Verfahrensverzeichnis nach § 11 LDSG BW

1 lfd. Nr. ☒ neues Verfahren ☐ Änderung ☐ Löschung

☒ Das Verzeichnis ist zur Einsichtnahme bestimmt (§ 11 Abs. 4 LDSG BW)

☐ Das Verzeichnis ist nicht zur Einsichtnahme bestimmt (§ 11 Abs. 4 Satz 2 LDSG BW)

☐ Das Verfahren ist Teil eines gemeinsamen Verfahrens.
Federführende Stelle:

1. Name und Anschrift der verantwortlichen Stelle

1.1	Name und Anschrift Pädagogische Hochschule Heidelberg Keplerstraße 87 69120 Heidelberg
1.2	Bezeichnung der organisatorischen Untereinheit der Universität, die das Verfahren einsetzt Rechenzentrum
1.2.1	Anschrift der organisatorischen Untereinheit, Ansprechpartner Im Neuenheimer Feld 561, Herr Johannes Peter Moos (Geschäftsführer), Email: moos@ph-heidelberg.de, Tel.: +49 6221 477 282 Fax: +49 6221 477 448
1.3	Name und Anschrift des Auftragnehmers nach § 7 LDSG (Datenverarbeitung im Auftrag): Zentrum für Informations- und Kommunikationstechnologie der PH Freiburg Kunzenweg 21, 79117 Freiburg

2. Bezeichnung des Verfahrens

2.1	Bezeichnung des Verfahrens **Zentrales Identitätsmanagement der PH Heidelberg.** **Kurzbezeichnung: IDM**.
2.2	Erstmaliger Einsatz des Verfahrens *Wird nachgetragen, sobald das System in den Produktivbetrieb geht.*
2.3	Stand der Verfahrensbeschreibung 22.06.2015

3. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

3.1	Zweckbestimmung Das Identitätsmanagement dient der zentralen und einheitlichen Verwaltung der Identitäten und der Berechtigungen zur Nutzung von IT-Dienstleistungen aller Mitglieder und Angehörigen der Hochschule, sowie externer Nutzer. Es dient der Authentifizierung sowie der Bereitstellung und Gewährung von Zugriffsrechten für alle hochschulbezogenen Informations- und Kommunikationssysteme und sichert somit Korrektheit und Aktualität der in diesen Systemen gespeicherten Personen-, Nutzer- und Berechtigungsdaten. Zudem sollen durch das IDM Transparenz Datensicherheit erhöht werden.
3.2	Rechtsgrundlage (ggf. nach Art der DV unterschieden) ☒ §§ 13, 15 LDSG
	☒ § 36 LDSG
	☒ spezielle Rechtsvorschrift
	Hochschulsatzung: „Ordnung zur Einrichtung und zum Betrieb des Identitätsmanagements an der PH Heidelberg“
	☐ Einwilligung

4. Art der gespeicherten Daten

lfd. Nr.		Datum nach § 33 Abs. 1 LDSG, BW	
		Ja	Nein
1	Daten zur eindeutigen Identifizierung einer Person bzw. Identität. Z.B. Name, Vorname, Geburtsdatum, Geburtsort, Email-Adresse, Schlüssel von Identitäten (IDs) in externen angeschlossenen Systemen und intern vom IDM generierte Schlüssel (Matrikelnummer, Personalnummer, Hochschul-ID, Benutzerkennungen).	☐	☒
2	Kontaktdaten (z.B. Email-Adresse, Dienst- und oder Semester-/Heimatanschrift)	☐	☒
3	Daten zur korrekten und zeitlich gesteuerten Zuweisung und Entziehung von Berechtigungen und Ressourcen: Kategorisierte Arten der Hochschulzugehörigkeit und weitere Rollen (Studierende, Beschäftigte, …), sowie deren Status und Dauer, Zugehörigkeiten zu Einrichtungen der Hochschule, Gruppenzugehörigkeiten, Studiengänge, Art des Dienstverhältnisses (Professor, Hilfskraft, …).	☐	☒
4	Daten zu zugewiesenen Ressourcen (z.B. Accounts, Chipkarten, Netzlaufwerke) und zu gewährten Berechtigungen (abhängig von der jeweiligen Zielanwendung).	☐	☒
5	Daten, die für den Betrieb bzw. die Nutzung von angebundenen Zielanwendungen notwendig sind.	☐	☒
6	Prozessdaten und Protokolldaten zur Nachvollziehbarkeit aller im IDM durchgeführten Änderungsvorgänge an Identitätsdaten, Ressourcen- und Berechtigungsdaten.	☐	☒

