IT-Sicherheitsrichtlinie zur Nutzung von Netzlaufwerken und Cloud-Speicherdiensten an der Fachhochschule Bielefeld

1. Zweck

Diese Richtlinie beinhaltet Regelungen der Fachhochschule Bielefeld für die Nutzung von Netzlaufwerken und Cloud-Speicherdiensten. Sie soll einerseits verbindliche Handlungsanleitungen für eine dienstliche Nutzung geben und andererseits zur Sensibilisierung beitragen.

Die Nutzung nicht-kommerzieller, öffentlicher Cloud-Speicherdienste ist mit einer Reihe von Risiken verbunden. Der Speicherort, die zugreifenden Personen sowie die Zuständigkeiten in Problemfällen haben Auswirkung auf die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Insbesondere müssen Daten mit hohem oder sehr hohem Schutzbedarf hinsichtlich Informationssicherheit und Datenschutz mit besonderer Sorgfalt gehandhabt werden.

2. Geltungsbereich

Diese Richtlinie gilt verbindlich für alle Mitglieder und Angehörigen der Fachhochschule Bielefeld, bei der Speicherung und Verarbeitung von Daten im Rahmen ihrer dienstlichen Tätigkeiten.

3. Begriffsdefinitionen

Netzlaufwerke

Netzlaufwerke (oft auch als Volumes oder Netzwerkverzeichnisse bezeichnet) sind reservierte Speicherbereiche auf einem zentral betriebenen Speichersystem, welche über das Datennetz auf Computern eingebunden werden können. Netzlaufwerke, wie z.B. das Home-Verzeichnis, werden durch die Datenverarbeitungszentrale (DVZ) bereitgestellt und bieten durch eine Reihe von Vorkehrungen (Spiegelung und regelmäßige Sicherung) ein hohes Maß an Verfügbarkeit, Vertraulichkeit und Integrität.

Cloud-Speicher

Der Begriff Cloud-Speicher (auch Online Speicher, Online Storage oder Cloud Storage) beschreibt einen Speicherort, der jederzeit und von jedem Ort über ein Daten- oder Kommunikationsnetz erreichbar ist. Dort abgelegte Daten können mit verschiedensten IT-Geräten bearbeitet, synchronisiert und mit Dritten geteilt werden. Anbieter dieser Dienste gibt es sowohl im kommerziellen, als auch im öffentlichen Bereich.

4. Regelungen

4.1 Nutzung der Netzlaufwerke

Für die Speicherung und Verarbeitung von dienstlichen Daten sind grundsätzlich die Netzlaufwerke der Fachhochschule Bielefeld zu nutzen.

4.2 Nutzung von Cloud-Diensten der Hochschule

Für den mobilen Zugriff auf Dateien und deren Austausch mit anderen Personen darf grundsätzlich nur der dafür vorgesehene Dienst der Fachhochschule Bielefeld (Sciebo) genutzt werden. Die dort hinterlegten Datenmengen sind dabei auf das erforderliche Mindestmaß zu begrenzen und es ist vorab sicherzustellen, dass keine besonders schützenswerten Daten betroffen sind. Darüber hinaus ist durch eine Prüfung der vergebenen Berechtigungen zu gewährleisten, dass die Daten ausschließlich einem berechtigten Personenkreis zugänglich gemacht werden.

4.3 Nutzung der Cloud-Dienste von Partnerorganisationen

Wenn in wissenschaftlichen Projekten unter Federführung einer anderen öffentlichen Einrichtung aus Kooperationsgründen Daten auf einem anderen Cloud-Speicherdienst als dem hochschuleigenen bereitgestellt werden müssen, so ist dies unter Berücksichtigung der zuvor - unter 4.2 - angeführten Punkte ebenfalls möglich.

4.4 Keine Nutzung von Cloud-Speicherdiensten kommerzieller Anbieter

Eine Speicherung und Verarbeitung von dienstlichen Daten der Fachhochschule Bielefeld in Cloud-Speicherdiensten kommerzieller Anbieter ist aus Datenschutz- und IT-Sicherheitsgründen nicht gestattet.

