# Richtlinie der Universität zu Lübeck über die Einführung und den Betrieb des Identity Management Systems mit den daran angeschlossenen Quell- und Zielsystemen an der Universität zu Lübeck

**vom 16. August 2016**

Aufgrund des § 22 Absatz 2 Satz 1 des Hochschulgesetzes (HSG) in der Fassung der Bekanntmachung vom 5. Februar 2016 (GVOBl. Schl.-H. S. 39) wird nach Beschlussfassung des Präsidiums vom 15. August 2016 die folgende Richtlinie erlassen:

## Präambel

Das IDM-Gesamtsystem dient der Schaffung und Verwaltung einer konsolidierten und ständig aktuellen Datenbasis für die Verwaltung von Identitäten und Berechtigungen innerhalb der Universität zu Lübeck und soll die Wirksamkeit von Arbeiten der Datenerfassung und des Datenabgleichs mit den angeschlossenen Systemen erhöhen. Ein wesentlicher Bestandteil des IDM-Systems ist das Meta Directory als zentrales Datenverzeichnis.

Die Richtlinie definiert Grundsätze für die Einführung und den Betrieb des Identity Management Systems sowie für den Anschluss von Quellsystemen, die Daten an das Identity Management System übergeben und Zielsystemen, an die Daten vom Identity Management System geliefert werden. Ziel der Einführung des Identity Management Systems ist die Stärkung der Leistungsfähigkeit und Erhöhung der Servicefreundlichkeit der Universität angesichts wachsender Datenmengen und zunehmender Aufgaben durch hinzukommende Anwendungen.

## § 1
## Geltungsbereich

(1) Diese Richtlinie regelt die Bedingungen für Einführung, Betrieb und Weiterentwicklung des IDM-Gesamtsystems an der Universität. Dazu gehören die insgesamt verwendeten Datenfelder bzw. Attribute für die Speicherung, Verarbeitung und Übermittlung personenbezogener Daten.

(2) Sie bezieht sich nicht auf die Einführung und den Betrieb der Systeme, die an das Identity Management System angeschlossen werden. Im Rahmen dieser Richtlinie werden aber Regelungen über eine Dokumentationspflicht dieser angeschlossenen Systeme und der Datenweitergabe an diese getroffen.

## § 2
## Ausschluss der Leistungs- und Verhaltenskontrolle, unbefugter Zugriff

(1) Das Identity Management System wird nicht zur Leistungs- und Verhaltenskontrolle genutzt. Statistische Auswertungen sind ausschließlich anonymisiert zulässig.

(2) Das Identity Management System ist gegen unbefugte Zugriffe von innen und außen zu schützen.

## § 3
## Beschreibung und Dokumentation des Systems

Eine detaillierte Beschreibung des Identity Management Systems ist als Anlage 1 dieser Richtlinie beigefügt.

## § 4
## Aufbau, Änderung und Erweiterung des Systems

(1) Die in der Anlage 1 beschriebenen Daten werden unter anderem vom Personaldatenverarbeitungssystem über einen Konnektor an das Meta Directory übergeben und können von anderen Quell- und Zielsystemen wie hier beschrieben genutzt werden.

(2) Bei der Entwicklung oder wesentlichen Erweiterung von Konnektoren für Quell- und Zielsysteme ist die Inbetriebnahme nur unter Einhaltung der datenschutzrechtlichen Bestimmungen zulässig. Die Anlage 2 der Richtlinie ist so zu gestalten, dass sie die in § 7 Absatz 3 genannten Informationen enthält.

(3) Die Beschäftigten sind zeitnah über wesentliche Änderungen und Erweiterungen zu informieren.

## § 5
## Verarbeitung personenbezogener Daten

Die Universität sichert personenbezogene Daten gegen Verlust, Ausspähung, Manipulation usw. durch entsprechende Maßnahmen. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Personenbezogene Daten dürfen im Identity Management System nur verarbeitet werden, wenn diese Verarbeitung unter Beachtung des Landesdatenschutzgesetzes Schleswig-Holstein in der jeweils geltenden Fassung geregelt ist. Art und Umfang der zu verarbeitenden personenbezogenen Daten ergeben sich aus der Anlage 1.

## § 6
## Datenschutz und Datensicherheit

(1) Durch geeignete technische und organisatorische Maßnahmen ist mit angemessener Sorgfalt und auf Grundlage des an der Universität zu Lübeck gegebenen Standes der Technik gemäß § 5 des Landesdatenschutzgesetzes Schleswig-Holstein sicherzustellen, dass Unbefugte keine Möglichkeit haben, die auf den Datenträgern gespeicherten Daten zu lesen, zu verändern oder zu kopieren.

