Universität Bielefeld

IT-Sicherheitsrichtlinie zur Nutzung von Netzlaufwerken und Cloud-Speicher-Diensten

Referenznummer	IT-SEC RL009
Titel	IT-Sicherheitsrichtlinie zur Nutzung von Netzlaufwerken und Cloud-Speicher-Diensten
Zielgruppe	Mitarbeiterinnen und Mitarbeiter, IT-Personal
Version	1.0
Status des Dokuments	Verabschiedet
Gültig seit	13.11.2015
Letzte Änderung	23.10.2015
Nächste Revision	14.11.2016
Autorinnen und Autoren des Dokuments	IT-Sicherheitsbeauftragter (Michael Sundermeyer) Mitglieder des Sicherheitsmanagement-Teams (SMT) Beschäftigte der Bioinformatics Resource Facility (BRF)
Verabschiedet durch	Sicherheitsmanagement-Team (SMT)
Implementiert durch	IT-Sicherheitsbeauftragter
Monitoring der Einhaltung	Bereichs-IT-Sicherheitsbeauftragte (BITS)
Kommentare	

1. Zweck

Diese Richtlinie beinhaltet verbindliche Regelungen der Universität Bielefeld für die dienstliche Nutzung von Netzlaufwerken und Cloud-Speicher-Diensten.

Die Nutzung insbesondere von öffentlichen Cloud-Speicher-Diensten ist mit einer Reihe von Risiken verbunden. Der unklare Speicherort, die unbekannte Anzahl der zugreifenden Personen sowie die ungeregelten Zuständigkeiten in Problemfällen gefährden die Vertraulichkeit, Integrität und Verfügbarkeit der Daten.

Die vorliegende Richtlinie soll einerseits verbindliche Handlungsanleitungen für eine dienstliche Nutzung von Netzlaufwerken und Cloud-Speicher-Diensten geben und andererseits zur Sensibilisierung beitragen. Denn insbesondere Daten der Universität mit hohem oder sehr hohem Schutzbedarf müssen hinsichtlich der Informationssicherheit mit besonderer Sorgfalt gehandhabt werden.

2. Begriffs-Definitionen

Netzlaufwerk	Ein Netzlaufwerk (oft auch als Volume, Heimatverzeichnis oder Home Directory bezeichnet) ist ein reservierter Speicherbereich auf einem zentral betriebenen Speichersystem, welches über das Datennetz auf einem Computer eingebunden wird. Netzlaufwerke bieten im Gegensatz zum Cloud-Speicher meist keine Möglichkeit, Daten zu synchronisieren d.h. ohne eine Verbindung zum Datennetz können die Daten nicht genutzt werden. Auch ein selbstverwaltetes Teilen von Daten mit Dritten ist nicht vorgesehen. Netzlaufwerke werden beispielsweise durch das HRZ bereitgestellt und bieten durch eine Reihe von Maßnahmen (Spiegelung und regelmäßiges Backup der Daten) einen hohen Schutz gegen Ausfall und Datenverlust.
Cloud Speicher	Der Begriff Cloud-Speicher (im englischen Cloud Storage) beschreibt die Möglichkeit, Datenspeicher unabhängig von Ort und Zeit über ein Daten- oder Kommunikationsnetz zu nutzen, den Umfang kurzfristig und dynamisch an Bedarfe anzupassen, die gespeicherten Daten mit den meisten gängigen IT-Geräten zu verarbeiten, und über verschiedene Geräte hinweg zu synchronisieren sowie selbstverwaltet mit Dritten zu teilen. Im täglichen Sprachgebrauch wird oft nur noch verkürzt von „der Cloud“ gesprochen. Beispiele für kommerziell angebotene Cloud-Speicher-Dienste sind Dropbox. OneDrive, Google Drive oder iCloud. Sciebo[1] (Abkürzung für „science box“) ist ein nicht-kommerzieller Cloud-Speicher-Dienst für Forschung und Lehre. Er basiert auf der quelloffenen Software „OwnCloud“, die ähnliche Funktionalitäten anbietet wie andere, kommerzielle Cloud-Speicher-Anbieter (zum Beispiel das Synchronisieren und Teilen von Daten). Sciebo wird gemeinsam von den Universitäten Münster, Bonn und Duisburg-Essen betrieben, von vielen Hochschulen in NRW genutzt und vom Land NRW gefördert. Die Universität Bielefeld ist Teilnehmer des Konsortiums und bietet Sciebo den Beschäftigten der Hochschule zur Nutzung für dienstliche Daten an.

[1] http://www.sciebo.de

3. Geltungsbereich

Diese Richtlinie gilt verbindlich für alle Mitglieder und Angehörige der Universität Bielefeld, wenn sie im Rahmen ihrer dienstlichen Tätigkeiten Daten auf Online Speicher-Diensten speichern und verarbeiten.

4. Verantwortlichkeiten

Die Leitungen der Fakultäten und Einrichtungen sind verantwortlich dafür, dass diese IT-Sicherheitsrichtlinie in ihrem Bereich Anwendung findet.

5. Regelungen

5.1 Netzlaufwerke der Universität nutzen

Vorrangig sind für die Speicherung und Verarbeitung von dienstlichen Daten die Netzlaufwerke der Universität Bielefeld zu nutzen. Diese werden insbesondere von den internen IT-Dienstleistern HRZ, TechFak und CeBiTec bereitgestellt. Daten, die einen sehr hohen Schutzbedarf haben, dürfen ausschließlich dort abgelegt werden. Darüber hinaus sind ggf. Regelungen der Fakultäten und Einrichtungen für die Nutzung von Netzlaufwerken zu berücksichtigen.

