Richtlinien zur Nutzung des Dienstes Sync+Share (Nextcloud)

Stand 10.10.2017

Diese Richtlinien beschreiben fachspezifische Aspekte des Betriebs und Vorgaben, die bei der Nutzung des Dienstes zu beachten sind. Sie ergänzen die Benutzungsordnung für Informationsverarbeitungssysteme der Hochschule Magdeburg-Stendal, die IT-Sicherheitsordnung für die Hochschule Magdeburg-Stendal (FH) und die Cloud-Richtlinie.

1. **Geltungsbereich und nutzungsberechtigte Personen und Einrichtungen**
   Diese Benutzungsrichtlinien gelten für den Dienst Sync+Share (Nextcloud) und die vom ZKI dafür bereitgehaltene IT-Infrastruktur.
   Nutzungsberechtigt sind Mitarbeiter, Studierende und Gäste der Hochschule Magdeburg-Stendal. Mitglieder der Hochschule haben außerdem die Möglichkeit, externe Personen zur gemeinsamen Nutzung des Diensts zusätzlich zu berechtigen. Auch für diese externen Nutzer gelten diese Richtlinien.

2. **Lesbarkeit der Daten**
   Das ZKI bemüht sich nach Kräften, mit den zur Verfügung stehenden Mitteln (z.B. Redundanz durch RAID; Spiegelung; regelmäßiges Backup usw.) die bestmöglichen technischen Voraussetzungen für eine hohe Lebensdauer und Sicherheit der Daten zu schaffen. Dazu gehören auch adäquate klimatechnische Voraussetzungen und der Gebäudeschutz.

3. **Haftung**
   Eine hundertprozentige Garantie für die unbefristete Lesbarkeit der Daten auf den Speichersystemen gibt es nicht. Weder der Hersteller der Speichersysteme bzw. der genutzten Software noch das ZKI als Dienstleister können im Fehlerfall haftbar gemacht werden. Die genannten Sicherungsmaßnahmen schaffen zuverlässige Rahmenbedingungen. Sie sind dennoch kein garantierter Schutz etwa gegen Bedienfehler. Die korrekte Anwendung und Konfiguration des Dienstes liegt in der Verantwortung des Nutzers.

4. **Verantwortung für Dateninhalte**
   Für die Rechts- und Verfassungskonformität der Inhalte der gespeicherten Daten ist alleinig der Nutzer/die Nutzerin des Dienstes verantwortlich. Der Nutzer verpflichtet sich, sensible Daten (z.B. personenbezogene Daten) nicht unverschlüsselt zu speichern und nicht unberechtigt an Dritte durch Teilen eines Bereiches weiter zu geben.
   Ein Nutzer, der Ordner für Dritte mit entsprechenden Rechten freigibt, ist als Besitzer des Ordners für die Dateninhalte verantwortlich, auch wenn diese von Dritten (externen Nutzern) stammen. Der Besitzer des Ordners ist damit auch für die Einhaltung des Urheberrechts, ob und wie Dokumente verteilt werden dürfen, verantwortlich. Es empfiehlt sich als Besitzer eines Ordners die Inhalte regelmäßig zu prüfen. Dies gilt auch in Bezug auf die Gefahr der Verteilung von Schadsoftware oder Malware-infizierter Dateien. Es wird empfohlen eine dezentrale Virenprüfung auf dem lokalen Gerät mittels einer geeigneten Antiviren Software durchzuführen. Es wird ausdrücklich darauf hingewiesen, dass eine zentrale Virenprüfung am ZKI nicht stattfindet.
   Das ZKI übernimmt keine Verantwortung bei etwaigem Missbrauch.

5. **Datensicherheit**
   Die Kommunikation zwischen den Endgeräten des Nutzers und der Dienstinfrastruktur des ZKI erfolgt verschlüsselt. Die Daten werden ausschließlich auf ZKI-eigenen Geräten in den Serverräumen des Rechenzentrums unverschlüsselt gespeichert. Das ZKI trifft angemessene Vorsichtsmaßnahmen, dass die Sicherheit und Unversehrtheit der Daten gewahrt wird. Weiterhin sorgt das ZKI mit den ihm zur Verfügung stehenden Mitteln dafür, dass kein unberechtigter Zugriff von außen auf die im Speichersystem liegenden Daten möglich ist. Die Daten werden nur dann an Dritte weitergegeben, wenn gesetzliche Verpflichtungen eingehalten werden müssen.

6. **Verfügbarkeit, Wartungszeiten**
   Das ZKI bemüht sich nach besten Kräften die höchstmögliche Verfügbarkeit des Online-Speichers sicherzustellen. Aus diesem Grund sind die wichtigsten Komponenten des Systems redundant konfiguriert. Eine jährliche Verfügbarkeit der Systeme von mindestens 99% wird angestrebt. Die Behebung von Störungen ist nur werktags zu den üblichen Geschäftszeiten garantiert. Durch geplante Wartungsarbeiten an Hard- und Software notwendige Betriebsunterbrechungen werden in den „Wartung und Störung“ (https://www.zki.hs-magdeburg.de/wartung - login erforderlich) mit mehreren Tagen Vorlauf angekündigt. In Ausnahmefällen (Notfallwartung) kann auch eine sofortige Betriebsunterbrechung angekündigt werden.

7. **Löschung von Daten**
   Die Nutzung des Dienstes bzw. die Bereitstellung der Daten ist grundsätzlich an den Account des Nutzers/der Nutzerin gekoppelt. Wird dieser Account deaktiviert oder gelöscht (z.B. beim Ausscheiden der Person), so werden die zugehörigen Dateien automatisch vom Speichersystem unwiederbringlich entfernt. Dabei kann es zu systembedingten Verzögerungen beim Löschen der Daten kommen. Sollte der Nutzer/die Nutzerin die Daten auch nach Löschung der Kennung noch benötigen, so ist er/sie selbst dafür verantwortlich, die Daten rechtzeitig auf andere Medien zu transferieren. Insbesondere haben auch externe Nutzer, die von der gelöschten bzw. deaktivierten Kennung die Berechtigung erhalten haben, keinen Zugriff mehr auf die Daten.

8. **Sperrung bzw. Einstellung des Dienstangebots**
   Das ZKI behält sich das Recht vor, die Nutzung des Sync+Share (Nextcloud)-Dienstes und damit den Zugang zu den gespeicherten Daten in Einzelfällen zu sperren. Der Dienst wird zum Beispiel gesperrt, wenn der Nutzer/die Nutzerin gegen geltendes Recht oder die hier genannten Richtlinien verstößt.

9. **Salvatorische Klausel**
   Sollten einzelne Bestimmungen dieser Richtlinie unwirksam oder undurchführbar sein oder nach Inkrafttreten unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Regelungen dieser Richtlinie im Übrigen unberührt.

10. **Schlussbestimmungen**
    Das ZKI behält sich das Recht vor, die Richtlinien zur Nutzung des Sync+Share (Nextcloud)-Dienstes zu ändern. Dies gilt insbesondere dann, wenn eine Änderung aufgrund zwingender gesetzlicher Vorschriften erforderlich wird. Es wird empfohlen, sich die jeweils aktuellen Nutzungsrichtlinien von Zeit zu Zeit erneut durchzulesen.