

# Dienstvereinbarung zu Einführung und Betrieb des Identity Management Systems mit den daran angeschlossenen Quell- und Zielsystemen

Zwischen der *TU Bergakademie Freiberg*,  
vertreten durch den Rektor sowie den Kanzler,  
und dem *Personalrat der TU Bergakademie Freiberg*,  
vertreten durch den Vorsitzenden,

wird nachfolgende Dienstvereinbarung über die Einführung und Anwendung des Identity Management Systems mit den daran angeschlossenen Quell- und Zielsystemen (nachfolgend als IDM-Gesamtsystem bezeichnet) abgeschlossen.

## **§ 1 Gegenstand und Anwendungsbereich**

- (1) Das IDM-Gesamtsystem dient der Schaffung und Verwaltung einer konsolidierten und ständig aktuellen Datenbasis für die Verwaltung von Identitäten und Berechtigungen innerhalb der TU Bergakademie Freiberg und soll die Wirksamkeit von Arbeiten der Datenerfassung und des Datenabgleichs mit den angeschlossenen Systemen erhöhen. Ein wesentlicher Bestandteil des IDM-Systems ist das Meta Directory als zentrales Datenverzeichnis.
- (2) Diese Dienstvereinbarung definiert Grundsätze für die Einführung und den Betrieb des Identity Management Systems sowie für den Anschluss von Quellsystemen, die Daten an das Identity Management System übergeben und Zielsystemen, an die Daten vom Identity Management System geliefert werden.

## **§ 2 Geltungsbereich**

- (1) Diese Dienstvereinbarung gilt für alle Einrichtungen der Universität.
- (2) Diese Dienstvereinbarung gilt für alle Beschäftigten und Auszubildenden der TU Bergakademie Freiberg.
- (3) Diese Dienstvereinbarung regelt die Bedingungen für Einführung, Betrieb und Weiterentwicklung des IDM-Gesamtsystems an der Universität. Dazu gehören das Berechtigungskonzept des Systems, die insgesamt verwendeten Datenfelder bzw. Attribute für die Speicherung, Verarbeitung und Übermittlung personenbezogener Daten.
- (4) Diese Dienstvereinbarung bezieht sich nicht auf die Einführung und den Betrieb der Systeme, die an das Identity Management System angeschlossen werden. Diese haben eigene Begründungen und Grundlagen für ihren Betrieb. Im Rahmen dieser Dienstvereinbarung werden aber Regelungen über eine Dokumentationspflicht dieser angeschlossenen Systeme und der Datenweitergabe an diese getroffen.

## **§ 3 Zielsetzung**

- (1) Ziel der Einführung des Identity Management Systems ist die Stärkung der Leistungsfähigkeit und Erhöhung der Servicefreundlichkeit der Universität

angesichts wachsender Datenmengen und zunehmender Aufgaben durch hinzukommende Anwendungen.

- (2) Der durch das Identity Management System ermöglichte Zugriff von zugelassenen Zielsystemen auf Daten, die von den Quellsystemen übernommen werden, darf nur für vereinbarte Zwecke genutzt werden. Das Identity Management System ist gegen unbefugte Zugriffe von innen und außen zu schützen.

#### **§ 4 Ausschluss der Leistungs- und Verhaltenskontrolle**

Anfallende Daten im Sinne dieser Dienstvereinbarung dürfen nur für die vereinbarten Zwecke verarbeitet werden. Sie dürfen nicht zu Zwecken einer Verhaltens- oder Leistungskontrolle oder zu Zwecken einer Ermittlung von Grundlagen für dienstliche Beurteilungen, Disziplinarmaßnahmen oder als Grundlage für die Feststellung des Gesundheitszustandes verarbeitet werden. Statistische Auswertungen sind ausschließlich anonymisiert zulässig. Der Systemadministrator gewährt dem Personalrat auf Verlangen Einsicht in die Systemdaten.