(2) Der Zugriff auf Protokolldaten ist ausschließlich den Systembetreibern und den von ihnen beauftragten Systemadministratoren, dem Datenschutzbeauftragten und den örtlichen

Personalräten im Rahmen des Landesdatenschutzgesetzes Schleswig-Holstein gestattet. Eingriffe der Systemadministratoren dürfen ausschließlich der Sicherstellung der technischen Funktionalität dienen.

(3) Die Universität ist zur Vermeidung jeglichen Missbrauchs des Identity Management Systems 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. Wird eine missbräuchliche Nutzung festgestellt, ist die Universität verpflichtet, die Ursachen dafür umgehend abzustellen. Besteht ein ausreichend begründeter Verdacht der missbräuchlichen Datenerhebung oder missbräuchlichen Nutzung des IDM-Gesamtsystems, findet eine gezielte Überprüfung statt.

(4) Beschäftigte erhalten auf Anfrage vom Betreiber des IDM-Gesamtsystems Auskunft zu allen dort zu ihrer Person gespeicherten Daten.

## § 7
## Anschluss von Zielsystemen

(1) Zielsysteme des Identity Management Systems sind Systeme oder Verzeichnisse, die das Identity Management System nutzen.

(2) Die Weitergabe von Daten und Zuteilung von Ressourcen oder Berechtigungen müssen dem Grundsatz genügen, dass nur diejenigen Daten übergeben werden, die für die Wahrnehmung der im Rahmen der vereinbarten Zwecke liegenden Ziele des Zielsystems erforderlich sind.

(3) Jedes Zielsystem ist nach dem Muster der Anlage 2 zu beschreiben und zu dokumentieren. Diese Dokumentation enthält folgende Informationen:

1. Grundsätzliche Beschreibung des Systems,
2. Darlegung der Ziele, die mit dem System verfolgt werden,
3. Aufstellung der vom Identity Management System weitergegebenen Datenfelder,
4. Beschreibung, wie das System administriert wird,
5. Beschreibung, wie in dem System Datenschutz garantiert wird,
6. 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.

Eine Übersicht der Zielsysteme befindet sich im IT-Service-Center und kann dort eingesehen werden.

(4) Die Systemadministratoren des IDM-Gesamtsystems und der angeschlossenen Quell- und Zielsysteme müssen in einer am Rechenzentrum geführten Liste erfasst werden.

## § 8
## Löschungsfristen

Die Löschungsfristen richten sich nach den geltenden gesetzlichen, insbesondere datenschutzrechtlichen Bestimmungen.

## § 9
## Inkrafttreten, Laufzeit, Kündigung

Diese Richtlinie tritt am Tage nach ihrer Bekanntmachung in Kraft.

Lübeck, den 16. August 2016

Prof. Dr. Hendrik Lehnert
Präsident der Universität zu Lübeck

**Anlagen:**

- Systembeschreibung und Datenfelder des Identity Management Systems (mit Grundsätzen für ein Sicherheitskonzept) (Anlage 1)
- Musterdokumentation für Zielsysteme des Identity Management Systems (Anlage 2)

**Anlage 1**

**Systembeschreibung und Datenfelder des Identity Management Systems**

# Verfahrensdokumentation über die Identity Management Lösung (FIM 2010 R2) der Universität zu Lübeck

Status: Stand 19.07.2016

| | |
|---|---|
| Version: | 1.1 |
| Datum: | 19.07.2016 |
| Verantwortlich: | Helge Illig<br>Betriebsleiter |


Universität zu Lübeck
IT-Service-Center
Ratzeburger Allee 160
23562 Lübeck

Tel.: +49 451 3101 2000
Fax.: +49 451 3101 2004
E-Mail : illig@itsc.uni-luebeck.de

## Historie der Dokumentversion

| Version | Datum | Autor | Änderungsgrund / Bemerkungen |
|---|---|---|---|
| 1.0 | 17.03.2013 | Czelk | |
| 1.1 | 19.07.2016 | Czelk | Änderungen an der eingesetzten Hardware und Virtualisierungs-Software |
| 1.2. | 28.07.2016 | Drefahl | Anpassungen Felder |