5. Schutzbedarf von Daten

Aus der Feststellung des Schutzbedarfs der zur Auslagerung vorgesehenen Daten folgt zunächst, ob eine Auslagerung überhaupt zulässig ist und im Weiteren, unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf für jedes, der drei nachfolgend aufgeführten Schutzziele festzustellen:

5.3.1 Vertraulichkeit

Bei hohen Anforderungen an die Vertraulichkeit ist der Einsatz von Verschlüsselung zwingend notwendig. Dabei sollte die Verschlüsselung stets selbst vorgenommen werden, auch wenn der Betreiber des Speicher-Dienstes ein eigenes, integriertes Verschlüsselungsverfahren anbietet. Beim Einsatz eines Verschlüsselungsverfahrens muss darauf geachtet werden, dass es dem Stand der Technik entspricht, also nach aktuellen, allgemein anerkannten Regeln als sicher gilt.
Bei Daten mit sehr hohen Anforderungen an die Vertraulichkeit ist von der Ablage in einer Cloud abzusehen.

5.3.2 Integrität

Bei hohen Anforderungen an die Integrität, also die Unverfälschtheit von Daten, müssen zumeist selbst geeignete Maßnahmen zu deren Gewährleistung ergriffen werden. Mit Hilfe von Prüfsummen können beispielsweise Manipulationen an den Daten erkannt werden. Derartige Verfahren sind in der Regel bei Verschlüsselungsverfahren (s. Vertraulichkeit) bereits integriert.
Bei Daten mit sehr hohen Anforderungen an die Integrität ist von der Ablage in einer Cloud abzusehen.

5.3.3 Verfügbarkeit

Bei hohen Anforderungen an die Verfügbarkeit muss sichergestellt werden, dass der Anbieter des Cloud-Speicher-Dienstes eine entsprechend hohe Verfügbarkeit garantiert.
Bei Daten mit sehr hohen Anforderungen an die Verfügbarkeit ist von der Ablage in einer Cloud abzusehen.

5.4 Gesetzliche Löschfristen

Anbieter von Cloud-Speicher setzen normalerweise Speichertechniken zur effizienten Ausnutzung der physikalischen Speicherkapazitäten ein. Aufgrund dieser Speichertechnik können Daten oft erst nach einer gewissen Zeitspanne gelöscht werden. Grundsätzlich kann nicht ausgeschlossen werden, dass beim Absetzen des Löschbefehls die Daten für den Anwender lediglich ausgeblendet, aber nicht wirklich gelöscht werden. Daher sind Daten, die beispielsweise einer gesetzlichen Löschverpflichtung unterliegen, für die Ablage in der Cloud ungeeignet.

5.5 Dienstrechtliche Vorgaben

Insbesondere für Daten der Verwaltung (vor allen Dingen Studierenden-, Personal- und Haushaltsdaten) existieren oft detaillierte Vorschriften, wie mit diesen Daten umzugehen ist. Beispielsweise regeln verschiedene Vorschriften, dass Personalakten die Personalabteilung nicht ohne weiteres verlassen dürfen. Somit dürfen derartige Daten auch nicht auf Cloud-Speicherbereichen abgelegt werden.

5.6 Schutzbedarfsprüfung bereitzustellender Daten

Die Möglichkeit der Bereitstellung von Daten über einen Cloud-Speicherdienst hängt vom jeweiligen Schutzbedarf der Daten ab und ist durch den Bereitstellenden ggf. mit der jeweiligen Leitung des Fachbereichs, der Einrichtung oder des Dezernates abzustimmen. Für die Feststellung des Schutzbedarfes sollen die nachfolgend aufgeführten Beispiele als Anhaltspunkte dienen.

