FH Bielefeld - Verkündungsblatt 2010- 8 – Seite 117-122

Fachhochschule Bielefeld
University of Applied Sciences

Richtlinie für PC-Arbeitsplätze in der Hochschulverwaltung sowie für externe PC-Arbeitsplätze in der Hochschulverwaltung

1. Zweck und Geltungsbereich dieser Richtlinie

Zweck dieser Richtlinie ist es, durch organisatorische Regeln im Umgang mit dem PC-Arbeitsplatz dazu beizutragen, die Daten- und Systemsicherheit zu gewährleisten (§ 10 Datenschutzgesetz Nordrhein-Westfalen - DSG NRW).

Diese Richtlinie gilt für
Rechner-Arbeitsplätze im Zuständigkeitsbereich der Datenverarbeitung Hochschulverwaltung sowie für
externe Rechner-Arbeitsplätze mit Zugriff auf das Verwaltungsnetz der Hochschulverwaltung.

2. Begriffsbestimmungen

Datenschutz:
Organisatorische und technische Maßnahmen zur Verhinderung von Missbrauch bei der Verarbeitung von personenbezogenen Daten (Schutz der Information).

Datensicherung:
Organisatorische und technische Maßnahmen zur Verhinderung von Beschädigung, Zerstörung, Verlust, Veruntreuung und Fehlleitung von Daten (physischer Schutz von Daten).

Schutzwürdige Daten
im Sinne der Arbeitsplatzordnung sind personenbezogene Daten, betriebssensitive Sachdaten sowie Dateien erheblichen Umfanges bzw. besonderer Qualität.

Personenbezogene Daten
im Sinne des DSG NRW sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (betroffene Person).

Betriebssensitive Sachdaten
sind Daten, die aus Gründen der Betriebssicherheit und der betriebsinternen Geheimhaltung nur bestimmten Stellen und Personen zugänglich gemacht werden sollen.

Daten erheblichen Umfangs bzw. besonderer Qualität
sind z. B. Datenbanken, Dokumente, Tabellen, Listen und Grafiken, deren Neuerstellung nach endgültigem Verlust unmöglich oder mit einem erheblichen Aufwand verbunden ist.

Mobile Datenträger
sind USB-Sticks, CDs, DVDs, Disketten, externe Festplatten u. ä.

Datenverarbeitung
umfasst begrifflich das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie das Nutzen von Daten.

Verantwortliche Stelle
Verantwortliche Stelle ist die Stelle/Person, die schutzwürdige Daten in eigener Verantwortung selbst verarbeitet oder in ihrem Auftrag von einer anderen Stelle verarbeiten lässt.

3. Grundsätze

Es dürfen nur zugelassene und vom Systembetreuer installierte Hardware- und Softwarekomponenten verwendet werden. Die Nutzung privater Geräte sowie die Installation und Nutzung selbst beschaffter Software ist unzulässig (z. B. kein Herunterladen von Programmen aus dem Internet).
Weder dienstliche noch private mobile Rechner dürfen an das Netzwerk angeschlossen werden.

Personenbezogene Daten und betriebssensitive Daten dürfen nur zu dienstlichen Zwecken verarbeitet werden. Die Verantwortung liegt bei der jeweiligen verantwortlichen Stelle/Person.

Jede Weitergabe von Programmen an Dritte ist nur zulässig, wenn durch die verantwortliche Stelle die Rechtmäßigkeit der Weitergabe geprüft worden ist. Der Zugriff auf die Betriebssystemebene ist nur auf besondere Weisung erlaubt.

Ortsveränderungen der Geräte und physikalische Veränderungen an den Geräten sind untersagt.

Dienstliche Daten dürfen auf der lokalen Festplatte nur nach vorheriger Absprache mit dem Systembetreuer bzw. der Systembetreuerin gespeichert werden, da lokale Festplatten nicht von der regelmäßigen automatischen Datensicherung erfasst werden.

4. Informationspflichten

Unerwartetes Systemverhalten, ungewöhnliche Ereignisse sowie jeder Datenverlust mit unbekannter Ursache sind dem Systemadministrator umgehend zu melden.

5. Zugangskontrolle / Umgang mit Passwörtern

Bei Verarbeitung von personenbezogenen Daten ist zu verhindern, dass Unbefugte Einblick in die laufende Datenverarbeitung haben.

Das persönliche Kennwort (Passwort) bestimmt der Nutzer selbst. Es darf keine Rückschlüsse auf seinen Besitzer zulassen. Einfache Passworte sowie solche mit persönlichem Bezug sind zu vermeiden. Passworte sind geheimzuhalten und dürfen unter keinen Umständen weitergegeben werden.