## Inhalt

## 1.0 Ausgangslage

Die Universität zu Lübeck hat zum 20.05.2015 ein neues Identity Managementsystem (IDM) in Betrieb genommen. Dazu wird der Forefront Identity Manager (FIM) 2010 R2 von Microsoft eingesetzt. Mit dem FIM lassen sich Identitäten, Anmeldeinformationen und Rollen-basierte Zugriffsrichtlinien in heterogenen Serversystemen verwalten. Die Identitäten an der Universität zu Lübeck umfassen dabei folgende Personengruppen:

- Mitarbeiter der Universität zu Lübeck
- Mitarbeiter des UKSH mit Lehrauftrag an der Universität zu Lübeck
- Studenten der Universität zu Lübeck

Gemäß § 3 (Absatz 2) der Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutzverordnung – DSVO) muss der ordnungsgemäße Einsatz von Informationstechnik dokumentiert werden (Verfahrensdokumentation).

## 2.0 Rechtsgrundlage

Die Hochschule ist berechtigt personenbezogene Daten von Studierenden zu erheben und zu verarbeiten. Dieses ist in der Landesverordnung zur Erhebung und Verarbeitung Personenbezogener Daten der Studienbewerberinnen, Studienbewerber, Studierenden, Prüfungskandidatinnen und Prüfungskandidaten für Verwaltungszwecke der Hochschule (Stud.-Daten-VO) geregelt.

Die Universität zu Lübeck verarbeitet weiterhin Daten von Mitarbeiter und Lehrbeauftragten der Universität aufgrund von Dienst- und Arbeitsverhältnissen gemäß § 23 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -).

## 3.0 Verfahrenszweck

Die Einführung des FIM 2010 R2 dient dem Zwecke, Benutzer-, Anmelde-Informationen, Rollen- oder Gruppen-basierte Eigenschaften und Zugriffsrichtlinien in der heterogenen IT-Umgebung der Universität zu Lübeck zentral verwalten und verteilen zu können.

## 4.0 Zu verarbeitende Daten

Die im FIM verarbeiteten personenbezogenen Daten haben 3 Quellen, die führend für das System sind. Das bedeutet, dass der Datenfluss nur lesend in Richtung FIM erfolgt. Die Quellen sind:

- HIS-SOS (Hochschul-Informations-System-Studenten-Organisations-System)
- HIS-SVA (Hochschul-Informations-System-Personal-und-Stellenverwaltung)
- Eine Textdatei des UKSH, in der sich durch Komma getrennte Werte befinden

Bis auf die Textdatei des UKSH werden die beiden anderen genannten Systeme bereits seit Dezember 2003 für die Verarbeitung von personenbezogenen Daten an der Hochhochschule verwendet.

Es werden im FIM gemäß § 4 Absatz 1 LDSG und § 11 Absatz 4 LDSG ausschließlich die Daten aus den Quellsystemen verwendet, die für den Verfahrenszweck erforderlich sind.

Folgende Datenfelder werden aus HIS-SOS im FIM verarbeitet:

| **Personenbezogene Daten** | **Beschreibung** |
|---|---|
| Abschlüsse | Angestrebte Abschlüsse |
| Exmatrikulationsdatum | Letztes Exmatrikulationsdatum |
| Geschlecht | Geschlecht des Studenten |
| Immatrikulationsdatum | Erstes Immatrikulationsdatum |
| Matrikelnummer | Matrikelnummer als eindeutiger Schlüssel |
| Nachnamen | Nachnamen |
| Namenszusatz | namenszusatz des Studenten z.B. von, van der, v. etc |
| Sektion | Sektionen |
| Semester | Semesteranzahl für jeden angestrebten Abschluss |
| Studiengänge | Studiengänge |
| Titel | Titel |
| Vornamen | Vornamen |
| PLZ | Postleitzahl der Adresse |
| Ort | Ort der Adresse |
| Adresszusatz | Adresszusatz der Adresse |
| Land | Land der Adresse |

| **Technische Daten** | **Beschreibung** |
|---|---|
| ID Abschluss | Eindeutige Nummer eines Abschlusses |
| ID Studiengang | Eindeutige Nummer eines Studienganges |
| ID Sektion | Eindeutige Nummer einer Sektion |
| Kurzname Abschluss | Abkürzung eines Abschlusses |
| Kurzname Studiengang | Abkürzung eines Studienganges |
| Kurzname Sektion | Abkürzung einer Sektion |
| Langname Abschluss | Anzeigename eines Abschlusses |
| Langname Studiengang | Anzeigename eines Studienganges |