5.2 Nutzung von Cloud-Speicher-Diensten

Sofern Funktionalitäten benötigt werden, die über die Möglichkeiten der Netzlaufwerke hinausgehen, besteht die Option, den von der Universität Bielefeld angebotenen Cloud-Speicher-Dienst „Sciebo“ zu nutzen. Ob die Daten in der Cloud verarbeitet werden dürfen, hängt jedoch von ihrem Schutzbedarf ab.

Darüber hinaus ist eine Speicherung und Verarbeitung von dienstlichen Daten in Cloud-Speicher-Diensten Dritter, wie beispielsweise Dropbox, OneDrive, Google Drive oder iCloud grundsätzlich nicht gestattet.

Wenn in einem wissenschaftlichen Projekt unter Federführung einer anderen Einrichtung aus Kooperationsgründen Daten auf einem anderen Cloud-Speicher-Dienst verarbeitet werden müssen, dann gelten für diese Daten dieselben Regelungen wie für die Nutzung von „Sciebo“. Diese werden in den folgenden Abschnitten dargelegt.

5.3 Schutzbedarf der Daten bestimmt den Umfang der Cloud-Nutzung

Für die Entscheidung, ob und wie Daten in der Cloud verarbeitet und gespeichert werden können, geben die unten aufgeführten, beispielhaften Kategorien Anhaltspunkte. Sollte Unklarheit bezüglich der Schutzwürdigkeit der Daten bestehen, so ist ihr Schutzbedarf mittels einer Schutzbedarfsanalyse zu bestimmen[2].

Beispiele	**Hinweis auf typischen Schutzbedarf**
Daten ohne Personenbezug, die aus öffentlich zugänglichen Quellen stammen	normal
Regelungen der Fakultäten und Einrichtungen wie beispielsweise Umläufe	normal

[2] Eine entsprechende Vorlage kann unter http://www.uni-bielefeld.de/it-sicherheit/schutzbedarf abgerufen werden.

Verträge mit Partnern der Universität, die keine Vertraulichkeit verlangen	normal
Personenbezogene Daten wie beispielsweise private Telefonnummern oder E-Mail Adressen von Beschäftigten	normal
Dienstliche (nicht wissenschaftliche) Daten (z. B. aus den Bereichen Verwaltung und Lehre)	normal oder hoch
Wissenschaftliche Daten (z. B. Untersuchungsergebnisse, Messreihen), die noch nicht publiziert worden sind	normal oder hoch
Haushaltsdaten	hoch
Wissenschaftliche Daten, die durch vertragliche Vereinbarungen (z. B. aus Kooperationen) oder rechtliche Anforderungen (z. B. Datenschutzbestimmungen für Gesundheitsdaten) einen besonderen Schutzbedarf haben.	hoch oder sehr hoch
Studierendendaten	hoch oder sehr hoch
Personalaktendaten	sehr hoch
Gesundheitsdaten	sehr hoch

Aus dem Schutzbedarf der Daten folgt, ob ihre Speicherung und Verarbeitung in der Cloud zulässig ist:

Schutzbedarf	Nutzung des Cloud-Speicher-Dienstes „Sciebo“	Nutzung sonstiger Cloud-Speicher-Dienste
Normaler Schutzbedarf	Zulässig	Nicht zulässig
Hoher Schutzbedarf	nur verschlüsselt zulässig	Nicht zulässig
Sehr hoher Schutzbedarf	Nicht zulässig	Nicht zulässig

Fragen zur Verschlüsselung von Daten sind an die zuständigen Ansprechpersonen zu richten (siehe Abschnitt 6).

5.4 Sparsamer Umgang

Bei der Nutzung von Cloud-Speicher-Diensten sind die in Frage kommenden Datenmengen auf das notwendige Mindestmaß zu begrenzen. Der primäre Speicherplatz für Daten bleiben weiterhin die Netzlaufwerke der Universität Bielefeld.

5.5 Erst prüfen, dann übertragen

Bei der Übertragung ganzer Verzeichnisbäume in Cloud-Speicher-Dienste ist zu prüfen, ob nicht in den Unterverzeichnissen besonders schützenswerte Daten abgelegt wurden, die die Universität nicht verlassen dürfen. Darüber hinaus ist durch eine Prüfung der vergebenen Berechtigungen sicherzustellen, dass die Daten ausschließlich einem berechtigten Personenkreis zugänglich gemacht werden.

6. Ansprechpersonen

Ansprechfall	Person/Bereich	Kontakt
Fragen zur Nutzung von Netzlaufwerken und Cloud-Speicher-Diensten in den Fakultäten und Einrichtungen	EDV-Betreuung der Fakultät oder Einrichtung	Im Personen- und Einrichtungsverzeichnis unter „Ansprechpersonen“
Fragen zur Nutzung von Netzlaufwerken und Cloud-Speicher-Diensten in der zentr. Verwaltung	Service Desk des Hochschulrechenzentrums	servicedesk@uni-bielefeld.de Durchwahl: -6000
Fragen zum Datenschutz	Datenschutzbeauftragte/r	datenschutzbeauftragte@uni-bielefeld.de Durchwahl: -5229
Fragen zur IT-Sicherheit oder zu dieser Richtlinie	IT-Sicherheitsbeauftragte/r	it-sicherheit@uni-bielefeld.de Durchwahl: -3032

7. Revision

Der oder die IT-Sicherheitsbeauftragte trägt die Verantwortung für die Prüfung der Umsetzung dieser Richtlinie. Des Weiteren überprüft dieser die Richtlinie regelmäßig, jedoch mindestens einmal pro Jahr, auf ihre Aktualität und Konformität mit den IT-Sicherheitsregelungen der Universität Bielefeld und überarbeitet die Richtlinie gegebenenfalls.