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

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

TECHNISCHE UNIVERSITÄT DARMSTADT

HRZ Hochschulrechenzentrum

Vorabkontrolle für das Identity Management System der TU Darmstadt nach § 7 Abs. 6 HDSG

Betrieben durch das Hochschulrechenzentrum der TU Darmstadt

Dokument Version: 1.5 vom 19.09.2008

Technische Universität Darmstadt
Hochschulrechenzentrum
Petersenstraße 30
64287 Darmstadt
Telefon (06151) 16-2054
Telefax (06151) 16-3050

Inhaltsverzeichnis

Vorabkontrolle für das Identity Management System

1. Grundangaben

Die Grundangaben sind im Verfahrensverzeichnis Identity Management System eingetragen.

2. Rechtsgrundlage und Zweckbestimmung

Das Identity Management System (IDM) ist eine Infrastrukturmaßnahme, die für die Identitäts- und Rechteverwaltung benötigt wird. Das IDM-System ermöglicht eine zeitnahe Synchronisierung von Identitäten und Berechtigungen zwischen den daran angeschlossenen Quell- und Zielsystemen. Damit sind eine konsistente Verteilung und fristgerechte Löschung bzw. Änderungen von personenbezogenen Daten und Berechtigungen in den am IDM-System angeschlossenen Systemen (Anwendungen) möglich. Das IDM-System ist daher für den täglichen Betrieb der IT-Infrastruktur der Technischen Universität Darmstadt notwendig und damit im Sinne von § 34 Abs. 1 HDSG als organisatorische Maßnahme sowie für die Eingehung, Durchführung und Beendigung des Dienstverhältnisses erforderlich.

Angaben zur Art der gespeicherten Daten, Übermittlung, Zugriffsberechtigten und Löschfristen sind im Verfahrensverzeichnis Identity Management System eingetragen.

3. Prüfung, ob die Rechte der Betroffenen nach § 8 HDSG gewahrt sind

Die gespeicherten, individuellen Daten sind jederzeit durch den einzelnen Benutzer über eine Weboberfläche nach einer Authentifizierung einsehbar. Der Benutzer erhält durch den selbst durchgeführten Registrierungsprozess Kenntnis über seine gespeicherten persönlichen Daten.

Die Berichtigung, Sperrung oder Löschung der zu seiner Person im IDM-System gespeicherten Daten muss im jeweiligen Quellsystem (hier: Personalabteilung) erfolgen. Daten, die das HRZ verwaltet und im IDM-System gespeichert werden, können durch den Benutzer selbst über eine Weboberfläche in dem jeweiligen vom HRZ betriebenen Quellsystem (hier: zentraler Verzeichnisdienst) eingesehen und geändert werden.

Im IDM-System ist eine umfassende Überwachung und Protokollierung aller Vorgänge (sog. „Audit") gemäß § 10 Abs. 2 HDSG integriert. Dies ermöglicht auch eine nachträgliche Überprüfung der im Verfahrensverzeichnis definierten Datenverarbeitung. Die Aufbewahrungsdauer der Protokolldaten siehe im Verfahrensverzeichnis Identity Management System unter Punkt 7.

4. Risikofaktoren für einen Missbrauch der Daten

Der Datenaustausch zwischen Personalabteilung und Hochschulrechenzentrum kann kompromittiert werden, beispielsweise könnten während des Transportes Daten ausgespäht und/oder verändert werden. Dieses Risiko wird durch eine gesicherte Übertragung der Daten, durch starke Verschlüsselung und Einsatz von Prüfsummenverfahren nach dem jeweils aktuellen Stand der Technik abgesichert.

Die Speicherung der personenbezogenen Daten im IDM-System erfolgt in einem Verzeichnisdienst (im Folgenden Datenablage genannt) lokal auf dem IDM-Server. Der Zugang zu dieser Datenablage ist durch die Maßnahmen, wie im Verfahrensverzeichnis Identity Management System unter Punkt 7 und 8 beschrieben, abgesichert. Ein Zugriff auf die Datenablage von außen durch andere Benutzer, Rechner oder sonstige Systeme ist unterbunden (geschlossenes System). Ein Zugriff auf die Datenablage ist nur im Zuge administrativer Tätigkeiten möglich und auf eine kleine Anzahl fest angestellter Mitarbeiterinnen und Mitarbeiter des Hochschulrechenzentrums beschränkt. Die Sicherungsmaßnahmen und die berechtigten Personen sind im Verfahrensverzeichnis Identity Management System beschrieben.