Aus HIS-SVA werden die nachfolgend genannten Daten verwendet:

| **Personenbezogene Daten** | **Beschreibung** |
|---|---|
| Institute | Institute des Beschäftigten |
| Namenszusatz | Namenszusatz des Beschäftigten z.B. von, van der, v. etc. |
| Personalnummer | Interner Identifikator im SVA |
| Austrittsdatum | Letztes Datum des Austritts des Beschäftigten aus der Uni |
| Eintrittsdatum | Erstes Datum des Eintritts des Beschäftigten in die Uni |
| Geschlecht | Geschlecht des Beschäftigten |
| Nachnamen | Nachnamen des Beschäftigten |
| Vornamen | Vorname(n) des Beschäftigten |
| Titel | Akademischer Titel des Beschäftigten |
| Funktion | Funktion z.B. WP, TAP, PROF etc. |

| | |
|---|---|
| Interne Hauspostanschrift | Interne Hauspostanschrift des Mitarbeiters |

| **Technische Daten** | **Beschreibung** |
|---|---|
| ID Institut | Eindeutige Nummer eines Institutes |
| Kurzname Institut | Abkürzung Institut |
| Langname Institut | Anzeigename Institut |
| Kurzname Funktion | Abkürzung einer Funktion |
| Langname Funktion | Anzeigename einer Funktion |

Das UKSH liefert in einer Textdatei folgende Daten:

| **Personenbezogene Daten** | **Beschreibung** |
|---|---|
| Personalnummer | Personalnummer des UKSH als eindeutiger Schlüssel |
| Titel | Akademischer Titel des Beschäftigten |
| Nachnamen | Nachnamen |
| Vornamen | Vornamen |
| Institut | z.B. Klinik für Neurologie etc. |
| UKSH-Emailadresse | Emailadresse |

## 5.0 Aufbewahrungsfristen

Die Benutzerkonten werden automatisch auf nur lesend gesetzt, wenn ein Exmatrikulationsdatum bei Studenten und ein Austrittsdatum bei Mitarbeitern vorliegt oder der Datensatz bei Mitarbeitern des UKSH nicht mehr in der Textdatei vorhanden ist. Ändert sich an dem Status des Benutzers nichts, so erfolgt die Löschung seiner Daten nach 3 Monaten. Der Mitarbeiter erhält zwei Wochen vor Ablauf dieser Frist eine E-Mailbenachrichtigung.

## 6.0 Standort und Informationstechnische Geräte

Die für das Verfahren verwendeten informationstechnischen Geräte befinden sich im Rechenzentrum der Universität zu Lübeck, Ratzeburger Alle 160, Gebäude 64, 1. OG, Raum 36.

Folgende Geräte werden für das Verfahren verwendet:

| **DNS-Name des Servers** | **Gerät** | **Funktion** |
|---|---|---|
| Server01 | IBM System x3550 M3 | Virtualisierungs-Server |
| Server02 | Cisco UCSB-B200-M3 | Virtualisierungs-Server |
| Server03 | IBM System x3550 M3 | Virtualisierungs-Server |
| Server04 | Dell PowerEdge R710 | Virtualisierungs-Server |
| Server05 | Dell PowerEdge R710 | Virtualisierungs-Server |
| Server06 | Cisco UCSB-B200-M3 | Virtualisierungs-Server |
| Server07 | Cisco N20-B6625-1 | Virtualisierungs-Server |
| Server08 | Cisco UCSB-B200-M3 | Virtualisierungs-Server |
| Server09 | Cisco UCSB-B200-M3 | Virtualisierungs-Server |
| Server10 | Cisco UCSB-B200-M3 | Virtualisierungs-Server |
| Server11 | Cisco N20-B6625-1 | Virtualisierungs-Server |
| Server12 | Cisco UCSB-B200-M3 | Virtualisierungs-Server |
| Server13 | Cisco UCSB-B200-M3 | Virtualisierungs-Server |
| Server14 | Cisco UCSB-B200-M3 | Virtualisierungs-Server |

| | | |
|---|---|---|
| Server15 | Cisco UCSB-B200-M3 | Virtualisierungs-Server |
| **DNS-Name** | **Gerät** | **Funktion** |
| Storage01 | Huawei S5500T | Datenspeicher Virtualisierung |
| Storage02 | Huawei S5500 V3 | Datenspeicher Virtualisierung |
| Storage03 | NetApp01, FAS2240-4 | Datenspeicher Backup |

Die aufgezählten Geräte bilden zusammen ein Cluster für die Virtualisierung. Die Server sind mit entsprechenden Aufklebern (DNS-Name) im Rechenzentrum gekennzeichnet.