5. Kreis der Betroffenen

lfd. Nr.	
1	Im IDM erfasste Mitglieder und Angehörige der PH Heidelberg (u.a. Studierende, Beschäftigte).
2	Im IDM erfasste berechtigte externe Nutzer von IT-Diensten der PH Heidelberg (z.B. Gasthörer, Gastdozierende, Gastwissenschaftler, Privatnutzer Bibliothek, etc.).
3	Identitäts- und Ressourcenverwalter, Systemadministratoren

6. Art regelmäßig übermittelter oder genutzter Daten sowie deren Empfänger

6.1	
lfd. Nr. aus Ziffer 4	Empfänger der Daten sowie die jeweiligen Datenarten, wenn vorgesehen ☐ die Daten zu übermitteln ☒ sie innerhalb der öffentlichen Stelle für einen weiteren Zweck zu nutzen ☐ sie im Auftrag verwalten zu lassen
1	An das IDM angeschlossene Zielsysteme.
6.2	
lfd. Nr. aus Ziffer 4	Gruppen vom Empfänger, wenn vorgesehen
	☐ die Daten zu übermitteln ☐ sie innerhalb der öffentlichen Stelle für einen weiteren Zweck zu nutzen ☐ sie im Auftrag verwalten zu lassen

7. Fristen für die Löschung gem. § 23 Abs. 3 LDSG BW und Sperrung gem § 24 LDSG BW

Frist für Löschung:	**Identitätsdaten** Im IDM gespeicherte Daten einer Identität, die ihr Gültigkeitsende erreicht hat, sowie Daten zu ihren mittels IDM verwalteten Ressourcen werden nach 24 Monaten (2 Jahren) gelöscht.
(ggfs. unterschiedliche Löschungsfristen für einzelne Datenarten aufführen)	**Spezielle Identitätsdaten**, die nach einer Löschung (länger als 24 Monate) keiner anderen Identität zugeordnet werden sollen (z.B. IDs, Benutzerkennungen, Emailadressen), werden bei einer Löschung der Identität aus dem IDM ohne Personenbezug als gesperrte Daten mit definierten Zeitpunkt ihrer erneuten Freigabe gespeichert. **Protokolldaten zur IDM Verfahrensdokumentation**, die Nachweise über die Rechteverwaltung zu Identitäten mittels IDM, sowie über die Vergabe und den Entzug von Zugriffsrechten zur Ausführung von Tätigkeiten im IDM (Zuweisung von Admin-Rollen) liefern, werden nach der gesetzlichen Aufbewahrungszeit von 5 Jahren gelöscht (§9 Abs. 3 Nr. 3,4,5 LDSG). **Protokolldaten zum Störfall- und Changemanagement**, d.h. Operating-Logs der eingesetzten Anwendungen und automatisierten Prozesse: Protokolldaten, die Nachweise über den Datenimport aus den Quellsystemen, über vorgenommene Datensicherungen und Rückeinspielungen, sowie über Änderungen am IDM System liefern werden nach der gesetzlichen Aufbewahrungszeit von 2 Wochen gelöscht (§9 Abs. 3 Nr. 2,7,9,10 LDSG).
Frist für die Sperrung	Im IDM gespeicherte Daten einer Identität, die ihr Statusende erreicht hat, werden nach 12 Monaten für Zugriffe durch Identitätsverwaltende Personen gesperrt. Ausnahmen: Einsicht zur Wahrung von Auskunftspflichten in begründeten Fällen, sowie der Registrierungsprozess des IDM zur Ermöglichung der Konsolidierung bei Gleichheit einer wieder eintretenden Identität mit der gesperrten Identität (Reaktivierung).

8. Zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind

lfd. Nr.	
1	Systemadministratoren
2	Identitäts- und Ressourcenverwalter
3	Im IDM registrierte Identitäten (Selbstverwaltungsfunktionen)

9. Technik des Verfahrens, Beschreibung der eingesetzten Hardware, der Vernetzung und der Software

9.1

☐ **nicht vernetzter Einzelplatzrechner / Arbeitsplatzrechner**

Betriebssystem:

☐ Unix ☐ Windows NT ☐ anderes

☐ Windows _____

weiter mit Ziff. 9.3

9.2

☒ **Vernetzte Rechner**

9.2.1 **Hardware**

☐ Großrechner

Betriebssystem: (z. B. UNIX) _____

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

☒ Server

Betriebssystem: (z. B. Windows, Unix, Linux) Linux

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

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

Für die Verbindung zum HSZ wird eine Site to Site VPN eingesetzt

9.2.2 **Netzstruktur**

☒ Netz innerhalb der Universität (Intranet)

☒ Lan ☐ Intranet ☐ sonstiges
☐ Typ und Topologie

☒ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises

☐ ISDN ☒ VPN ☐ sonstiges Für die Verbindung zum HSZ wird eine Site to Site VPN eingesetzt.