Art der Daten	typ. Schutzbedarf
Daten ohne Personenbezug aus öffentlich zugänglichen Quellen	normal
Organisatorische Daten der Fachbereiche und Einrichtungen	normal
Verträge mit Hochschulpartnern, die keine Vertraulichkeit verlangen	normal
Personenbezogene, dienstliche Daten wie z.B. Telefonnummern oder E-Mail Adressen von Beschäftigten	normal
Dienstliche Daten aus den Bereichen Verwaltung und Lehre	normal oder hoch
Gebäudedaten, die zum organisatorischen und rechtssicheren Betrieb notwendig sind	normal oder hoch
Wissenschaftliche Daten, wie z.B. Untersuchungsergebnisse oder Messprotokolle, die noch nicht publiziert wurden	normal oder hoch
Wissenschaftliche Daten, die aufgrund vertraglicher Vereinbarungen (z.B. aus Kooperationen) oder rechtlicher Anforderungen (z.B. Datenschutzbestimmungen) einen besonderen Schutzbedarf haben.	hoch oder sehr hoch
Haushaltsdaten	hoch
Studierendendaten	hoch
Personalaktendaten	sehr hoch
Gesundheitsdaten	sehr hoch

Aus dem Schutzbedarf der Daten folgt, ob und wie eine Bereitstellung zulässig ist.

Schutzbedarf	Nutzung des Cloud-Speichers „Sciebo“	Nutzung des Cloud-Speichers öffentlicher Partnerorganisationen
normal	zulässig	grundsätzlich zulässig
hoch	nur verschlüsselt zulässig	nur verschlüsselt zulässig
sehr hoch	nicht zulässig	nicht zulässig

Die Bereitstellung von Daten, die gesetzlichen Löschfristen unterliegen, ist auf Online-Speicher-Diensten generell unzulässig.
Die Nutzung kommerzieller Cloud-Speicherdienste, wie z.B. Dropbox, OneDrive, Google Drive oder iCloud ist **nicht gestattet**.

6. Verantwortlichkeiten

Die Leitungen der Fachbereiche und zentralen Einrichtungen sind verantwortlich dafür, dass diese IT-Sicherheitsrichtlinie in ihrem Bereich Anwendung findet. Verantwortlich für die freigegebenen Daten ist die/der jeweils Freigebende.

7. 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.

8. Ansprechpartner

Fragen zur IT-Sicherheit
IT-Sicherheitsbeauftragte/r it-sicherheit@fh-bielefeld.de

Fragen zum Datenschutz
Datenschutzbeauftragte/r datenschutzbeauftragte@fh-bielefeld.de

9. Inkrafttreten, Veröffentlichung

Diese IT-Sicherheitsrichtlinie wird im Verkündungsblatt der Fachhochschule Bielefeld – Amtliche Bekanntmachungen – bekannt gegeben. Sie tritt einen Tag nach ihrer Veröffentlichung in Kraft.

Ausgefertigt aufgrund des Beschlusses des Präsidiums der Fachhochschule Bielefeld vom 29.04.2019.

Die Präsidentin
der Fachhochschule Bielefeld

gez. Prof. Dr. Ingeborg Schramm-Wölk

Dokumenthistorie

Datum	**Tätigkeit**	**Autor**
08.09.2016	Erster Entwurf in Anlehnung an Richtlinie der Uni-Bi	Hanns-J. Gerlach
16.03.2017	Überarbeitung in Abstimmung mit DVZ-Leiter bzgl. eines hochschuleigenen Dienstes	Hanns-J. Gerlach
29.05.2017	Inhaltliche Überarbeitung in Abstimmung mit DVZ	Hanns-J. Gerlach
29.06.2017	Inhaltliche Überarbeitung in Abstimmung mit DSB	Hanns-J. Gerlach
13.07.2017	Umarbeitung zu einer produktunabhängigen Richtlinie	Hanns-J. Gerlach
09.11.2018	Überarbeitung in Abstimmung mit DVZ-Leiter bzgl. eines hochschulübergreifenden Dienstes (Sciebo)	Hanns-J. Gerlach
04.04.2018	Letzte Korrekturen zur Präsidiumsvorlage	Hanns-J. Gerlach