Das IDM besteht aus zwei virtuellen Servern. Diese werden nachfolgend beschrieben:

| | |
|---|---|
| **Funktion:** | Datenbankserver / FIM Synchronisations-Service |
| **CPU:** | 8 virtuelle CPUs |
| **RAM:** | 16 GB |
| **HD:** | 500 GB |

| | |
|---|---|
| **Funktion:** | FIM-Webportal |
| **CPU:** | 4 virtuelle CPUs |
| **RAM:** | 8 GB |
| **HD:** | 100 GB |

## 7.0 Verwendete Programme, Inbetriebnahme, verantwortliche Personen

Die Virtualisierung erfolgt mittels ESXi, 6.0.0 von VMware. Das IDM besteht aus 2 virtuellen Servern. Der eine Server stellt die Datenbank und die Synchronisations-Engine des IDM zur Verfügung, der andere Server stellt das FIM-Webportal bereit.

Die Datenbank enthält die unter Kapitel 4 genannten personenbezogenen Daten.

Die Synchronisations-Engine befüllt die Datenbank des FIM mit den Daten der Quellsysteme (HIS-SOS, HIS-SVA, Textdatei des UKSH) und ändert, ergänzt oder löscht Datensätze gemäß den Veränderungen im Quellsystem.

Das Portal ermöglicht den Nutzern innerhalb des Universitätsnetzwerkes, ihre im System hinterlegten Daten einzusehen, ihr Benutzerkennwort zurückzusetzen oder zu ändern, eine E-Mail-Weiterleitung einzurichten und eine Nachricht an den Administrator zu senden, damit dieser ggf. Änderungen veranlasst (Namensänderung wegen Heirat etc.). Der Administrator hat darüber hinaus weitere Funktionen. Dazu zählt die Deaktivierung von Accounts, das Zuweisen von Emailverteilern, das Deaktivieren des E-Mail-Accounts. Alle anderen Änderungen, die der Administrator aufgrund einer Benutzernachricht vornehmen soll, kann dieser nur an die Verantwortlichen der Quellsysteme (HIS-SOS, HIS-SVA, UKSH-Textdatei) weiterleiten, damit diese die Änderungen vornehmen. Manuelle Änderungen an der Datenbank des FIM würden bei der nächsten Synchronisation mit den Quellsystemen überschrieben werden.

Nachfolgend werden die verwendeten Programme der beiden Server dokumentiert:

Datenbankserver/FIM Synchronisations-Service

- Microsoft Windows Server 2008 R2
- SQL Server 2008 R2
- FIM 2010 R2 Synchronisations-Service

FIM-Webportalserver

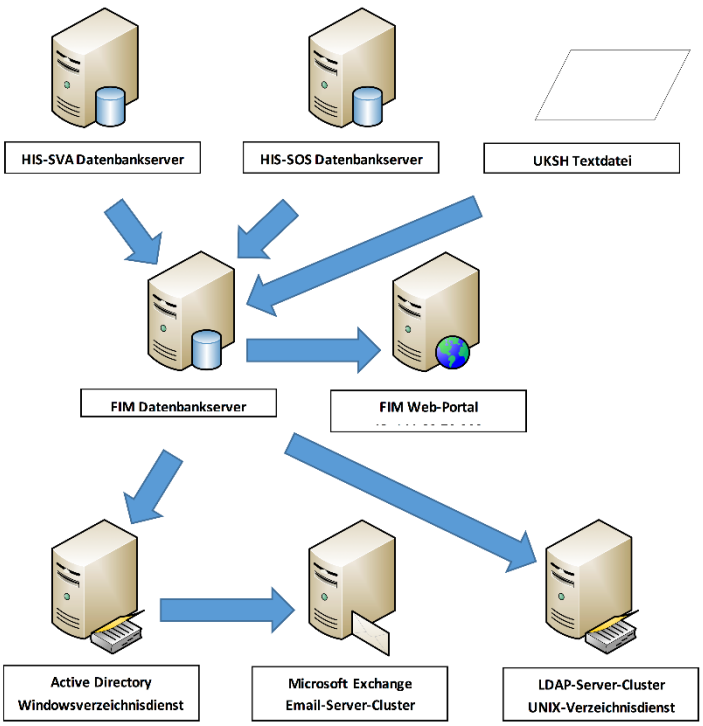
- Microsoft Windows Server 2008 R2 mit Internet Information Services 7
- Microsoft SharePoint Services 2010
- FIM 2010 R2 Portal-Service

Verantwortlich für die Installation sind die folgenden Personen:

| **Name** | **Organisation** |
|---|---|
| Andreas Zemla | Oxford Computer Group GmbH, Gießereistraße 16, 85435 Erding |
| Jörn Schrubbe | Oxford Computer Group GmbH, Gießereistraße 16, 85435 Erding |
| Jens Hannemann | Universität zu Lübeck |
| Martin Behr | Universität zu Lübeck |

## 8.0 Datenflussplan

Das nachfolgende Diagramm zeigt die physikalischen und logischen Verbindungen zu anderen informationstechnischen Geräten sowie die Richtungen des Datenflusses.