#### **§ 5 Aufbau, Änderung und Erweiterung des Systems**

- (1) Die in der Anlage beschriebenen Daten werden von den Quellsystemen über einen Konnektor an das Meta Directory übergeben und können von anderen Quell- und Zielsystemen wie vereinbart genutzt werden.
- (2) Bei der Entwicklung oder Erweiterung von Konnektoren für Quell- und Zielsysteme ist die Inbetriebnahme nur unter Einhaltung der datenschutzrechtlichen Bestimmungen und nach rechtzeitiger Beteiligung bzw. Einbeziehung des örtlichen Personalrates zulässig. Die Anlagen sind entsprechend anzupassen.
- (3) Die Beschäftigten sind unverzüglich über wesentliche Änderungen und Erweiterungen zu informieren.

#### **§ 6 Beschreibung und Dokumentation des Systems**

- (1) Das IDM-Gesamtsystem wird von der TU Bergakademie Freiberg betrieben.
- (2) In den Anlagen zu dieser Dienstvereinbarung werden Software und technischer Umfang des DV-Systems, Regelungen zum Datenschutz und zur Datensicherung, Festlegungen von Datenfeldern, Standardauswertungen und Zugriffsberechtigungen beschrieben. Die Anlagen sind Bestandteil dieser Dienstvereinbarung und konkretisieren sie. Im Einzelnen sind folgende Anlagen beigefügt:
  - Anlage 1: Enthält Systembeschreibung und Datenfelder des Identity Management Systems und der Quellsysteme
  - Anlage 2: enthält Beschreibungen zu den Zielsystemen des Identity Management Systems (vgl. § 9 dieser Dienstvereinbarung)

## **§ 7 Verarbeitung personenbezogener Daten**

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Personenbezogene Daten dürfen im Identity Management System nur verarbeitet werden, wenn diese Verarbeitung unter Beachtung des Sächsischen Datenschutzgesetzes in der jeweils geltenden Fassung geregelt und die Freigabe durch den sächsischen Datenschutzbeauftragten erfolgt ist. Art und Umfang der zu verarbeitenden personenbezogenen Daten ergeben sich aus Anlage 1, Abschnitt 2.

## **§ 8 Datenschutz und Datensicherheit**

- (1) Durch geeignete technische und organisatorische Maßnahmen ist mit angemessener Sorgfalt und auf Grundlage des an der TU Bergakademie Freiberg gegebenen Standes der Technik gemäß Art. 9 des Sächsischen Datenschutzgesetzes sicherzustellen, dass Unbefugte keine Möglichkeit haben, die auf den Datenträgern gespeicherten Daten zu lesen, zu verändern oder zu kopieren.
- (2) Vorgänge im Identity Management System, bei denen personenbezogene Daten protokolliert werden, sind in der Anlage 1, Abschnitt 3.2 aufgeführt.
- (3) Der Zugriff auf Protokolldaten ist ausschließlich den von der TU Bergakademie Freiberg beauftragten Systemadministratoren, dem Datenschutzbeauftragten und dem örtlichen Personalrat im Rahmen des Sächsischen Datenschutzgesetzes gestattet. Eingriffe der Systemadministratoren dürfen ausschließlich der Sicherstellung der technischen Funktionalität dienen. Eine Herausgabe von Daten an Einzelpersonen ist nicht statthaft.
- (4) Die Systemadministratoren des IDM-Gesamtsystems und der angeschlossenen Quell- und Zielsysteme müssen in einer am Rechenzentrum geführten Liste erfasst werden. Diese Liste wird dem Personalrat zur Verfügung gestellt, etwaige Änderungen werden umgehend mitgeteilt. Die Beschäftigten, insbesondere die mit der Wartung des IDM-System betrauten Mitarbeiter, sind auf das Datengeheimnis nach §6 SächsDSG zu verpflichten, dass Sie die ihnen zur Kenntnis gelangten Informationen weder weitergeben noch verwenden dürfen.
- (5) Die Universität ist zur Vermeidung jeglichen Missbrauchs des Identity Management Systems und aller angebundenen Quell- und Zielsysteme verpflichtet. Missbräuchlich ist insbesondere die Verwendung von Daten, die entgegen den datenschutzrechtlichen Vorschriften oder durch ungerechtfertigten Eingriff in das Persönlichkeitsrecht erhoben werden. Nähere Bestimmungen werden in den Regelungen zu den Quell- und Zielsystemen getroffen. Wird eine missbräuchliche Nutzung festgestellt, ist die Universität verpflichtet, die Ursachen dafür umgehend abzustellen und den Personalrat zu informieren. Besteht ein ausreichend begründeter Verdacht der missbräuchlichen Datenerhebung oder missbräuchlichen Nutzung des IDM-Gesamtsystems, findet unter Beteiligung des Personalrates eine gezielte Überprüfung statt.
- (6) Die Beschäftigten werden rechtzeitig und in geeigneter Art und Weise durch den Systembetreiber über die Einführung und Funktionsweise des IDM-Systems