Die Verarbeitung der gespeicherten, personenbezogenen Daten im IDM-System wird durch ein sog. „Audit-System" überwacht. Alle Aktivitäten, Änderungen, Löschungen etc. werden damit protokolliert. Es wird sichergestellt, dass unerlaubte und unerwünschte Aktivitäten und

Änderungen erkannt und verhindert werden können. Eine Revision aller Aktivitäten des IDM-Systems ist damit jederzeit möglich. Das Audit-System dient ferner auch zur Fehlersuche und –Analyse (mittels Standard-Logging-Funktionen). Es ist ein Bestandteil des IDM-Systems, daher ist der Zugriff auf das Audit-System auf den gleichen Personenkreis wie das IDM-System beschränkt.

Die Maßnahmen aus Verfahrensverzeichnis Identity Management System werden fortlaufend dem jeweils aktuellen Stand der Technik angepasst. Das beinhaltet Sicherheitsaktualisierungen sowie Einsatz von neuen, aktuelleren Maßnahmen.

5. Beurteilung der möglichen Folgen bei missbräuchlicher Verwendung der Daten

Es wurden alle erforderlichen Maßnahmen nach dem jeweils aktuellen Stand der Technik zum Schutz vor Missbrauch der personenbezogenen Daten getroffen. Die im Verfahrensverzeichnis Identity Management System unter Punkt 3 genannten Daten könnten durch vorsätzliche missbräuchliche Verwendung veröffentlicht werden. Im Zuge der Datensparsamkeit handelt es sich nicht um kritische Daten im Sinne von § 7 Abs. 4 HDSG. Es werden auch keine Daten zum Familienstand verarbeitet. Insoweit bestehen bei der Veröffentlichung der Daten keine direkten Gefahren, Nachteile oder finanzielle Schäden für den Einzelnen.

6. Angaben zu der Technik des Verfahrens

Die Angaben zu der Technik des Verfahrens sind im Verfahrensverzeichnis Identity Management System eingetragen.

7. Ergebnis der Vorabkontrolle

Der Einsatz des IDM-Systems als Infrastrukturmaßnahme ist für die Organisation der IT an der Technischen Universität Darmstadt erforderlich. Die aufgezeigten Risiken sind durch entsprechende Maßnahmen (siehe Verfahrensverzeichnis Identity Management System Abs. 7) nach dem jeweils aktuellem Stand der Technik abgesichert. Ferner wird durch das IDM-System eine Revision durch das sog. „Audit" realisiert und ermöglicht damit eine effektive Kontrolle der Sicherungsmaßnahmen und eine fortwährende Anpassung an neue Bedrohungsszenarien.

Der Einsatz des IDM-Systems bietet eine starke Verbesserung für bestehende Defizite in der derzeitigen IT-Infrastruktur, wie beispielsweise inkonsistente und intransparente Datenhaltung von personenbezogenen Daten und Berechtigungen. Insbesondere bietet das IDM-System eine zentrale Möglichkeit zu Auskünften über gespeicherte Daten, Berichtigungen von Daten, Sperrungen und Löschungen von Identitäten und Berechtigungen. Durch den automatisierten Bezug der Daten aus der Personalverwaltung (technisch das SAP HR Modul) wird eine taggenaue Aktualität der Daten in dem IDM-System sowie in allen Zielsystemen bzw. Zielanwendungen, in die das IDM-System Daten transportiert, gewährleistet. Dadurch wird das Risiko in den angeschlossenen Zielsystemen durch beispielsweise verspätete oder vergessene Löschungen von Benutzerkonten und Berechtigungen oder Änderungen derselben nach dem jeweils aktuellen Stand der Technik abgesichert. Insgesamt trägt daher das IDM-System zu einer deutlichen Erhöhung der Sicherheit und des Datenschutzes in der gesamten IT der Technischen Universität Darmstadt bei.

Es wurden alle erforderlichen Maßnahmen nach dem jeweils aktuellen Stand der Technik zum Schutz vor Missbrauch der personenbezogenen Daten getroffen. Zudem werden im Sinne der Datensparsamkeit nur die für die Zielanwendungen nötigsten Daten gespeichert und verarbeitet. Die Risiken des vorliegenden Verfahrens sind daher minimal, das vorliegende Verfahren unterstützt und verbessert den Datenschutz in der IT-Infrastruktur der Technischen Universität Darmstadt deutlich. Es ist damit sichergestellt, dass die Rechte der informationellen Selbstbestimmung durch das vorliegende Verfahren nicht verletzt werden

TECHNISCHE UNIVERSITÄT DARMSTADT

HRZ Hochschulrechenzentrum

Verfahrensverzeichnis TUDcard nach § 6 HDSG

Betrieben durch das Hochschulrechenzentrum der TU Darmstadt

Dokument Version: 1.5 vom 26.09.2008

Technische Universität Darmstadt

Hochschulrechenzentrum

Petersenstraße 30
64287 Darmstadt
Telefon (06151) 16-2054
Telefax (06151) 16-3050

Inhaltsverzeichnis

Verfahrensverzeichnis TUDcard

lfd. Nr. ☒ neues Verfahren ☐ Änderung

☒ Das Verzeichnis ist zur Einsichtnahme bestimmt (§ 6 Abs. 2 HDSG).

