Philipps Universität Marburg

Hochschulrechenzentrum (HRZ)

Dienstvereinbarung über den Betrieb eines zentralen Identity & Access Management Systems (IAM) an der Philipps-Universität Marburg (UMR)

Ersteller/in	Manuel Haim
Datum	10.04.2024
Stand	Entwurf 0-1, 04.01.2023, M. Haim Entwurf 0-2, 06.03.2023, M. Haim Entwurf 0-3, 15.02.2024, M. Haim Entwurf 0-4, 27.03.2024, M. Heinrich Entwurf 0-5, 10.04.2024, M. Haim Version/Entwurf <x-y>, Datum, Name
Teilnehmer/innen	<Vorname Nachname>
Unterlagen	<Dateinamen>

§ 1 Gegenstand und Intention

(1) Das Identity & Access Management System (IAM, ehemals IDM) der Philipps-Universität Marburg dient der zentralen und einheitlichen Verwaltung der Identitäten aller Universitätsmitglieder und -angehörigen sowie der ihnen zugeordneten Ressourcen und Zugriffsberechtigungen auf der Grundlage einer konsolidierten und ständig aktuellen Datenbasis. Ziel des Betriebs ist neben der Stärkung der Leistungsfähigkeit und Erhöhung der Servicefreundlichkeit der Universität auch die Erhöhung der Transparenz und Datensicherheit. Dies wird durch die Vereinheitlichung und Automatisierung von Datentransfers sowie durch die Möglichkeit der zentralen Authentifizierung und Autorisierung gegenüber allen von der Universität betriebenen IT-Systemen gewährleistet.

(2) Zum Betrieb des IAM (d.h. zum Gegenstand dieser Dienstvereinbarung) gehören gleichermaßen das administrative Personal, die organisatorischen Prozesse und die unterstützenden IT-Systeme.

(3) Technische Grundlage des IAM ist die vom Hochschulrechenzentrum seit dem Jahr 1995 betriebene und kontinuierlich weiterentwickelte Benutzerverwaltung für Staff- und Students-Accounts. Diese hat mittlerweile einen IAM-typischen Funktionsumfang erreicht und soll künftig vollautomatisiert Daten mit den IT-Systemen der Personalverwaltung abgleichen. Hierzu zählen z.B. der Abruf von Personaldaten wie Name, Vertragszeitraum und Organisationszugehörigkeit sowie auch das Zurückspielen von persönlichen Benutzerattributen wie Account-Name und E-Mail-Adresse.

(4) Diese Dienstvereinbarung definiert Grundsätze für den Betrieb des IAM. Weitere Systeme, die Daten in das IAM einspeisen (Quellsysteme) und Systeme, die Daten aus dem IAM erhalten (Zielsysteme), haben jeweils eigene Begründungen und Grundlagen für ihren Betrieb. Die Dienstvereinbarung regelt die Übernahme von Daten über Mitarbeiterinnen und Mitarbeiter an das IAM sowie Grundsätze für die Speicherung der Daten und für die Weitergabe der Daten an andere Systeme. Darüber hinaus werden Grundsätze getroffen, wie mit dem IAM gearbeitet wird und wie es administriert wird.

§ 2 Geltungsbereich

Diese Dienstvereinbarung gilt für alle Beschäftigten der Philipps-Universität Marburg im Sinne des Hessischen Personalvertretungsgesetzes.

§ 3 Aufgaben und Ziele des IAM

(1) Der im IAM verwaltete Bestand von Personendaten wird aus den IT-Systemen der Personalverwaltung, des Studierendensekretariats sowie aus verschiedenen weiteren Einzel- und Sammel-Meldeverfahren übernommen, die in der Summe sämtliche Universitätsmitglieder und -angehörige abdecken.

(2) Das IAM soll eine Infrastruktur schaffen, die es den Hochschulangehörigen erlaubt, sich gegenüber allen IT-Systemen der Hochschule in einheitlicher Weise zu authentifizieren. Die Möglichkeit der persönlichen Authentifizierung soll u.a. genutzt werden, um Verwaltungsprozesse durch Self-Service-Funktionen zu unterstützen. Darüber hinaus sollen Daten über Personen, die von allgemeinem Interesse sind (z.B. Räume, Telefonnummern, E-Mail-Adressen), die den Personen aber in unterschiedlichen Prozessen und Quellsystemen zugeteilt werden, im IAM zusammengeführt werden.

(3) Mit dem Betrieb des IAM 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 hinsichtlich der Speicherung von Personendaten und hinsichtlich der 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

Die im IAM verarbeiteten Daten werden nicht für Persönlichkeits- und Leistungsprofile der einzelnen Beschäftigten verwendet. Auch die aus Gründen der Datensicherheit gespeicherten Daten werden nicht als Hilfsmittel zur individuellen Leistungs- und Verhaltenskontrolle genutzt. Statistische Auswertungen und Dokumentation sind nur im Rahmen des in § 1 genannten Verwendungszwecks zulässig, oder wenn ein Gesetz dies vorschreibt.

