TECHNISCHE UNIVERSITÄT DARMSTADT

Dienstvereinbarung über die Einführung und Anwendung eines Identity Management Systems
mit den daran angeschlossenen Quell- und Zielsystemen
an der Technischen Universität Darmstadt

§ 1 Gegenstand und Intention

(1) Das Identity Management System (IDM) dient der Verwaltung von Personal-Identitäten und ihnen zugeordneten Ressourcen und Zugriffsberechtigungen auf der Grundlage einer konsolidierten und ständig aktuellen Datenbasis. Ziel der Einführung ist neben der Stärkung der Leistungsfähigkeit und Erhöhung der Servicefreundlichkeit der Universität, die Erhöhung der Datensicherheit durch die Möglichkeit der Authentifizierung im Rahmen des Datentransfers.

(2) Diese Dienstverarbeitung definiert Grundsätze für die Einführung und den Betrieb des IDM sowie für Systeme, die Daten in das IDM einspeisen (Quellen) und Systemen, die Daten aus dem IDM erhalten (Ziele). Diese haben eigene Begründungen und Grundlagen für ihren Betrieb. Im Rahmen dieser Dienstvereinbarung werden auch Regelungen über eine Dokumentationspflicht dieser angeschlossenen Systeme und der Datenweitergabe an diese getroffen. Die Dienstvereinbarung regelt die Übernahme von Daten über Mitarbeiterinnen und Mitarbeiter an das IDM sowie Grundsätze für die Speicherung der Daten und für die Weitergabe der Daten an andere Systeme. Darüber hinaus werden Grundsätze getroffen, wie mit dem IDM gearbeitet wird, und wie es administriert wird.

§ 2 Geltungsbereich

Diese Dienstvereinbarung gilt für alle Beschäftigten der TU Darmstadt nach § 3 HPVG und alle Einrichtungen der TU Darmstadt.

§ 3 Aufgaben und Ziele des Identitätsmanagements

(1) Der im IDM verwaltete Bestand von Personendaten wird aus den EDV-Systemen der Personalverwaltung, des Hochschulrechenzentrums, sowie der Studentenverwaltung übernommen.

(2) Das Identitätsmanagement soll eine Infrastruktur schaffen die es den Hochschulmitgliedern erlaubt, sich gegenüber allen EDV-Systemen der Hochschule in einheitlicher Weise zu authentifizieren. Die Möglichkeit der persönlichen Authentifizierung soll u.a. genutzt werden um Verwaltungsprozesse durch Selfcare-Funktionen zu stützen. Darüber hinaus sollen Daten über Personen, die von allgemeinen Interesse sind (Räume, Telefonnummern, Email-Adressen), die aber in unabhängiger Weise den Personen zugeteilt werden, im Identitätsmanagement zusammengeführt werden.

(3) Mit dem Betrieb des IDM werden insbesondere folgende Ziele verfolgt:

a) Rationalisierung von Administrations- und Verwaltungsvorgängen
b) Erhöhung der Datenqualität
c) Erfüllung des Prinzips der Datensparsamkeit
d) Erhöhung von Datenschutz durch Transparenz über Speicherung von Personendaten und über Datenflüsse
e) Erhöhung von Datenschutz durch gezielte Verwaltung von Zugriffsberechtigungen
f) Erhöhung von Sicherheit durch eindeutige elektronische Identitäten
g) Erhöhung von informationeller Selbstbestimmung

§ 4 Ausschluss der Leistungs- und Verhaltenskontrolle

Das IDM wird nicht zur Leistungs- und Verhaltenskontrolle genutzt. Statistische Auswertungen sind ausschließlich anonymisiert zulässig.

§ 5 Rechte der Beschäftigten

Die Beschäftigten werden rechtzeitig und in geeigneter Art und Weise über die Einführung und Funktionsweise des IDM informiert. Sie erhalten auf Anfrage kostenlos Auskunft über alle zu ihrer Person gespeicherten Daten.

§ 6 Einarbeitung, Qualifizierung der Beschäftigten

Beschäftigte, deren Tätigkeiten mit Quell- oder Zielsystemen des Identitätsmanagements im Zusammenhang stehen, werden über die Veränderungen betrieblicher Abläufe umfassend informiert. Beschäftigte werden rechtzeitig umfassend und gründlich geschult. Hierzu werden geeignete Schulungsangebote unterbreitet. Beschäftigte, deren Aufgaben sich durch die Einführung des Identitätsmanagements ändern, werden mindestens gleichwertig eingesetzt und dafür entsprechend qualifiziert.

§ 7 Rechte des Personalrats

Die Personalräte werden über Änderung des Identitätsmanagements rechtzeitig und gemäß der Dokumentation nach §7 und §9 informiert, dies gilt insbesondere für Änderungen in Bezug auf die Quell- und Zielsysteme. Die Personalräte werden, wenn sie es für notwendig erachten, mit jeweils bis zu 2 Vertreterinnen oder Vertretern in entsprechende Arbeitsgruppen einbezogen, welche dann auch Vorschläge für erforderliche Veränderungen dieser Dienstvereinbarung vorbereiten. Die Personalräte haben das Recht, unter Hinzuziehung des Datenschutzbeauftragten, Aufklärung und Einsicht in die Systemdaten zu verlangen.