☐ Das Verzeichnis ist nur teilweise zur Einsichtnahme bestimmt.
Ausgenommen sind die Angaben nach § 6 Abs. 1 Satz 1 Ziffern 7, 8 und 11 HDSG.

☐ Das Verzeichnis ist nicht zur Einsichtnahme bestimmt (§ 6 Abs. 2 Satz 2 HDSG).

☐ Das Verfahren ist Teil eines gemeinsamen Verfahrens nach § 15 HDSG.
Federführende Stelle:

1. Name und Anschrift der datenverarbeitenden Stelle

1.1	Name und Anschrift ***Technische Universität Darmstadt, Karolinenplatz 5, 64289 Darmstadt***
1.2	Organisationskennziffer, Amt, Abteilung, ggf. Sachgebiet ***Hochschulrechenzentrum (HRZ), Petersenstr. 30, 64287 Darmstadt***
1.3	Name u. Anschrift des Auftragnehmers, wenn die Daten nach § 4 HDSG in Auftrag verarbeitet werden

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung ***Multifunktionale Chipkarte für die Bediensteten der Technischen Universität***
2.2	ggf. Bezeichnung des Verfahrens ***TUDcard***
2.3	Rechtsgrundlage (ggf. nach Art der DV unterschieden) ***§ 34 Abs. 1 HDSG***

3. Art der gespeicherten Daten

		Datum nach § 7 Abs. 4 HDSG

lfd. Nr.	Herkunft: Datum (SAP bzw. HRZ Datenelementname)	Datum nach § 7 Abs. 4 HDSG	
		Ja	Nein
1	***SAP: Vorname (VORNA)***	☐	☒
2	***SAP: Nachname (NACHN)***	☐	☒
3	***SAP: Vorsatzwort (VORSW)***	☐	☒
4	***SAP: Zusatzwort (NAMZU)***	☐	☒
5	***SAP: Aufbereiteter Name des Mitarbeiters (ENAME)***	☐	☒
6	***HRZ: Name Benutzerkonto (cn)***	☐	☒
7	***HRZ: Name Organisationsobjekt (ou)***	☐	☒
8	***HRZ: E-Mail Adresse (Flexitrust:User:AssignedMail)***	☐	☒
9	***TUDcard: Asymmetrisches Schlüsselpaar („public key", „private key")***	☐	☒
10	***HRZ: Zertifikat mit „public key"***	☐	☒

4. Kreis der Betroffenen

lfd. Nr.	
1	***Angehörige der TU Darmstadt***
2	***Privatdozenten und Gastwissenschaftler***

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

5.1 Empfänger der Daten

lfd. Nr. aus Ziffer 3	Empfänger der Daten
1-10	***HRZ (Chipkarten-Management System)***

5.2 Herkunft der Daten

lfd. Nr. aus Ziffer 3	Herkunft der Daten
1-8,10	***HRZ (Identity Management System)***
9	***Wird vom Hersteller der Karten generiert***

6. Zugriffsberechtigte Personen oder Personengruppen

lfd. Nr.	

	Projektgruppe „TUDcard", AG „PC-Gruppe", AG „U+N" (Jochen Becker, Markus Borst, Mathias Frohna, Reiner Hoenig, Manfred Lang, Christiane Schäfer, Petra Schödler, Nadine Thybusch, Angelika Zielinski)
1-8, 10	***Mitarbeitern des HRZ-Services***
	Folgende Personen haben vollen Zugriff auf das System und können anderen Personen Zugriffsrechte erteilen und entziehen: Systemadministratoren (Jochen Becker, Markus Borst, Mathias Frohna, Reiner Hoenig, Manfred Lang, Petra Schödler)
9	***Der „private Key" ist fest auf der Karte gespeichert und kann nicht ausgelesen oder kopiert werden. Der „public key" steht jedem zur Verfügung, der eine gesicherte Kommunikation mit dem Besitzer des „private key" durchführen möchte.***

7. Technische und organisatorische Maßnahmen (§ 10 Abs. 2 HDSG)

Folgende aufeinander aufbauende Festlegungen wurden getroffen:

☐ Hinsichtlich der allgemeinen Sicherheit wird auf das vorhandene Sicherheitskonzept verwiesen.