informiert. Bei Neueinstellung erhalten die Mitarbeiter ein entsprechendes Formblatt.

- (7) Beschäftigte haben die Möglichkeit Auskunft über alle im Identity Management System zu ihrer Person gespeicherten Daten zu erhalten, s. Anlage 2 Abschnitt 11.1.

### **§ 9 Anschluss von Zielsystemen**

- (1) Zielsysteme des Identity Management Systems sind Systeme oder Verzeichnisse, die das Identity Management System als Datenquelle nutzen, um bestehende Geschäftsprozesse zu unterstützen.
- (2) Die Weitergabe von Daten und Zuteilung von Ressourcen oder Berechtigungen müssen dem Grundsatz genügen, dass nur diejenigen Daten übergeben werden, die im Zielsystem für die Wahrnehmung der Ziele des Zielsystems erforderlich sind.
- (3) Eine Übersicht aller aktuellen Zielsysteme ist in der Anlage 2, Abschnitt 1.1 aufgeführt. Jedes Zielsystem ist durch einen Gliederungspunkt in der Anlage 2 an diese Dienstvereinbarung dokumentiert. Diese Dokumentation enthält folgende Informationen:
1. Grundsätzliche Beschreibung des Systems
  2. Darlegung der Ziele, die mit dem System verfolgt werden.
  3. Aufstellung der vom Identity Management System weitergegebenen Datenfelder.
  4. Beschreibung, wie das System administriert wird.
  5. Beschreibung, wie in dem System Datenschutz garantiert wird.
  6. Beschreibung und Begründung der Regeln, die der Weitergabe der Daten oder der Zuteilung einer Ressource oder einer Berechtigung zugrunde liegen. Insbesondere ist darzulegen, ob die Regeln grundsätzlich auf einem Automatismus basieren oder durch einen zusätzlichen Administrationsvorgang beeinflusst werden.

### **§ 10 Lösungsfristen**

Nach Ablauf des letzten Vertrages einer Person/eines Mitarbeiters gelten eine 30 tägige Ablaufphase und eine 180 Tage währende Inaktivitätsphase. Danach wird das Benutzerkonto inklusive der personenbezogenen Daten im IDM-System vollständig gelöscht. Weiterführende Informationen sind in Abschnitt 3.4 der Anlage 1 zu finden.

## § 11 Inkrafttreten, Laufzeit, Kündigung

- (1) Die Dienstvereinbarung tritt am Tag nach ihrer Unterzeichnung in Kraft.
- (2) Für die Kündigung dieser Vereinbarung gilt § 84 des Sächsischen Personalvertretungsgesetzes in der jeweils gültigen Fassung. Die Parteien haben unverzüglich Verhandlungen über eine neue Dienstvereinbarung aufzunehmen. Bis zum Abschluss einer neuen Dienstvereinbarung gilt die bisherige fort.

Freiberg, den 12. November 2015

Für die TU Bergakademie  
Freiberg

Der Rektor

  
Prof. Barbknecht

Der Kanzler

  
Dr. Handschuh

Für den Personalrat

Die Vorsitzende

  
Frau Engelhardt