



Ordnung zum Betrieb des Identitätsmanagementsystems (IDM) der Hochschule Zittau/Görlitz

Gemäß § 13 Abs. 5 SächsHSFG

Präambel

Für die sichere und effektive Nutzung von zentralen Diensten ist ein Identitätsmanagementsystem (im Folgenden: IDM) für die gesamte Hochschule Zittau/Görlitz (HSZG) eingerichtet. Die zentrale Verwaltung der Benutzerdaten erhöht das Sicherheitsniveau und bietet effektive Möglichkeiten, den Benutzern die Berechtigungen und Ressourcen automatisch zuzuweisen bzw. zu entziehen.

Für die innerhalb des IDM verarbeiteten Daten gelten die einschlägigen Bestimmungen zum Datenschutz, insbesondere die des Gesetzes über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulfreiheitsgesetz - SächsHSFG) und des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz - SächsDSG) sowie der IuK-Benutzungsordnung der HSZG in der jeweils geltenden Fassung.

§ 1

Geltungsbereich und Zweck

- (1) Der Geltungsbereich dieser Ordnung umfasst alle Struktureinheiten der HSZG. (Fakultäten, Zentrale Einrichtungen, Hochschulverwaltung).
- (2) Der Betrieb des IDM ist ausschließlich zum Zweck der zentralen Verwaltung von Benutzerdaten zur Authentifizierung, Provisionierung und Autorisierung für die Mitglieder, Angehörigen und Gäste der HSZG sowie vertraglich an die HSZG gebundene Personen/Einrichtungen (Dritte) zugelassen.
- (3) Die Nutzung des IDM für Prozesse der Verwaltung von Personal oder ähnlicher Aufgaben der HSZG sowie zur Leistungs- und Verhaltensfeststellung und Bewertung der Mitarbeiter und Studierenden ist unzulässig.
- (4) Für die Veröffentlichung von personenbezogenen Daten von Mitarbeitern nach § 2 Abs. 2 dieser Ordnung gelten die Bestimmungen des § 37 Abs. 2 SächsDSG. Für die Veröffentlichung personenbezogener Daten der Studierenden und Dritter ist diese Vorschrift sinngemäß anzuwenden.

§ 2

Begriffsbestimmungen

- (1) Das IDM dient der zentralen Verwaltung von Benutzerdaten zum Zweck der Authentifizierung, Provisionierung und Autorisierung für alle IT- und Kommunikationssysteme der HSZG.
- (2) Benutzer im Sinne dieser Ordnung sind Mitglieder, Angehörige und Gäste der HSZG sowie vertraglich an die HSZG gebundene Personen/Einrichtungen (Dritte).
- (3) Benutzerdaten im Sinne dieser Ordnung sind Daten, die die Authentifizierung eines Benutzers erlauben oder für die Provisionierung und Autorisierung des Benutzers für die Dienste und Daten, die er im Rahmen seiner Tätigkeit an der HSZG benötigt, erforderlich sind.
- (4) Authentifizierung im Sinne dieser Ordnung ist der eindeutige Nachweis einer vom Benutzer behaupteten Identität.
- (5) Provisionierung im Sinne dieser Ordnung ist die Bereitstellung von Zugriffsrechten auf Dienste und Daten, die ein Benutzer im Rahmen seiner Tätigkeit benötigt.
- (6) Autorisierung im Sinne dieser Ordnung ist die Überprüfung von Zugriffsrechten auf Dienste und Daten.
- (7) Konsolidierung im Sinne dieser Ordnung ist die eindeutige und quellsystemübergreifende Feststellung der Identität eines Benutzers.
- (8) Die Stammdaten der im IDM verwalteten Benutzer werden aus dem durch die DV-Verwaltung betriebenen DataWarehouse (DWH) importiert. Das DWH wiederum erhält die Daten aus Quellsystemen der Verwaltungsbereiche.
- (9) Der Betrieb des IDM umfasst den Import von Daten aus dem DWH, die interne Verarbeitung von Daten und die definierte Übermittlung von Daten an die angebotenen Zielsysteme. Ein Zielsystem nutzt die nach § 4 Abs. 3 dieser Ordnung erforderliche Teilmenge der im IDM verarbeiteten Daten. Die an das Zielsystem übermittelten Daten können auf zwei verschiedene Arten genutzt werden:
 1. Authentifizierung und Autorisierung der Benutzer,
 2. Abfrage der zentralen Informationen zur Synchronisation der Benutzerdaten

Eine zu aktualisierende bzw. fortzuschreibende Übersicht der gemäß dieser Ordnung zulässigen Zielsysteme und der Art und des Umfangs der übermittelten Daten sowie der im IDM gespeicherten Daten wird im ZKI, Hochschulrechenzentrum geführt.