☒ Erläuterungen zu den einzelnen Maßnahmen, insbesondere soweit diese das Verfahren betreffen:

Zutrittskontrolle (z.B. EDV-Technik in gesicherten Räumen, Sicherheitsschlösser vorhanden)

EDV-Technik in gesicherten Räumen

Benutzerkontrolle (z.B. Passwortregelungen zur Authentifizierung, automatische Bildschirmsperrung)

Individuelle Authentifizierung aller Berechtigten mit Benutzername und Passwort

Zugriffskontrolle (z.B. Differenzierte Zugriffe auf einzelne Felder, unterschiedliche Berechtigungen)

Berechtigungen in Form von Access Control Lists (ACL) und Rollen

Datenverarbeitungskontrolle (z.B. kein Zugriff auf Betriebssystemebene, Verschlüsselung von Daten)

Zugriff auf die Daten mit verschlüsselter Übertragung nach jeweils aktuellem Stand der Technik

Kein direkter Zugriff auf Betriebssystemebene (kontrollierte Schnittstellen) nach jeweils aktuellem Stand der Technik

verschlüsseltes Backup nach jeweils aktuellem Stand der Technik (siehe Punkt 12.5)

Verantwortlichkeitskontrolle (z.B. Protokollierung der Dateneingabe, Aufbewahren der Protokolldaten)

Sicherung (Backup) der Datenbank (siehe Punkt 12.5)

Protokollierung aller Vorgänge (Anlegen, Ändern und Löschen von Daten)

Die Aufbewahrungsdauer der Protokolldaten und des Backups beträgt ein Jahr (siehe Punkt 12.5)

Auftragskontrolle (z.B. klare Vertragsregelungen mit dem Auftragnehmer, Prüfung der Zuverlässigkeit)

Produktion der Chipkarten. Siehe Punkt 12.2

Dokumentationskontrolle (z.B. klare und umsetzbare Dokumentation, Überprüfung der Maßnahme)

TUD-interne Betriebsorganisation

Art der ausgetauschten Daten (Datenfeldkatalog), Auflistung von Auswertungen und berechtigte Personen im HRZ sind unter Punkt 6 dokumentiert

Verfahren und Prozesse zur Schlüsselsicherung („Key-Backup") und zur Schlüsselwiederherstellung („Key-Recovery") sind in der Anlage Schlüsselverwaltung dokumentiert

Organisationskontrolle (Festlegung klarer Zuständigkeiten und Verantwortlichkeiten)

HRZ-interne Betriebsorganisation mit zwei Zuständigkeitsstufen

Third-Level: Projektmanagement

First-Level: Tägliche Organisation in den Büros des HRZ-Service (Kartenverlust, Kartendefekt, Sperre, Neuausgabe) und Unterstützung der Benutzer bei Fragen und Problemen

8. Technik des Verfahrens

8.1

☐ **Einzelplatzrechner/Arbeitsplatzrechner/Stand Alone PC**

Betriebssystem:

☐ Unix ☐ Windows NT ☐ Windows _____ ☐ anderes _____

weiter mit Ziff. 8.3

8.2

☒ **Vernetzte Rechner**

8.2.1 **Hardware**

☐ Großrechner

Betriebssystem: (z.B. UNIX/OS)

Datenendgerät:

☐ Terminal/Netz-PC (ohne Laufwerk/Festplatte)

☐ PC (Arbeitsplatzrechner/Workstation)

☒ Server

Betriebssystem: (z.B. Windows NT) ***Novell Netware, Linux***

Datenendgerät:

☐ Terminal/Netz-PC (ohne Laufwerk/Festplatte)

☒ PC (Arbeitsplatzrechner/Workstation)

☐ Sonstige eingesetzte Hardware (z.B. Chipkarte, Kartenlesegeräte, Videogeräte)

8.2.2 **Netzstruktur**

☒ Netz innerhalb der Behörde (Intranet)

☒ Lan ☐ Intranet ☐ sonstiges

☐ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises (z.B. KIV, KGRZ, Hessische Landesverwaltung)

☐ KIV/KGRZ ☐ Netz der Landesverwaltung (HCN 2000) ☐ sonstiges

☐ Offene Netze (z.B. Internet)

8.2.3 **Datenspeicherung auf:**	**Art der Daten (lfd. Nr. aus Ziffer 3):**
☐ Großrechner	
☒ Server innerhalb der Behörde	***1-8, 10***
☐ Server bei anderen Institutionen	
☒ TUD-Chipkarte	***1-10***

	Eingesetzte Software (einschl. Standardverfahren)	Version/Stand/Datum:
8.3	▪ ***Novell eDirectory*** ▪ ***FlexSecure „FlexiTrust" (Trustcenter-Software)*** ▪ ***FlexSecure TUD Cardmanager*** ▪ ***Eigene Softwareentwicklung:Benutzerschnittstelle „ando", Administrationstools zum Kartenmanagement***	

9. Fristen für die Löschung gem. § 19 Abs. 3 HDSG

Frist für Löschung:	***Die Dienstspezifischen Daten werden bei der Deaktivierung des Dienstes gelöscht und gültige Zertifikate revoziert*** ***Fristen für die Benutzerdaten siehe Verfahrensverzeichnis Identity Management System unter Punkt 9***
(ggfs. unterschiedliche Löschungsfristen für einzelne Datenarten aufführen)	
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände (§ 19 Abs. 3 HDSG)	***Die Daten werden automatisch gelöscht. Eine Kontrolle der Erforderlichkeit der Speicherung von Daten über diesen Zeitraum hinaus ist damit nicht notwendig.***