☐ Offene Netze (z. B. Internet)

☒ Aktive Netzkomponenten Zentrale Firewall/Routing Komponenten

9.2.3 **Datenspeicherung auf:** **Art der Daten (lfd. Nr. aus Ziffer 4):**

☐ Großrechner

☐ Server innerhalb der Behörde

☒ Server bei anderen Institutionen **Nr. 1 – 6 (Server verortet in Zentrum für Informations- und Kommunikationstechnologie der PH Freiburg)**

☐ PC / Arbeitsplatzrechner

9.3 Eingesetzte Software (einschl. Standardverfahren)	Version/Stand/Datum:
• Linux („Security Enhanced“ Distribution)	2014
• Perl (IDM Core Applikation)	5.16
• VMware (Virtualisierung IDM Core)	
• Apache Webserver (IDM Webschnittstellen)	2.2
• OpenSSH Server	
9.3.1 Sicherheitssoftware	
• Cisco Catalyst 6500 Firewall	
• Site to Site VPN (SSL Tunnel)	
9.3.2 Datenbanksysteme	
• IDM Core DB: Postgresql	9.3
• IDM Audit DB: Postgresql	9.3

10. Technische und organisatorische Maßnahmen (§ 9 Abs. 3 LDSG BW)

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:

1. Zutrittskontrolle

- Daten und Anwendungen liegen auf Servern im Serverraum des Rechenzentrums der PH Freiburg. Fenster zeigen in einen vergitterten Lichthof. Von außen keine Einsicht in den Serverraum.
- Sicherung des Serverraums durch drei Sicherheitsschlösser (ein Schlüssel). Schlüsselinhaber sind namentlich in der zentralen Registratur der PH Freiburg dokumentierte Administratoren des ZIK, Mitarbeiter des technischen Dienstes sowie Hausmeister.
- Endgeräte für die Administration in abschließbaren Räumen, die bei Abwesenheit der Beschäftigten abzuschließen sind.

2. Datenträgerkontrolle

- Medien verbleiben im Serverraum, dort kein weiterer Zugriffsschutz.
- Bei etwaigem Ausschuss an Datenträgern (z.B. Defekt) werden diese physikalisch unbrauchbar gemacht.
- Keine Verwendung von mobilen Datenträgern.

3. Speicherkontrolle

- Datenzugriffe ausschließlich authentisiert mit persönlichem Login und qualifiziertem Passwort (mind. 8 Zeichen, mind. ein Großbuchstabe, eine Ziffer, ein Sonderzeichen).
- Datenzugriffe nur durch autorisierte Benutzer, nach Rollen-basierter Vergabe von Zugriffsrechten.
- Protokollierung aller Daten verändernden Zugriffe und Prozesse samt Benutzerbezug in der Protokolldatenbank des IDM-Systems (IDM Audit) und in Logdateien der Datenbankanwendung.
- Protokollierung der Ausführung von Daten verändernden Prozessen in Logdateien.
- Speicherung von Protokolldaten auf einem separaten System (IDM Audit, Syslog), das IDM Anwendung kann nur Protokolldaten hinzufügen und lesen jedoch nicht verändern oder löschen.
- Regelmäßige Kontrolle und Auswertung der protokollierten Datenänderungen.
- Session-Timeouts bei Webbasierten Zugriffen (IDM Webapplikation).

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

- Authentisierung berechtigter Benutzer über persönlichem Login und qualifiziertem Passwort (mind. 8 Zeichen, mind. ein Großbuchstabe, eine Ziffer, ein Sonderzeichen)
- Autorisierung berechtigter Benutzer durch explizite Vergabe von Administrationsrechten (Rollenbasiertes Berechtigungskonzept).
- Zugriff über die IDM Webschnittstelle ist nur indirekt unter Verwendung vordefinierter Webmasken (Formulare) möglich, zu denen sich Nutzungsberechtigte authentifiziert anmelden müssen.
- Protokollierung von Vergabe und Entzug von Administrationsrechten (IDM Audit).
- Protokollierung der Benutzeranmeldungen (Benutzerkennung, Zeitpunkt) und Speicherung des Benutzerbezugs bei allen protokollierten Zugriffen.
- Persönliche Systemnutzerkonten auf dem IDM System für Systemadministratoren.
- Nutzerkonten für die IDM Applikation in angeschlossenen Systemen, Anwendungen, (Datenbanken).

