

Richtlinien der Informatikdienste zur Anbindung von privaten oder selbst administrierten IT-Geräten an das allgemeine universitäre Netzwerk

Versionskontrolle und Prüfstellen			
Version	Bearbeitung	Ersteller	Datum
X0100	Dokument erstellt	M. Sinzig	5. April 2005
X0104	Diverse Überarbeitungen + Ergänzungen ID-Mini, CH, rt, pm	R. Zumstein	17. Mai 2011
X0105	Ueberprüfung durch Rechtsdienst, F. Kaderli	R. Zumstein	1. Juni 2011
X0106	Ergänzungen nach Feedback von T. Braun, IAM	R. Zumstein	1. Juli 2011
V0100	Freigegebene Fassung	R. Zumstein	8. Juli 2011

Geltungsbereich	Mitarbeitende, Dozierende und Studierende der Uni Bern
Klassifikation	Für uni-internen Gebrauch
Dokumentenstatus	Freigegeben
Freigabe	Leiter ID, 8. Juli 2011

Ziel und Zweck

Der Anschluss von nicht universitätseigenen, privaten IT-Geräten oder von Geräten, welche primär durch die/den Benutzer/in selbst administriert werden, stellt ein erhöhtes Sicherheitsrisiko dar. Einerseits können solche Geräte durch Fehlkonfigurationen zu Netzwerkblockaden führen und somit den Datenverkehr bzw. die Verfügbarkeit beeinträchtigen, andererseits besteht die Gefahr, dass unkontrolliert Malware (Viren, Würmer, Trojaner, Spyware etc.) eingeschleust und verbreitet wird. Diese Richtlinie definiert die Voraussetzung für die Anbindung von privaten oder selbst administrierten Geräten an das allgemeine universitäre Netzwerk via LAN, Wireless-LAN und VPN.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeitenden, Dozierenden und Studierenden der Universität Bern, welche private oder selbst administrierte Geräte an das allgemeine universitäre Netzwerk anschliessen wollen.

Verpflichtungen und Regelungen

Die Anbindung und Integration von privaten oder selbst administrierten Geräten an das allgemeine universitäre Netzwerk bedarf verschiedener Anpassungen und untersteht diversen Verpflichtungen und Regelungen:

- Die Geräte müssen mit den aktuellsten Sicherheitsupdates (Patches) ausgerüstet sein und neue Updates/Patches müssen fortlaufend, entweder manuell oder automatisch installiert werden.
- Die Geräte müssen über einen ausreichenden und aktuellen Schutz gegen Viren, Malware, etc. verfügen sowie mit einer aktiven Firewall gegenüber ungeschützten Zugriffen aus dem Netz gesichert werden.
- Es dürfen keine Benutzeraccounts sowie Dateifreigaben ohne Passwörter (Passwörter mind. 8 Zeichen) vorhanden sein.
- Die kabelgebundene Integration der Geräte in das universitäre Netzwerk hat nur durch die/den zuständige/n IT-Verantwortliche/n oder in den durch die Informatikdienste betreuten Bereichen durch diese zu erfolgen. Die Anbindung via WLAN- und VPN-Infrastruktur erfolgt durch die/den Endbenutzer/in. Universitäre Institutionen, welche kabelgebundene Integration von Geräten im Rahmen der Forschungs- und Lehrtätigkeit zulassen müssen, können dies selbständig nach Information der Informatikdienste tun. Der ordnungsgemäße Zustand des Netzwerks darf nicht beeinträchtigt werden.
- Sobald die Integration in das universitäre Netzwerk erfolgt ist, werden die Geräte einem universitätseigenen Gerät gleichgestellt. Das heisst, dass die/der Benutzer/in die entsprechenden Pflichten, Aufgaben und Zuständigkeiten für die Geräte übernimmt und sicherstellt, dass diese eingehalten und umgesetzt werden. In nicht-öffentlichen Bereichen ist die/der IT-Verantwortliche der entsprechenden Institution gehalten, die Einhaltung der bestehenden Weisungen zu überprüfen und bei Feststellen von Verstössen Massnahmen einzuleiten.
- Falls auf solchen Geräten Software der Universität Bern installiert wird, ist die/der Benutzer/in verantwortlich, dass die Software korrekt lizenziert ist und dass diese nach ihrem/seinem Ausscheiden aus der Universität Bern wieder deinstalliert wird. Nach dem Austritt ist eine Weiterbenutzung der Software ausserhalb der Universität Bern nicht erlaubt.
- Daten der Universität Bern, welche als schützenswert oder besonders schützenswert einzustufen sind, dürfen nicht auf den privaten bzw. selbst administrierten Geräten abgelegt werden.
- Nach dem kabelgebundenen Anschluss der privaten oder selbst administrierten Geräte an das universitäre Netzwerk muss der WLAN-Empfang ausgeschaltet werden. Das Gerät darf zudem nicht zeitgleich mit mehreren Netzen (z.B. Uni- und privatem Netz) verbunden sein und die Routing-Funktionalität über mehrere Netze (z.B. Internetsharing) darf nicht aktiviert werden. Universitäre Institutionen, welche im Rahmen der Forschungs- und Lehrtätigkeit Routing- oder Multi-Homing-Funktionalität ermöglichen, können dies nach Information der Informatikdienste tun. Der ordnungsgemäße Zustand des Netzwerks darf nicht beeinträchtigt werden.

Des Weiteren gelten die Weisungen, Beschlüsse und Richtlinien der Universität Bern, insbesondere die "Weisungen der Universitätsleitung über die Benutzung der IT-Ressourcen an der Universität Bern", die "Weisungen der Universitätsleitung über das Netzwerk der Universität Bern" sowie die „Richtlinien zum Datenschutz im IT-Bereich“. Allenfalls vorhandene weitere Weisungen und Richtlinien in den Bereichen sind ebenfalls bindend.

Informatikdienste der Universität Bern
Bern, 8. Juli 2011

Leiter Informatikdienste