10. Beabsichtigte Datenübermittlung nach § 17 Abs. 2 HDSG

lfd. Nr. aus Ziffer 3	Empfänger

11. Begründetes Ergebnis der Vorabkontrolle gemäß § 7 Abs. 6 HDSG

Dokumentation der Vorabkontrolle
Durch die Vorabkontrolle nach § 7 Abs. 6 HDSG ist sichergestellt, dass Rechte der informationellen Selbstbestimmung durch das vorliegende Verfahren nicht verletzt werden.

12. Ergänzungen

Wenn der Raum einzelner Spalten nicht ausreicht, sind dort Buchstaben (o. andere Zeichen) einzutragen, die an dieser Stelle näher erläutert werden.

12.1

Die Chipkarte besitzt zwei Prozessoren. Den sichtbaren Kryptoprozessor für die Funktionen Signatur und Verschlüsselung sowie den eingebetteten Funkchip (Typ „Mifare") für die Bezahlfunktion.

Auf dem Kryptoprozessor befinden sich zwei kryptographische Schlüsselpaare sowie zwei Zertifikate. In den Zertifikaten sind Vor- und Nachname, die Dienststellen E-Mail-Adresse gespeichert.

Individuelle, personenbezogene Angaben (in [ ] eckigen Klammern):

- ***Serial Number (eindeutige Seriennummer)***
- ***Validity Not Before (Beginn der Gültigkeit)***
- ***Validity Not After (Ende der Gültigkeit)***
- ***Subject (Inhaber: „C=DE, ST=Hessen, L=Darmstadt, O=Technische Universitaet Darmstadt, OU=[Kürzel der Organisationseinheit des Inhabers], CN=[Vor- und Nachname des Inhabers]"***
- ***X509v3 Subject Alternative Name (Zertifikatserweiterung mit Angabe der Dienststellen E-Mail-Adresse des Inhabers)***
- ***X509v3 Subject Key Identifier***
- ***X509v3 Authority Key Identifier***
- ***RSA Public Key (Angabe und Länge des „public key")***

Technische Angaben (i.d.R. überall gleich):

- ***Version (Versionsnummer zur Struktur des Zertifikates an sich: X509v3)***
- ***Signature Algorithm (Verwendeter Signaturalgorithmus)***
- ***Issuer (Austeller des Zertifikates: „C=DE, ST=Hessen, L=Darmstadt, O=Technische Universitaet Darmstadt, CN=TU Darmstadt Classic CA 01")***
- ***Public Key Algorithm (Verwendeter „public-key" Algorithmus)***
- ***X509v3 Key Usage (Angabe zur Schlüsselverwendung)***
- ***X509v3 Extended Key Usage (Erweiterte Angabe zur Schlüsselverwendung)***
- ***X509v3 Certificate Policies (Lokation der PKI zugrundeliegenden Sicherheitsrichtlinie)***
- ***X509v3 CRL Distribution Points (Lokation der Widerrufsliste)***

Die Bezahlfunktion ist analog zur bisherigen Mensakarte pseudonym. Auf dem Funkchip befinden sich keine personenbezogenen Daten. Folgende Daten sind gespeichert:

- ***auf der Karte aufgedruckte Nummer für die Bezahlfunktion***
- ***aktuelles Guthaben***
- ***letzte Transaktion***
- ***Personenkennziffer (Unterscheidung Studierender, Bedienstete TUD, Bedienstete Studentenwerk Darmstadt)***
- ***Organisationskennziffer (TUD, h_da, usw.)***

Es existiert keine Verknüpfung zwischen den Daten der Kryptofunktion und der Bezahlfunktion.
12.2 ***Die Chipkarten werden von einem Generalunternehmen (Firma Kobil Systems GmbH in Worms) gefertigt und beschlüsselt. Die TUD erhält damit die Karten in einer Form, in der diese sofort an den Bediensteten ausgegeben werden kann. Die Zuordnung einer Karte zu einem Bediensteten erfolgt innerhalb des HRZ. Es werden also für die Produktion keine personenbezogenen Daten an das Generalunternehmen geliefert. Für die Beschlüsselung der Karten und für die Erstellung eines Schlüsselbackups („Key-Backup") wurde eine Vereinbarung zur Auftragsdatenverarbeitung mit Kobil Systems getroffen.***
12.3 ***Die Daten unter Punkt 5.2 stammen aus dem Identity Management System des HRZ. Diese Daten wiederum werden aus der Personalabteilung (SAP/HR) bezogen (siehe Verfahrensverzeichnis Identity Management System).***
12.4 ***Die Prozesse und die Organisation zur TUD Chipkarte sind unter http://www.hrz.tu-darmstadt.de/chipkarte/ dokumentiert.***
12.5 ***Backup: Die Datensicherung wird auf dem TSM (IBM Tivoli Storage Manager) System des HRZ ausgeführt. Die Datensicherung erfolgt einmal täglich. Die Daten werden verschlüsselt übertragen und verschlüsselt gespeichert. Es werden die letzten drei Versionen aufbewahrt. Das System ist revisionssicher, d.h. Daten können nicht unbemerkt gelöscht oder verändert werden. Zugriffsberechtigte Personen im HRZ sind Dr. Norbert Conrad und Dr. Andreas Schönfeld.***

