Universität Bielefeld	**IT-Sicherheitsrichtlinie für Telearbeitsplätze**
Art: IT-Sicherheitsrichtlinie	Version: 1.0
Verfassende: Michael Sundermeyer	Freigabedatum: 10.06.2008
Zielgruppe: Beschäftigte	Letzte Änderung: 09.06.2008

1. Geltungsbereich

Diese Richtlinie ist für alle Beschäftigten der Universität, die im Rahmen der „Dienstvereinbarung zur alternierenden Telearbeit an der Universität Bielefeld“ (§ 9 DV Telearbeit) Telearbeit nutzen, verbindlich.

2. Allgemeines

Der Telearbeitsplatz darf nur durch autorisierte Beschäftigte der Universität Bielefeld genutzt werden. Die IT-Ausstattung des Telearbeitsplatzes wird von der Dienststelle gestellt, alle Hard- und Softwarekomponenten müssen durch diese freigegeben werden. Die technische Administration der IT-Ausstattung erfolgt ausschließlich durch das IT-Personal der Dienststelle.

Eine Deaktivierung oder Umgehung von Sicherheitsmechanismen, insbesondere von Sicherheitssoftware wie Virenscanner oder Firewall ist, ebenso wie die eigenmächtige Installation von Fremdsoftware auf dem Telearbeitsplatz, nicht gestattet. Bitte beachten Sie die Regelungen der Universität Bielefeld zur Nutzung von Passwörtern[1]. Eine Weitergabe von Passwörtern ist untersagt.

Ein Zugang zum „Intranet“ der Universität Bielefeld erfolgt ausschließlich über eine gesicherte, kabelgebundene VPN-Verbindung zwischen dem Telearbeitsplatz der Beschäftigten und der Dienststelle. Die Nutzung anderer Zugangswege (Wireless LAN, separater DSL-Zugang etc.), ist nicht gestattet.

3. Handhabung von Informationen

Dienstfremden Personen darf kein Zugriff auf dienstliche schriftliche oder elektronische Informationen gewährt werden. Dies ist insbesondere bei einer Unterbrechung oder Beendigung der Arbeit durch Sperrung des Arbeitsplatzes bzw. Verwahrung des Schriftgutes in verschlossenen Behältnissen sicherzustellen.

Die Ablage von Daten hat grundsätzlich auf dem jeweiligen zentralen Speicher („Gruppenlaufwerk“) zu erfolgen („führender“ Speicherort). Eine lokale Speicherung von Daten-Kopien ist nur in einem verschlüsselten Speicherbereich der Festplatte gestattet. Dies gilt insbesondere für vertrauliche oder personenbezogene Daten. Daten-Kopien die lokal bearbeitet werden, sind schnellstmöglich wieder auf dem zentralen Speicher abzulegen. Ist dies aus technischen Gründen nicht über die VPN-Verbindung mit dem Universitätsnetzwerk möglich, sind die Informationen mit Hilfe der IT-Ausstattung (Laptop) vor Ort auf den zentralen Speicher zu übertragen.

Nicht mehr benötigte Daten sind zu löschen. Datenträger, die nicht mehr benötigt werden, sind ausschließlich in der Dienststelle durch hierfür geeignete Verfahren zu vernichten. Vertrauliche Ausdrucke sind in der Dienststelle oder vor Ort durch einen geeigneten Aktenvernichter zu entsorgen.

[1] Dienstanweisung Datenschutz und Datensicherheit beim Einsatz von DV-Anlagen und –Geräten in der Verwaltung vom 28.04.2004

Der Datentransport bzw. die Datenübermittlungen zwischen Telearbeitsplatz und Dienststelle haben nur in verschlüsselter Form zu erfolgen. Dies gilt sowohl für einen Datenaustausch per VPN als auch für den physischen Datenaustausch per Speichermedium.

4. Ausnahmen

Ausnahmen von diesen Regelungen sind schriftlich im Personaldezernat zu beantragen.

5. Ansprechpartner

Bei technischen Problemen des Telearbeitsplatzes, setzen Sie sich bitte mit Ihrer zuständigen EDV/IT-Administration in Verbindung. Bei Fragen zu dieser Richtlinie und zur IT-Sicherheit wenden Sie sich an den IT-Sicherheitsbeauftragte unter der Durchwahl -67052 und per E-Mail unter it-sicherheit@uni-bielefeld.de.

6. Konsequenzen bei Zuwiderhandlung

Im Falle der Zuwiderhandlung gegen Pflichten zum Datenschutz und Datensicherheit gemäß § 9 Abs. 9 DV Telearbeit, kann das Teledienstarbeitsverhältnis mit sofortiger Wirkung beendet werden.

7. Revision

Diese Richtlinie wird regelmäßig, jedoch mindestens einmal pro Jahr, durch den oder die IT-Sicherheitsbeauftragte/n auf Ihre Aktualität und Konformität mit der DV Telearbeit und den Regelungen zur IT-Sicherheit der Universität Bielefeld überprüft.