Ordnung zur Errichtung und zum Betrieb eines Identitätsmanagementsystems an der Technischen Universität Dresden

Vom 26. Juli 2011

Aufgrund von § 13 Abs. 5 des Gesetzes über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz – SächsHSG) vom 10.12.2008 (SächsGVBl. S. 900) hat das Rektorat der TU Dresden folgende Ordnung beschlossen:

Präambel

Die TU Dresden strebt eine Integration ihrer komplexen und heterogenen IT-Systemlandschaft zu einer nahtlosen und redundanzfreien Umgebung im Sinne zentraler Dienste an. Zur effektiven und sicheren Nutzung zentraler Dienste ist ein einheitliches Identitätsmanagement, im folgenden IDM genannt, notwendig. Die zentrale Verwaltung der Benutzerdaten am ZIH entlastet die einzelnen Dienstbetreiber von aufwendigen Routinearbeiten und erhöht das allgemeine Sicherheitsniveau durch die Möglichkeit, 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 Hochschulgesetz - SächsHSG), des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz - SächsDSG) sowie der Rahmenordnung für die Rechen- und Kommunikationstechnik und die Informationssicherheit an der TU Dresden (IuK-Rahmenordnung) in der jeweils geltenden Fassung.

§ 1
Geltungsbereich und Zweck

(1) Das IDM umfasst den Geltungsbereich nach § 1 Abs. 1 und Abs. 3 der IuK-Rahmenordnung. Für andere Einrichtungen nach § 1 Abs. 2 IuK-Rahmenordnung sind mit den jeweiligen Einrichtungen gesonderte Vereinbarungen notwendig.

(2) Die Errichtung und der Betrieb eines IDM ist ausschließlich zum Zweck der zentralen Verwaltung von Benutzerdaten für die Authentifizierung, Provisionierung und Autorisierung für alle Einrichtungen nach § 1 Abs. 1 IuK-Rahmenordnung zugelassen.

(3) Die Nutzung zu Zwecken der Personalverwaltung oder ähnlicher Aufgaben der Technischen Universität Dresden sowie zur Leistungs- und Verhaltensfeststellung und Bewertung der Mitarbeiter und Studenten 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 Studenten und Gäste ist diese Vorschrift sinngemäß anzuwenden.

§ 2
Begriffsbestimmungen

(1) Ein IDM dient der zentralen Verwaltung von Benutzerdaten zum Zweck der Authentifizierung, Provisionierung und Autorisierung für alle rechen- und kommunikationstechnischen Einrichtungen der TU Dresden.

(2) Benutzer im Sinne dieser Ordnung sind die Mitglieder der geschlossenen Benutzergruppe gemäß § 1 Abs. 3 IuK-Rahmenordnung.

(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 TU Dresden 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 Quellsystemen importiert. An der TU Dresden können folgende Typen von Quellsystemen an das IDM angebunden sein:

1. Personalverwaltung
2. Studentenverwaltung

Für eine vorgesehene Gästeverwaltung gelten die Bestimmungen dieser Ordnung entsprechend. Eine fortzuschreibende Übersicht der gemäß dieser Ordnung zulässigen Quellsysteme und der Art und des Umfangs der übermittelten Daten ist in Anlage 1 dokumentiert.

(9) Der Betrieb des IDM umfasst den Import von Daten aus den angebundenen Quellsystemen, die interne Verarbeitung von Daten und die definierte Übermittlung von Daten an die angebundenen 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

(10) Eine fortzuschreibende Übersicht der gemäß dieser Ordnung zulässigen Zielsysteme und der Art und des Umfangs der übermittelten Daten ist in Anlage 2 dokumentiert.

§ 3
Verantwortlichkeiten

(1) Für den Betrieb des IDM ist das Zentrum für Informationsdienste und Hochleistungsrechnen (ZIH) der TU Dresden 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 ZIH zuständig.

(3) Vorrausetzung 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 Verfahrensverzeichnis nach RS D4/2/04 sowie der Nachweis der 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 die geschlossene Benutzergruppe nach § 1 Abs. 3 IuK-Rahmenordnung. Eine fortzuschreibende Übersicht der Art und des Umfangs der im IDM verarbeiteten Daten ist in Anlage 3 dokumentiert.

(2) Die Verarbeitung personenbezogener Daten erfolgt im IDM ausschließlich zu den in § 1 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) Beim Ausscheiden eines Benutzers aus der geschlossenen Benutzergruppe gemäß § 1 Abs. 3 IuK-Rahmenordnung wird die zentrale Benutzerkennung des Benutzers gesperrt. Die Löschung der Benutzerdaten erfolgt spätestens nach Ablauf von 15 Kalendermonaten nach der Sperrung der zentralen Benutzerkennung.

(5) Die Login-Kennzeichen und E-Mail-Aliase der Benutzer werden mit Ablauf der Löschfrist ausschließlich zum Zweck der Verhinderung der nochmaligen Vergabe an Dritte dauerhaft archiviert.

(6) Sofern die Daten für eine Abrechnung der genutzten IT-Dienstleistungen und Ressourcen erforderlich sind, kann die Löschung der Benutzerdaten unterbleiben. Die Speicherung kann für den Zeitraum erfolgen, für den diese Daten zu Zwecken der Rechnungslegung und Rechnungsprüfung erforderlich sind.

§ 5
Zugriffsrechte

(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) Für die Nutzung, die Erteilung und den Entzug von Zugriffsberechtigungen gelten insbesondere die Bestimmungen des § 14 IuK-Rahmenordung.

(3) Eine fortzuschreibende Übersicht der Zugriffsberechtigungen auf das IDM ist Bestandteil des Sicherheitskonzepts gemäß § 6 dieser Ordnung.

§ 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 IT-Sicherheitskonzept in Anlage 4 beschrieben.

§ 7
Schlussbestimmungen und Übergangsvorschriften

(1) Für die Entwicklung des IDM wird ein iteratives Vorgehen benutzt. Als Ergebnis der ersten Iteration wird das IDM den Funktionsumfang der derzeitigen Benutzerverwaltung des ZIH umfassen. In weiteren Iterationen wird der Funktionsumfang des IDM gemäß den Anforderungen der TU Dresden erweitert.

(2) Die derzeitige Benutzerverwaltung des ZIH verbleibt im Produktivbetrieb, bis ihre Funktionalität vollständig durch das IDM abgelöst ist. In der Übergangszeit werden beide Systeme parallel betrieben.

(3) Das IDM sowie diese Ordnung sind nach Ablauf von 12 Kalendermonaten nach Inkrafttreten dieser Ordnung durch das SMT gemäß § 19 IuK-Rahmenordnung und unter Berücksichtigung der einschlägigen Bestimmungen des Sächsischen Personalvertretungsgesetz in der jeweils gültigen Fassung zu evaluieren.

§ 8
Veröffentlichung, Inkrafttreten

(1) Diese Ordnung tritt am Tage nach Veröffentlichung in den Amtlichen Bekanntmachungen der TU Dresden in Kraft.
(2) Diese Ordnung ist ausgefertigt aufgrund des Beschlusses des Rektorats der TU Dresden vom 26. Juli 2011.

Dresden, den 26. Juli 2011

Der Rektor
Der Technischen Universität Dresden

Prof. Dr. Dr.-Ing. habil. Hans Müller-Steinhagen

Einsicht in die Anlagen ist im Einzelfall auf Antrag beim Datenschutzbeauftragten möglich.