TECHNISCHE UNIVERSITÄT DARMSTADT

HRZ Hochschulrechenzentrum

Verfahrensverzeichnis Identity Management System nach § 6 HDSG

Betrieben durch das Hochschulrechenzentrum der TU Darmstadt

Dokument Version: 1.5 vom 17.09.2008

Technische Universität Darmstadt
Hochschulrechenzentrum
Petersenstraße 30
64287 Darmstadt
Telefon (06151) 16-2054
Telefax (06151) 16-3050

Inhaltsverzeichnis

Verfahrensverzeichnis Identity Management System

lfd. Nr. ☒ neues Verfahren ☐ Änderung

☒ Das Verzeichnis ist zur Einsichtnahme bestimmt (§ 6 Abs. 2 HDSG).

☐ Das Verzeichnis ist nur teilweise zur Einsichtnahme bestimmt.
Ausgenommen sind die Angaben nach § 6 Abs. 1 Satz 1 Ziffern 7, 8 und 11 HDSG.

☐ Das Verzeichnis ist nicht zur Einsichtnahme bestimmt (§ 6 Abs. 2 Satz 2 HDSG).

☐ Das Verfahren ist Teil eines gemeinsamen Verfahrens nach § 15 HDSG.
Federführende Stelle:

1. Name und Anschrift der datenverarbeitenden Stelle

1.1	Name und Anschrift ***Technische Universität Darmstadt, Karolinenplatz 5, 64289 Darmstadt***
1.2	Organisationskennziffer, Amt, Abteilung, ggf. Sachgebiet ***Hochschulrechenzentrum (HRZ), Petersenstr. 30, 64287 Darmstadt***
1.3	Name u. Anschrift des Auftragnehmers, wenn die Daten nach § 4 HDSG in Auftrag verarbeitet werden

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung ***Ganzheitliche Verwaltung von Identitäten, die für die Bereitstellung von IT-Ressourcen des Hochschulrechenzentrums sowie für die notwendigen Mechanismen zur Zugangskontrolle und Zugangsberechtigung benötigt werden.***
2.2	ggf. Bezeichnung des Verfahrens ***Identity Management System (IDM)***
2.3	Rechtsgrundlage (ggf. nach Art der DV unterschieden) ***§ 34 Abs. 1 HDSG***

3. Art der gespeicherten Daten

lfd. Nr.	Herkunft: Datum (SAP bzw. HRZ Datenelementname)	Datum nach § 7 Abs. 4 HDSG	
		Ja	Nein

1	***SAP: Objekt-id (OBJID)***	☐	☒
2	***SAP: Organisationsschlüssel (VDSK1)***	☐	☒
3	***SAP: Objektbezeichnung (STEXT)***	☐	☒
4	***-entfällt-***	☐	☒
5	***-entfällt-***	☐	☒
6	***SAP: Personalnummer (PERNR)***	☐	☒
7	***SAP: Mitarbeitergruppe (PERSG)***	☐	☒
8	***SAP: Mitarbeiterkreis (PERSK)***	☐	☒
9	***SAP: Anredetext (ANREX)***	☐	☒
10	***SAP: Anredeschlüssel (ANRED)***	☐	☒
11	***SAP: Titel (ZZTITEL1)***	☐	☒
12	***SAP: Titel (ZZTITEL2)***	☐	☒
13	***SAP: Titel (ZZTITEL3)***	☐	☒
14	***SAP: Vorname (VORNA)***	☐	☒
15	***SAP: Nachname (NACHN)***	☐	☒
16	***SAP: Vorsatzwort (VORSW)***	☐	☒
17	***SAP: Zusatzwort (NAMZU)***	☐	☒
18	***SAP: Aufbereiteter Name des Mitarbeiters (ENAME)***	☐	☒
19	***HRZ: Name Benutzerkonto (cn)***	☐	☒
20	***HRZ: Name Organisationsobjekt (cn)***	☐	☒
21	***HRZ: E-Mail Adresse (mail)***	☐	☒
22	***HRZ: Telefonnummer (telephoneNumber)***	☐	☒
23	***HRZ: Faxnummer (facsimileNumber)***	☐	☒
24	***HRZ: Mobiltelefonnummer (mobil)***	☐	☒
25	***HRZ: Raum (l)***	☐	☒