§ 3 Verantwortlichkeiten

- (1) Für den Betrieb des IDM ist das ZKI, Hochschulrechenzentrum verantwortlich.
- (2) Für die Zulässigkeit der Errichtung und des Betriebes der zutreffenden Import- und Exportschnittstellen ist die jeweilige datenverarbeitende Stelle verantwortlich. Für den Betrieb der Import- und Exportschnittstellen ist das HRZ zuständig.
- (3) Voraussetzung für die Zulässigkeit einer Übermittlung von personenbezogenen Daten von einem Quellsystem an das IDM sowie vom IDM an ein Zielsystem ist ein Eintrag des Quell- bzw. Zielsystems in das Verzeichnissverzeichnis sowie der Nachweis der im Quell- bzw. Zielsystem und für die Übermittlung getroffenen Maßnahmen nach § 9 Abs. 2 Nr. 1 bis Nr. 6 SächsDSG.

§ 4 Verarbeitung personenbezogener Daten

- (1) Im IDM erfolgt die Verarbeitung personenbezogener Daten für Mitglieder, Angehörige und Gäste der HSZG sowie vertraglich an die HSZG gebundene Personen/Einrichtungen (Dritte).
- (2) Die Verarbeitung personenbezogener Daten erfolgt im IDM ausschließlich zu den in § 1 Abs. 2 dieser Ordnung genannten Zwecken.
- (3) Die im IDM gespeicherten Daten dürfen nur an Zielsysteme übermittelt werden, sofern die Übermittlung zum ordnungsgemäßen Betrieb des Zielsystems erforderlich ist und dem in § 1 dieser Ordnung genannten Zweck dient.
- (4) Bei Beendigung des Rechtsverhältnisses eines Benutzers wird die zentrale Benutzerkennung des Benutzers nach vorgegebenen Fristen gesperrt (Inaktiv setzen) und später gelöscht. Die einschlägigen Fristen ergeben sich aus den entsprechenden Verzeichnissen.
- (5) Die Login-Kennzeichen und E-Mail-Adressen der Benutzer werden mit Ablauf der Löschfrist ausschließlich zum Zweck der Verhinderung der nochmaligen Vergabe dauerhaft für die Dauer von 3 Jahren gespeichert und blockiert.

§ 5 Zugriffsberechtigungen

- (1) Grundlage für die Vergabe der Zugriffsberechtigungen im IDM ist ein mehrstufiges Rechtekonzept:
 1. IDM-Benutzer haben Zugriff auf die über ihre Person verarbeiteten Daten,
 2. Zielsystem-Administratoren haben Zugriff auf Daten der für ihren Dienst provisionierten IDM-Benutzer,
 3. IDM-Administratoren haben Zugriff auf die Daten aller IDM-Benutzer.
- (2) Zur Gewährleistung des § 1 Abs. 2 ist eine Herausgabe von personenbezogenen Daten durch die Administratoren an die Dienststellenleitung nur im Einvernehmen mit dem Datenschutzbeauftragten und dem Personalrat der HSZG zulässig.

§ 6

Technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit

Die Festlegungen zur Gewährleistung des Datenschutzes und der Datensicherheit, insbesondere die Maßnahmen nach § 9 Abs. 2 Nr. 1 bis 6 SächsDSG, sind im vom Datenschutzbeauftragten der HSZG geführten Verzeichnisses zugehörig zum entsprechenden System beschrieben.

§ 7

Inkrafttreten, Veröffentlichung

- (1) Diese Ordnung wurde am 20.04.2016 vom Rektorat beschlossen und tritt mit ihrer Veröffentlichung in Kraft.
- (2) Die Bekanntmachung dieser Ordnung erfolgt in den Amtlichen Bekanntmachungen der HSZG.

Zittau, den 17.05.2016



Prof. Dr. phil. Albrecht
Rektor