.

Der Zugang zum Gerät ist durch geeignete Maßnahmen (z.B. Passwort) zu schützen.

Es ist Aufgabe des Netzverantwortlichen, die genannten grundsätzlichen Einstellungen initial zu kontrollieren. Dem Netzverantwortlichen muss hierzu (im Beisein des Nutzers) der Zugriff auf das Endgerät ermöglicht werden. Änderungen an diesen Einstellungen dürfen nur in Absprache mit dem Netzverantwortlichen vorgenommen werden.

Im Fehlerfall kann die Zugangsberechtigung durch den Netzverantwortlichen bzw. IT-Bereichsmanager bis zur Behebung widerrufen werden.

4. Haftung und Datensicherheit

Der Benutzer wird darauf hingewiesen, dass die Hochschule bzw. der lokale Bereich für die Sicherheit der Daten auf dem Endgerät (Zerstörung, Diebstahl, Manipulation etc.) keine Haftung übernimmt. Es liegt in der Verantwortung des Nutzers geeignete Maßnahmen (z.B. Backups, Sicherung auf Netzlaufwerke, Abschließen des Raumes) zu ergreifen.

5. Schutzwürdige Daten

Der Benutzer verpflichtet sich, keine personenbezogenen oder sonst schutzwürdigen Daten zu verarbeiten und die jeweils geltenden datenschutzrechtlichen Bestimmungen zu beachten.

6. Lizenzpflichtige Software

Bei Einsatz lizenzpflichtiger Software sind die Lizenzbedingungen durch den Nutzer einzuhalten. Insbesondere bei mobilen Endgeräten stellt sich dabei die Problematik, dass Lizenzbedingungen verschiedener Hersteller explizit zwischen „Home“- und „Office“-Einsatz (evtl. mit Ausnahmen für „Lehre und Forschung“) unterscheiden. Es ist Aufgabe des Nutzers zu überprüfen, ob eine spezielle Softwarelizenz den gewünschten Einsatz abdeckt und bei Bedarf zusätzliche Lizenzen über seinen Bereich zu beantragen.

Bei der Nutzung des zentralen Softwareangebots des RZ (Applikationen im Novellnetz, Software aus dem Webshop) können Kosten anfallen. Falls für Softwarelizenzen Kosten entstehen, so sind diese durch den Bereich zu tragen.

Bei Entfallen der Nutzungsgrundlage ist die im Rahmen der Nutzung installierte Software entsprechend der jeweils gültigen Lizenzbestimmungen zu deinstallieren. Dienstlich erworbene Softwarelizenzen verbleiben nach der Nutzung im Eigentum der Universität.

Zuwiderhandlungen können erhebliche Schadenersatzforderungen der Lizenzgeber nach sich ziehen. Die Universität wird in diesem Fall beim Benutzer Regress nehmen.

7. Urheberrecht

Der Benutzer wird darauf hingewiesen, dass kein Teil eines urheberrechtlich geschützten Werks ohne schriftliche Genehmigung des Rechteinhabers reproduziert, verarbeitet, vervielfältigt oder verbreitet werden darf. Dies gilt auch für Zwecke der Forschung oder Lehre.

8. Datenschutzklausel

Der Benutzer erklärt mit seiner Unterschrift sein Einverständnis, dass

a) die umseitig gemachten Angaben elektronisch verarbeitet (Art. 42 Abs. 4 Satz 1 und 2 BayHSchG, Art. 15 Abs. 1 Nr. 1 und 2, Art. 16 Abs. 1, Art. 17 Abs. 1 und 2 BayDG) und in der Komponentendatenbank des Rechenzentrums gespeichert werden,

b) bei der Inanspruchnahme von Diensten die erforderlichen personenbezogenen Daten (z.B. Absender- und Empfängeradresse, Versendungszeit, Nutzungszeiten) elektronisch protokolliert werden,

c) die mit der DV-Administration betrauten Mitarbeiter des Rechenzentrums oder der zuständige IT-Bereichsmanager nach Absprache mit dem Datenschutzbeauftragten der Universität

- zum Zweck der Aufrechterhaltung eines ordnungsgemäßen Rechen- und Netzwerkbetriebs (z.B. technische Verwaltung des Netzwerks, Behebung von Funktionsstörungen),

- beim Verdacht von Mißbräuchen (z.B. strafbare Informationsverbreitung oder –speicherung, Benutzung zu nicht erlaubten Zwecken) zu deren Verhinderung

Zugriff auf die Daten des Benutzers (insbes. auf die Verbindungs-Protokolldaten sowie die auf dem Endgerät gespeicherten Daten) nehmen können, sofern dies im jeweiligen Einzelfall erforderlich ist.

Ich erkläre, dass ich diese Bedingungen einhalten werde und die Datenschutzklausel (Nr. 8) gelesen und verstanden habe.

Datum

Unterschrift Benutzer/in