## 9.0 Verantwortlichkeit und Datenübermittlung

Das Verfahren wird eigenverantwortlich von der Universität zu Lübeck betrieben. Eine Übermittlung der Daten an andere Stellen erfolgt nicht.

Für den Betrieb der informationstechnischen Geräte des im vorherigen Kapitel dargestellten Netzplans sind folgende Einrichtungen verantwortlich:

HIS-SVA Datenbankserver

- Dateneingabe: Personaldezernat
- Betrieb des Servers: Campus-Management-Team (CMT) des IT-Service-Centers (ITSC)
- Datensicherheit: CMT und die Gruppe Datennetz des ITSC

HIS-SOS Datenbankserver

- Dateneingabe: Studierenden Service Center (SSC)
- Betrieb des Servers: CMT des ITSC
- Datensicherheit: CMT und die Gruppe Datennetz des ITSC

UKSH Textdatei

- Datenbeschaffung: Personaldezernat

FIM Datenbankserver, FIM Web-Portal, Active Directory, Exchange-Server-Cluster, LDAP-Server-Cluster

- Betrieb der Server: Die Gruppe Zentrale Anwender-Server des ITSC
- Datensicherheit: Die Gruppen Zentrale Anwender-Server und Datennetz des ITSC

## 10.0 Sicherheitsmaßnahmen

Das Rechenzentrum ist durch eine elektronische Schließung nur für Mitarbeiter mit Zugangsberechtigung zugänglich. Der administrative Zugriff auf die verwendeten Systeme kann lediglich aus einem Netz, das dem Rechenzentrum zugeordnet ist, erfolgen. Es sind nur bestimmte Computer für den Zugriff zugelassen (Point-to-Point-Verbindung). Weiterhin werden komplexe Passwörter verwendet, um auf die Systeme zugreifen zu können. Die Computer werden an Werktagen täglich überprüft (Logbuch). Sicherheitskritische Updates werden umgehend eingespielt. Weiterhin werden Firewalls eingesetzt, die nur die erforderlichen Ports für die Kommunikation öffnen sowie Angriffe erkennen und abwehren können. Die Datenübertragung zwischen den Systemen erfolgt verschlüsselt.

# Anlage 2

# Musterbeschreibung für Zielsysteme des IDM-Systems

Bei der Anbindung der Zielsysteme wird eine Dokumentation mit den Informationen gemäß § 7 Absatz 3 der Richtlinie nach **folgendem Muster** erstellt und ist im IT-Service-Center einsehbar:

## Zielsystem
## *Titel des Zielsystems/des Projektes*

## 1. Systembeschreibung
*Kurze Beschreibung der Aufgaben des Zielsystems und der Funktion des Zielsystems.*

## 2. Ziele
*Beschreibung des Ziels des Systems.*

## 3. Benötigte Daten
Folgende Daten von Beschäftigten werden durch das Identity Management System im Zielsystem benötigt:

| Nr. | Information | Kurzbeschreibung |
|---|---|---|
| *1.* | *Nachname* | *Identifizierung von Personen und Generierung von Basisdaten, z.B. Mailadresse, Login Name* |
| *2.* | *Vorname(n)* | *Siehe 1.* |
| *...* | *...* | *...* |
| *N.* | *Ablaufdatum* | *Gültigkeit des Benutzerkontos* |

## 4. Administration
*Welche Personen, persönlich benannt, haben Administrationsrechte im Zielsystem*

## 5. Datenschutz
*Maßnahmen zur Verarbeitung von Daten im Zielsystem unter Beachtung der DSVO SH*

## 6. Art der Datenweitergabe und -verwendung
*Werden die Daten im Zielsystem aus dem IDM-System automatisiert oder manuell angepasst? Werden die Daten an Dritte weitergegeben? Sollen Daten aus dem Zielsystem in das IDM-System eingelesen werden?*

Stand: xx.xx.xxxx