§ 8 Beschreibung und Dokumentation des Systems

(1) Eine detaillierte Beschreibung des Identitätsmanagements ist als **Anlage** 1 zu dieser Dienstvereinbarung beigefügt (Vorabkontrolle und Verfahrensverzeichnis „Identity Managament" Stand: xy) . Diese Anlage enthält insbesondere folgende Punkte:

a) Beschreibung der enthaltenen Daten
b) Beschreibung des Aufbaus und der grundsätzlichen Arbeitsweise des IDM
c) Beschreibung der Mechanismen, die das IDM vor unberechtigten Zugriff schützen
d) Beschreibung der Vorgänge, die im IDM protokolliert werden

(2) Die in Abs. 1 genannte Anlage wird das aktuelle Administrationskonzept des Identitätsmanagement beschrieben. Der Systembetreiber des IDM (Hochschulleitung) ist verpflichtet, dieses Dokument soweit erforderlich anzupassen.

§ 9 Datenschutz und Datensicherheit

(1) Die Universität ist verpflichtet, personenbezogene Daten gegen Verlust, Ausspähung, Manipulation usw. durch entsprechende Maßnahmen zu sichern.
(2) Der Zugriff auf Protokolldaten ist ausschließlich dem Systembetreiber und den von ihm beauftragten Systemadministratoren und dem Datenschutzbeauftragten zur Erfüllung der ihnen obliegenden Aufgaben gestattet. Eingriffe der Systemadministratoren dürfen ausschließlich der Sicherstellung der technischen Funktionalität dienen.
(3) Die in § 8 Abs. 1 und § 10 Abs. 3 genannten Verfahrensverzeichnisse werden regelmäßig, mindestens im Abstand von 2 Jahren auf ihre Aktualität und Gültigkeit überprüft.

§ 10 Anschluss von Quell- und Zielsystemen

(1) Quellsysteme des Identitätsmanagements sind Systeme oder Verzeichnisse, die das IDM als Datengrundlage nutzt. Die Speicherung von Daten muss soweit erfolgen, dass eine Identität eindeutig erkannt und zugeordnet werden kann und von einer zentralen Stelle aus alle Zielsysteme mit denen für sie jeweils notwendigen Daten versorgt werden können. Die erfassten Daten werden jeweils pro Quellsystem ermittelt und sind dem zuvor genannten Zweck angepasst.

(2) Zielsysteme des Identitätsmanagements sind Systeme oder Verzeichnisse, die das IDM nutzen. Das kann z.B. die Weitergabe von Daten an das Zielsystem bedeuten, oder die Verwaltung von Ressourcen des Zielsystems im Identitätsmanagement. Die Weitergabe von Daten soll dem Grundsatz genü-

gen, dass nur diejenigen Daten übergeben werden, die im Zielsystem für die Wahrnehmung der Ziele des Zielsystems erforderlich sind. Die Zuteilung von Ressourcen oder Berechtigungen soll jeweils nach ausformulierten Grundsätzen erfolgen, die dem Zweck des Zielsystems angepasst sind.

(3) Jedes angeschlossene System wird in Form eines Verfahrensverzeichnisses, welches dieser Dienstvereinbarung als Anlage beigefügt wird, dokumentiert Diese Dokumentation muss, folgende Informationen enthalten:

a) Eine grundsätzliche Beschreibung des Systems
b) Eine Darlegung der Ziele, die mit dem System verfolgt werden
c) Eine Aufstellung der vom Identitätsmanagement weitergegebenen Datenfelder
d) Eine Beschreibung, wie das System administriert wird
e) Eine Beschreibung, wie in dem System Datenschutz gewährleistet wird
f) Eine 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.

§ 11 Missbrauch

Die Universität ist zur Vermeidung jeglichen Missbrauchs des IDM 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 sind in den Regelungen zu den Quell- und Zielsystemen getroffen. Wird eine missbräuchliche Nutzung festgestellt, ist die Hochschule verpflichtet, die Ursachen dafür umgehend abzustellen und die Personalräte und die Datenschutzbeauftragte(n) zu informieren. Besteht ein ausreichend begründeter Verdacht der missbräuchlichen Datenerhebung oder missbräuchlichen Nutzung des Identitätsmanagements und der Zielsysteme, findet unter Beteiligung des Personalrates eine gezielte Überprüfung statt.

§ 12 Verpflichtung der Systemadministratoren

Die Systemadministratoren werden aktenkundig auf die Einhaltung des Datenschutzgesetzes und auf die strafrechtlichen Konsequenzen bei Verstößen hingewiesen sowie über den Inhalt dieser Dienstvereinbarung informiert.

§ 13 Inkrafttreten

(1) Die Dienstvereinbarung tritt am Tag nach ihrer Unterzeichnung in Kraft.

TECHNISCHE UNIVERSITÄT DARMSTADT

(2) Die Vereinbarung kann sowohl von Seiten des Personalrats als auch von Seiten der Dienststelle unter Einhaltung einer Frist von 6 Monaten zum Quartalsende gekündigt werden. Wird die Fortwirkung von den Beteiligten verlangt, so gelten die Bestimmungen dieser Vereinbarung bis zum Abschluss einer neuen Vereinbarung fort.

(3) Änderungen der Vereinbarung bedürfen der Schriftform.

Darmstadt, den 20.04.2009

Für die Dienststelle:

Dr. Manfred Efinger, Kanzler

Für den Personalrat:

Anlagen:

Anlage 1:
Verfahrensverzeichnis IDM, Version: 1.5 vom 17.09.2008
Vorabkontrolle IDM, Version: 1.5 vom 19.09.2008

Anlage 2:
Verfahrensverzeichnis Chipkarte, Version: 1.5 vom 26.09.2008