Die Mindestlänge des Passwortes soll sieben Zeichen betragen.
Kann nicht ausgeschlossen werden, dass ein Unbefugter Kenntnis erlangt hat, z. B. durch Einblick bei der Eingabe des Passwortes, so ist das Passwort unverzüglich zu ändern.

Passwörter, die Zugang zu dem System der Fachhochschule Bielefeld gewähren, dürfen nicht auf dem Rechner gespeichert werden.

Die Überlassung des eigenen Zugangs durch Einloggen des Zugang-Inhabers und anschließendes unbeaufsichtigtes Überlassen des Rechners an Dritte (z. B. Auszubildende, Praktikanten, Aushilfen) ist untersagt.

6. Verlassen des Arbeitsplatzes

Beim Verlassen des Arbeitsplatzes ist der passwortgeschützte Bildschirmschoner zu aktivieren.

Aus Sicherheitsgründen ist der passwortgeschützte Bildschirmschoner so einzustellen, dass er sich nach einer an den jeweiligen Arbeitsplatz sinnvoll angepassten Anzahl von Minuten aktiviert (5 bis maximal 10 Minuten).

7. Mobile Datenträger

Personenbezogene Daten und betriebssensitive Sachdaten, die auf mobilen Datenträgern abgelegt werden, sind zu verschlüsseln.

Mobile Datenträger sind vom berechtigten Nutzer stets diebstahlsicher zu verwahren. Sollte ein mobiler Datenträger abhanden gekommen sein, ist die/der Vorgesetzte unverzüglich zu informieren.

Personenbezogene Daten und betriebssensitive Daten sind von mobilen Datenträgern sicher zu löschen, sobald sie nicht mehr benötigt werden.

8. E-Mail-Kommunikation

Personenbezogene Daten und betriebssensitive Daten sind grundsätzlich verschlüsselt per E-Mail zu versenden.

Innerhalb der Hochschulverwaltung können E-Mails unverschlüsselt versandt werden, da diese auf ihrem Weg vom Sender zum Empfänger das interne System nicht verlassen; dies gilt nur für Adressen, die im Novell Groupwise Adressbuch verzeichnet sind und an folgendem Adressaufbau zu erkennen sind: NAME@zv.fh-bielefeld.de.

Bei voraussehbarer Abwesenheit der Nutzerin/des Nutzers ist eine automatische Rückantwort mit Abwesenheitsmitteilung und ggf. E-Mail-Adresse der Vertreterin / des Vertreters zu aktivieren. Die Liste zur Unterdrückung von Abwesenheitsmitteilungen ist individuell zu pflegen und aktuell zu halten.

Für personenbasierte E-Mail-Adressen (z. B.: vorname.nachname@fh-bielefeld.de) gilt: Eine generelle automatische Weiterleitung aller E-Mails ist grundsätzlich nicht gestattet.

Für rollenbasierte E-Mail-Adressen (z. B.: poststelle@fh-bielefeld.de) gilt:
Eine generelle automatische Weiterleitung aller E-Mails ist zulässig, da der Absender in diesen Fällen nicht davon ausgehen kann, dass er seine E-Mail an eine bestimmte Person richtet.

9. Datenübermittlung, -entnahme

Die jeweils verantwortliche Stelle hat dafür zu sorgen, dass die datenschutzrechtlichen Vorschriften eingehalten werden.

Sie ist verpflichtet, vorab die Rechtmäßigkeit einer Weitergabe oder Übermittlung zu prüfen und diese zu dokumentieren.

10. Externe Rechner

Für externe Rechner-Arbeitsplätze mit Zugriff auf das Verwaltungsnetz der Hochschulverwaltung gilt zusätzlich:

Ein Virenscanner muss installiert sein.

Ein VPN-Client wird mit konfigurierter Firewall ausgeliefert und darf nicht verändert werden. Clients dürfen nur durch berechtigte Personen und nur im zulässigen Umfang genutzt werden.

11. Verstöße

Bei Verstößen gegen diese Richtlinie führt der Vorgesetzte ein Gespräch mit dem bzw. der Beschäftigten mit dem Ziel, die Verstöße abzustellen und eine Wiederholung zu vermeiden.

12. Inkrafttreten

Diese Richtlinie tritt am Tage nach ihrer Veröffentlichung im Verkündungsblatt/Amtliche Bekanntmachungen der Fachhochschule Bielefeld in Kraft.
Ausgefertigt aufgrund des Präsidiumsbeschlusses vom 17.03.2010.

Bielefeld, den 22.03.2010

Die Präsidentin

gez. Rennen-Allhoff

Prof. Dr. B. Rennen-Allhoff