§ 5 Rechte der Beschäftigten

(1) Das Recht der Beschäftigten auf informationelle Selbstbestimmung bleibt gewahrt. Die Beschäftigten werden automatisiert (oder auf Antrag der jeweiligen Dienststelle) mit einem zentralen Benutzerkonto versorgt. Sie erhalten auf Anfrage kostenlos Auskunft über alle zu ihrer Person gespeicherten Daten.

(2) Die Beschäftigten können Berichtigungen bzw. Ergänzungen der gespeicherten Daten verlangen, wenn sich deren Unrichtigkeit bzw. Unvollständigkeit erweist. Die Beschäftigten haben die Personalverantwortlichen zu informieren, wenn ihnen bekannt wird, dass falsche Daten gespeichert oder Daten fehlerhaft verarbeitet wurden.

(3) Die Daten werden gelöscht bzw. gesperrt, wenn ihre Speicherung nicht mehr erforderlich ist und Rechtsvorschriften nicht entgegenstehen.

§ 6 Rechte des Personalrats

Der Personalrat hat das Recht, jederzeit die Einhaltung dieser Dienstvereinbarung zu kontrollieren. Über Änderungen des IAM, insbesondere bei Änderungen der Quell- und Zielsysteme sowie bei Erweiterungen der im IAM verarbeiteten Daten, ist der Personalrat rechtzeitig und umfassend zu informieren und seine Beteiligungsrechte zu wahren. Die Personalräte haben das Recht, unter Hinzuziehung des Datenschutzbeauftragten, Aufklärung und Einsicht in die Funktionsweise des IAM inkl. anonymisierter Systemdaten zu verlangen.

§ 7 Beschreibung und Dokumentation des Systems

Eine detaillierte Beschreibung des IAM ist der jeweils aktuellen, gesetzlich verpflichtenden Dokumentation nach DSGVO zu entnehmen. Ein aktueller Stand ist dieser Dienstvereinbarung als Anlage beigefügt (Verarbeitungsverzeichnis, Sicherheitskonzept).

§ 8 Datenschutz und Datensicherheit

(1) Die Universität ist verpflichtet, personenbezogene Daten gegen Verlust, Ausspähung, Manipulation usw. durch entsprechende Maßnahmen abzusichern.

(2) Der Zugriff auf Protokolldaten ist ausschließlich dem Systembetreiber und den von ihm beauftragten Systemadministratoren sowie dem Datenschutzbeauftragten zur Erfüllung der ihnen obliegenden Aufgaben gestattet. Eingriffe der Systemadministratoren dürfen ausschließlich der Sicherstellung der technischen Funktionalität dienen.

(3) Das in § 7 Abs. 1 genannte Verarbeitungsverzeichnis wird regelmäßig, mindestens im Abstand von 2 Jahren auf seine Aktualität und Gültigkeit überprüft.

§ 9 Anschluss von Quell- und Zielsystemen

(1) Quellsysteme des IAM sind Systeme oder Verzeichnisse, die Daten an das IAM zuliefern. Die Speicherung von Daten muss soweit erfolgen, dass eine Identität vom IAM eindeutig erkannt und zugeordnet werden kann. Nur so lassen sich Dubletten im IAM vermeiden und alle Zielsysteme mit den für sie jeweils notwendigen Daten versorgen.

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

§ 10 Missbrauch

Die Universität ist zur Vermeidung jeglichen Missbrauchs des IAM verpflichtet. Missbräuchlich ist insbesondere die Verwendung von Daten, die entgegen den datenschutzrechtlichen Vorschriften oder durch ungerechtfertigten Eingriff in das Persönlichkeitsrecht erhoben werden. Wird eine missbräuchliche Nutzung festgestellt, ist die Hochschule verpflichtet, die Ursachen dafür umgehend abzustellen und die Personalräte und Datenschutzbeauftragten zu informieren. Besteht ein ausreichend begründeter Verdacht der missbräuchlichen Datenerhebung oder missbräuchlichen Nutzung des IAM, findet unter Beteiligung des Personalrats eine gezielte Überprüfung statt.

§ 11 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.

§ 12 Inkrafttreten

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

(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. Die Bestimmungen dieser Vereinbarung gelten bis zum Abschluss einer neuen Vereinbarung fort.

(3) Änderungen der Vereinbarung bedürfen der Schriftform.

Marburg, den 17.04.24

Für die Dienststelle:

Für den Personalrat:

Anlagen:

Anlage 1: Verarbeitungstätigkeit IDM, Stand 06.03.2023
Anlage 2: Sicherheitskonzept IDM, Stand 30.07.2018