4. Kreis der Betroffenen

lfd. Nr.	
1	***Festangestellte Bedienstete***
2	***Privatdozenten und Gastwissenschaftler***
3	***Studierende an der TU Darmstadt***
4	***Externe Mitarbeiter***

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

5.1 Empfänger der Daten

lfd. Nr. aus Ziffer 3	Empfänger der Daten
1-18	***Hochschulrechenzentrum***
19-25	***SAP/HR, Personalverwaltung der Universität Darmstadt, Dezernat III***

5.2 Herkunft der Daten

lfd. Nr. aus Ziffer 3	Herkunft der Daten
1-18	***SAP/HR, Personalverwaltung der Universität Darmstadt, Dezernat III***
19-20	***Hochschulrechenzentrum***
21-25	***Hochschulrechenzentrum oder jeweilige Angabe des Benutzer***

6. Zugriffsberechtigte Personen oder Personengruppen

lfd. Nr.	
1-25	***Diese Personen haben vollen Zugriff auf das System, können anderen Personen Zugriffsrechte erteilen und diesen sowie anderen Personen Zugriffsrechte entziehen: Admistratorengruppe des IDM (Jochen Becker, Markus Borst, Mathias Frohna, Reiner Hoenig)***

7. Technische und organisatorische Maßnahmen (§ 10 Abs. 2 HDSG)

Folgende aufeinander aufbauende Festlegungen wurden getroffen:

☐ Hinsichtlich der allgemeinen Sicherheit wird auf das vorhandene Sicherheitskonzept verwiesen.

☒ Erläuterungen zu den einzelnen Maßnahmen, insbesondere soweit diese das Verfahren betreffen:

Zutrittskontrolle (z.B. EDV-Technik in gesicherten Räumen, Sicherheitsschlösser vorhanden)

EDV-Technik in gesicherten Räumen

Benutzerkontrolle (z.B. Passwortregelungen zur Authentifizierung, automatische Bildschirmsperrung)

Individuelle Authentifizierung aller Berechtigten mit Benutzername und Passwort

Zugriffskontrolle (z.B. Differenzierte Zugriffe auf einzelne Felder, unterschiedliche Berechtigungen)

Berechtigungen in Form von Access Control Lists (ACL) und Rollen

Datenverarbeitungskontrolle (z.B. kein Zugriff auf Betriebssystemebene, Verschlüsselung von Daten)

Austausch der Daten über verschlüsselte Kommunikationswege nach jeweils aktuellem Stand der Technik

Zugriff auf die Daten mit verschlüsselter Übertragung nach jeweils aktuellem Stand der Technik

Kein direkter Zugriff auf Betriebssystemebene (kontrollierte Schnittstellen) nach jeweils aktuellem Stand der Technik

verschlüsseltes Backup nach jeweils aktuellem Stand der Technik (siehe Punkt 12.4)

Verantwortlichkeitskontrolle (z.B. Protokollierung der Dateneingabe, Aufbewahren der Protokolldaten)

Sicherung (Backup) der Datenbank (siehe auch Punkt 12.4)

Audit aller Vorgänge (Anlegen, Ändern und Löschen von Daten)

Die Aufbewahrungsdauer der Protokolldaten und des Backups beträgt ein Jahr (siehe Punkt 12.4)

Auftragskontrolle (z.B. klare Vertragsregelungen mit dem Auftragnehmer, Prüfung der Zuverlässigkeit)

Es findet keine externe Auftragsvergabe statt

Dokumentationskontrolle (z.B. klare und umsetzbare Dokumentation, Überprüfung der Maßnahme)

TUD-interne Betriebsorganisation

Art der ausgetauschten Daten (Datenfeldkatalog), Auflistung von Auswertungen und berechtigte Personen im HRZ sind unter Punkt 6 dokumentiert

Organisationskontrolle (Festlegung klarer Zuständigkeiten und Verantwortlichkeiten)

Der Datenaustausch zwischen dem SAP/HR-System und dem HRZ erfolgt auf der Basis einer Vereinbarung zwischen Personalrat und der Personalabteilung (Dezernat III). Im Anhang „Auswertungen der Personaldaten aus SAP HR" ***sind die zwischen dem HRZ, dem Datenschutzbeauftragten, dem Personalrat und der Personalabteilung vereinbarten Auswertungen dokumentiert.***

8. Technik des Verfahrens

8.1

☐ **Einzelplatzrechner/Arbeitsplatzrechner/Stand Alone PC**

Betriebssystem:

☐ Unix ☐ Windows NT ☐ Windows _____ ☐ anderes _____

weiter mit Ziff. 8.3

8.2

☒ **Vernetzte Rechner**

8.2.1 **Hardware**

☐ Großrechner

Betriebssystem: (z.B. UNIX/OS)

