IT-Sicherheitsrichtlinie für die Nutzung

vernetzter dienstlicher Endgeräte in der Hochschulverwaltung

1. Zweck und Geltungsbereich dieser Richtlinie

Zweck dieser Richtlinie ist es, durch organisatorische und technische Maßnahmen die Informationssicherheit und den Datenschutz bei der Nutzung vernetzter dienstlicher Endgeräte (Arbeitsplatzrechner, Notebooks, Tablets, etc.) im Netzbereich der Hochschulverwaltung zu gewährleisten. Die Richtlinie ist für alle Beschäftigten in der Hochschulverwaltung der Fachhochschule Bielefeld verbindlich. Sie ergänzt und konkretisiert für den Bereich der Hochschulverwaltung die aktuell gültige IT-Nutzungsordnung, wobei diese im Falle von Unstimmigkeiten oder Widersprüchen maßgeblich ist.

2. Grundsätze

Die IT-Ausstattung jedes Arbeitsplatzes wird von der Dienststelle gestellt. Die Datenverarbeitungszentrale (DVZ) zeichnet sich dabei für Aufbau, Betrieb und Abbau der benötigten Geräte verantwortlich. Der Zugriff auf das Verwaltungsnetz darf ausschließlich über diese Geräte erfolgen. Die Nutzung anderer, insbesondere privater Geräte jedweder Art ist im Netzbereich der Hochschulverwaltung nicht gestattet.

Alle Hard- und Softwarekomponenten werden durch die DVZ freigegeben und installiert. Die Installation und Nutzung selbst beschaffter Hard- oder Softwarekomponenten ist unzulässig. Der Zugriff auf die Betriebssystemebene ist nur dem Personal der DVZ erlaubt. Ortsveränderungen und physische Veränderungen bei Arbeitsplatzrechnern werden ausschließlich von der DVZ vorgenommen.

Ein Endgerät darf nur durch Beschäftigte der Hochschulverwaltung genutzt werden. Anderen Personen ist der Zugang zu verwehren. Jede Deaktivierung oder Umgehung von Sicherheitsmechanismen ist nicht gestattet.

Jede(r) Mitarbeiter(in) muss zum Beschäftigungsbeginn eine Einweisung in die verwendeten IT-Systeme und Programme erhalten, soweit deren Anwendung (wie z.B. bei Office-Software) nicht als bekannt unterstellt werden kann. Für die Bedienung von Fachanwendungen wird vor Aufnahme der vorgesehenen Tätigkeiten eine umfassende Einweisung durch eine(n) Mitarbeiter(in) derselben Abteilung durchgeführt, der/die die notwendigen Kenntnisse bereits besitzt.
Personenbezogene und betriebssensitive Daten dürfen nur zu dienstlichen Zwecken verarbeitet werden. Die Verantwortung liegt bei der jeweiligen verantwortlichen Stelle/Person.

3. Informationspflichten

Unerwartetes Systemverhalten, ungewöhnliche Ereignisse sowie jeder Datenverlust mit unbekannter Ursache müssen der DVZ umgehend gemeldet werden.

4. Vertraulichkeit

Ein Büro ist beim Verlassen grundsätzlich abzuschließen. Beim Verlassen des Büros ist immer sicherzustellen, dass niemand anderes über ein Endgerät Zugriff erhalten kann (z.B. per Bildschirmsperre). Die Überlassung des eigenen Zugangs an Dritte (z.B. Auszubildende, Praktikanten, Aushilfen) sollte nur in Ausnahmefällen und dann ausschließlich unter permanenter, persönlicher Aufsicht erfolgen. Eine Weitergabe des persönlichen Passwortes an andere Personen, auch an Kolleginnen oder Kollegen, darf nicht erfolgen.

5. Integrität

Bei der Eingabe von Daten, vorwiegend in datenbankbasierte Systeme, ist vorher zu sicherzustellen, dass die Daten tatsächlich für das Zielsystem vorgesehen sind, sie korrekt und auch für die Art der Eingabe und Verarbeitung bestimmt sind.

6. Verfügbarkeit

Dienstlich relevante Dateien dürfen nicht lokal auf einem Endgerät, sondern müssen grundsätzlich auf einem Netzwerklaufwerk gespeichert werden. Nur so kann gewährleistet werden, dass die Daten jederzeit zur Verfügung stehen und von einer zentralen Datensicherung erfasst werden können.
Sofern die lokale Speicherung dienstlicher Daten auf einem (mobilen) Endgerät unumgänglich erscheint, so ist das gesamte Endgerät zu verschlüsseln.

7. Datenweitergabe / Datentransport

Bei Verwendung externer Medien, wie z.B. USB-Sticks, USB-Festplatten, CD‘s, DVD’s, etc. ist dafür zu sorgen, dass keine unbefugte Person Zugriff auf die darauf gespeicherten Daten erhalten kann (z.B. durch Verschlüsselung).
Sollte es sich bei den Daten gar um datenschutzrelevante oder betriebssensitive Informationen handeln, sind die Rechtmäßigkeit, die Notwendigkeit und auch die Art der Datenübermittlung vorher mit dem bzw. der zuständigen Vorgesetzten abzuklären und entsprechende Schutzmaßnahmen vorzunehmen.

8. Verstöße

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

9. Revision

Der oder die IT-Sicherheitsbeauftragte überprüft die Richtlinie regelmäßig, jedoch mindestens einmal pro Jahr, auf ihre Aktualität und Konformität mit den IT-Sicherheitsregelungen der Fachhochschule Bielefeld und überarbeitet und kommuniziert die Anpassungen der Richtlinie gegebenenfalls.

10. Inkrafttreten

Diese Richtlinie tritt am Tage nach ihrer Veröffentlichung im Verkündungsblatt/Amtliche Bekanntmachungen der Fachhochschule Bielefeld in Kraft. Gleichzeitig wird die „Richtlinie für PC-Arbeitsplätze in der Hochschulverwaltung sowie für externe PC-Arbeitsplätze in der Hochschulverwaltung“ vom 22.03.2010 außer Kraft gesetzt.

Ausgefertigt aufgrund des Beschlusses des Präsidiums der Fachhochschule Bielefeld vom 13.01.2020.

Die Präsidentin
der Fachhochschule Bielefeld
gez. I. Schramm-Wölk

Prof. Dr. Ingeborg Schramm-Wölk

Dokumenthistorie

Datum	**Tätigkeit**	**Autor**
30.03.2018	Erster Entwurf	Hanns-J. Gerlach
30.04.2018	Überarbeitung in Abstimmung mit DVZ-Leiter & DSB	Hanns-J. Gerlach
03.06.2018	Überarbeitung in Abstimmung für P.-Vorlage	Hanns-J. Gerlach
06.08.2018	Überarbeitung nach Abstimmung mit Dezernentenrunde	Hanns-J. Gerlach
18.12.2019	Letzte Korrekturen zur Präsidiumsvorlage	Hanns-J. Gerlach