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

- Differenzierte Zugriffsrechte auf Systeme, Anwendungen und Daten entsprechend Funktion als Systemadministrator oder Verwalter von Identitäten und Ressourcen.
- Rollenbasiertes Berechtigungskonzept zur Zuweisung von Berechtigungen in der IDM-System Anwendung.
- Auf das notwendige Minimum eingeschränkte Zugriffsberechtigungen über Netzwerkschnittstellen der Systeme und Anwendungen durch Regeln in der zentralen Firewall, sowie in den Systemen und Anwendungsschnittstellen.
- Von Personen manuell durchgeführte Verwaltungsvorgänge des ID Managements erfolgen mittels der Webbasierten Schnittstelle des IDM-Systems, authentisiert (persönlicher Account) und autorisiert (IDM Administrationsberechtigungen).
- Regelmäßige Kontrolle und Auswertung der protokollierten Zugriffe auf Systeme und Anwendungen

6. Übermittlungskontrolle

- Die Übermittlung von Daten an das IDM-System aus den Quellsystemen, sowie vom IDM-System an die Zielsysteme wird protokolliert (IDM Audit)
- Datenübertragungen zwischen Systemen erfolgen verschlüsselt sowie mit Authentizitätsprüfung über Zertifikate (DFN-Zertifikate).

7. Eingabekontrolle (z. B. Protokollierung der Dateneingabe, Aufbewahren der Protokolldaten)

- Protokollierung der Abläufe von Daten verarbeitenden Prozessen in Logdateien und Datenbank (IDM Audit).
- Protokollierung aller Eingaben und Änderungen von Daten in einer separaten Datenbank (IDM Audit) mit Bezug zu verantwortlichem Benutzer (Person, Prozess).
- Regelmäßige Kontrolle und Auswertung der protokollierten Datenänderungen.

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

- Die Tätigkeit des Rechenzentrums der PH Heidelberg im Rahmen des IDM ist umfassend in entsprechenden Dokumenten festgelegt, die der zugehörigen Ordnung zur Einrichtung und zum Betrieb des Identitätsmanagements an der PH Heidelberg als Anlage beigefügt sind bzw. mit etwaigen Auftraggebern im Rahmen des Verbundprojektes ausdrücklich vereinbart wurden (Verwaltungsvereinbarungen)

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

- Datenübertragungen erfolgen ausschließlich verschlüsselt (SSL/TLS Verfahren).

10. Verfügbarkeitskontrolle (z. B. Sicherungsmaßnahmen gegen zufällige Zerstörung oder Verlust)

- Geregelte Verfahren für laufende Sicherungen der Datenbanken und Systeme.
- Bereitstehende Standby Systemkopien (Virtualisierte IDM-Systeme).
- Bereitstehende Datenbank Kopien (Datenbank Replikation).
- Nutzung einer unterbrechungsfreien Stromversorgung.

11. Organisationskontrolle (Festlegung klarer Zuständigkeiten und Verantwortlichkeiten)

- Zuständigkeiten und Verantwortlichkeiten für Systemadministration und ID Management definiert und Berechtigungen für ID Management Funktion klar erteilt.
- Administratoren und ID Manager sind zur Einhaltung des Datengeheimnisses angehalten.

11. Begründetes Ergebnis der Vorabkontrolle gemäß § 12 LDSG BW

11.1 Dokumentation der Vorabkontrolle

Rechtmäßigkeit
Als Gestattungsgrundlage für die Erhebung und Verwendung personenbezogener Daten zu Zwecken des Identitätsmanagements liegt ein Datenschutzrechtliches Gutachten der zur Vorabprüfung beauftragten Firma it.sec GmbH & Co. KG vom 16.03.2012 vor.
Rechtsgrundlage für den Betrieb des Identitätsmanagements ist in erster Linie die am 25.07.2015 vom Senat der PH Heidelberg beschlossene Hochschulsatzung „Ordnung zur Einrichtung und zum Betrieb des Identitätsmanagements an der PH Heidelberg“. Ergänzend ergibt sich die Rechtmäßigkeit nach den §§ 13, 15 und 16 LDSG.

Datenminimierung
Für den Betrieb des IDM werden nur die zur Erfüllung der Aufgaben/Ziele erforderlichen personenbezogenen Daten verarbeitet

Betroffenenrechte
Durch die Bereitstellung der IDM Self Management Funktionen werden die Auskunftsrechte der Betroffenen erfüllt. Das vorliegende Löschkonzept gewährleistet die datenschutzgerechte Löschung der Daten.

Sicherheit
Für das IDM liegt ein detailliertes Administrations- und Berechtigungskonzept vor. Die Gefahren für das Recht auf informationelle Selbstbestimmung werden durch technische Maßnahmen ausreichend verhindert.

11.2 ☐ am _____ dem LfD zur Prüfung zugeleitet

☒ am 01.09.2013 dem beh. DSB zur Prüfung zugeleitet

12. Ergänzungen

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