Datenendgerät: ☐ Terminal/Netz-PC (ohne Laufwerk/Festplatte) ☐ PC (Arbeitsplatzrechner/Workstation)

☒ Server

Betriebssystem: (z.B. Windows NT) ***Novell Open Enterprise Server***

Datenendgerät: ☐ Terminal/Netz-PC (ohne Laufwerk/Festplatte) ☒ PC (Arbeitsplatzrechner/Workstation)

☐ Sonstige eingesetzte Hardware (z.B. Chipkarte, Kartenlesegeräte, Videogeräte)

8.2.2 **Netzstruktur**

☒ Netz innerhalb der Behörde (Intranet)

☒ Lan ☐ Intranet ☐ sonstiges

☐ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises (z.B. KIV, KGRZ, Hessische Landesverwaltung)

☐ KIV/KGRZ ☐ Netz der Landesverwaltung (HCN 2000) ☐ sonstiges

☐ Offene Netze (z. B. Internet)

8.2.3 **Datenspeicherung auf:**	**Art der Daten (lfd. Nr. aus Ziffer 3):**
☐ Großrechner	
☒ Server innerhalb der Behörde	***1-25***
☐ Server bei anderen Institutionen	
☐ PC/Arbeitsplatzrechner	

8.3	**Eingesetzte Software** (einschl. Standardverfahren)	Version/Stand/Datum:
	▪ ***Novell Identity Manager*** ▪ ***Novell eDirectory*** ▪ ***Freie Softwaretools zur verschlüsselten Datenübertragung (Authentifizierung und Datenstrom) zwischen VDV und HRZ: „SlavaSoft Optimizing Checksum Utility - fsum 2.51" und „PuTTY Secure File Transfer (SFTP) Client"*** ▪ ***Benutzerschnittstelle „ando"***	

9. Fristen für die Löschung gem. § 19 Abs. 3 HDSG

Frist für Löschung:	***Die Daten 1-5, 7-10, 18, 22-25 werden 3 Monate nach der Löschung aus SAP/HR automatisch gelöscht*** ***Die Daten 6, 11-19, 20, 21 werden ein Jahr länger aufbewahrt und anschließend automatisch gelöscht, sofern keine weitere technische Notwenigkeit besteht***
(ggfs. unterschiedliche Löschungsfristen für einzelne Datenarten aufführen)	
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände (§ 19 Abs. 3 HDSG)	***Die Daten werden automatisch gelöscht. Eine Kontrolle der Erforderlichkeit der Speicherung von Daten über diesen Zeitraum hinaus ist damit nicht notwendig.***

10. Beabsichtigte Datenübermittlung nach § 17 Abs. 2 HDSG

lfd. Nr. aus Ziffer 3	Empfänger

11. Begründetes Ergebnis der Vorabkontrolle gemäß § 7 Abs. 6 HDSG

Dokumentation der Vorabkontrolle
Durch die Vorabkontrolle nach § 7 Abs. 6 HDSG ist sichergestellt, dass Rechte der informationellen Selbstbestimmung durch das vorliegende Verfahren nicht verletzt werden.

12. Ergänzungen

Wenn der Raum einzelner Spalten nicht ausreicht, sind dort Buchstaben (o. andere Zeichen) einzutragen, die an dieser Stelle näher erläutert werden.
12.1 ***Es werden im Sinne der Datensparsamkeit nur die nötigsten Daten verwendet. Der Kreis der zugriffsberechtigten Personen ist stark eingeschränkt.***
12.2 ***Das angestrebte Ziel, Daten in den IT-Systemen des Hochschulrechenzentrums konsistent und aktuell zu halten, kann nur durch einen automatischen Bezug der Daten aus einem führenden System (einer Datenreferenzquelle) erreicht werden.***
12.3 ***Audit-System: Alle Vorgänge im IDM werden im Audit-System gespeichert. Das Audit-System besteht aus Agenten, die Ereignisse aus dem IDM in die Audit-Datenbank schreiben. Zugang zu dieser Datenbank haben die unter Punkt 6 genannten Personen.***
12.4 ***Backup: Die Datensicherung wird auf dem TSM (IBM Tivoli Storage Manager) System des HRZ ausgeführt. Die Datensicherung erfolgt einmal täglich. Die Daten werden verschlüsselt übertragen und verschlüsselt gespeichert. Es werden die letzten drei Versionen aufbewahrt. Das System ist revisionssicher, d.h. Daten können nicht unbemerkt gelöscht oder verändert werden. Zugriffsberechtige Personen im HRZ sind Dr. Norbert Conrad und Dr. Andreas Schönfeld.***
12.5 ***Der Austausch der Personaldaten erfolgt automatisiert.***