– Nur für den internen Dienstgebrauch –

Freie Universität Berlin

FU Directory and Identity Service

– FUDIS –

der ZEDAT

Ablauf des Antragsverfahrens

Fassung: Juli 2009
Version 1.4

Inhalt

1 Vorbemerkung

Der Einsatz eines einheitlichen Identitäts- und Authentifizierungssystems an der Freien Universität ist wünschenswert, weil unnötige Doppelarbeit und Inkonsistenzen bei der Organisation und Pflege von Benutzerkennungen und -verwaltungen vermieden werden. Der Aufwand für Prüfung und Sicherstellung der Datenqualität sowie für die wirksame Vermeidung von Doppeleinträgen ist nur an einer Stelle leistbar. Für Datenschutzbeauftragte und Personalvertretungen ist eine wirksame Kontrolle erheblich einfacher. Den diversen Vorteilen steht allerdings ein erhöhtes Schadensrisiko gegenüber:

- Mit der unberechtigten Nutzung einer fremden Zugangskennung ist ein größerer Schaden anzurichten, da die Zugangskennung Zugriff auf eine größere Anzahl von Systemen bietet.
- Durch eine größere Anzahl teilnehmender Systeme wächst das Risiko, dass eines der Systeme durch Sicherheitslücken zum Ausspähen von Usernamen oder kompletter Zugangskennungen verwendet wird.

Da diese Probleme sich nicht vermeiden lassen, müssen alle Anstrengungen unternommen werden, um das Schadensrisiko so gering wie möglich zu halten. Mit dem Antrag sollen die Verantwortlichkeiten der an FUDIS teilnehmenden IT-Verfahren ermittelt und der Verwendungszweck für die benötigten Daten begründet werden. Daneben müssen sich die Verfahrensverantwortlichen verpflichten, die teilnehmenden IT-Verfahren bzw. die teilnehmenden IT-Systeme ggf. einem Sicherheits-Audit zu unterziehen. Das Audit wird von der dafür zuständigen Stelle in der Freien Universität durchgeführt und orientiert sich an den ISO 27001- bzw. den BSI 100-1, 100-2 und 100-3-Standards. Das Ergebnis des Audits entscheidet maßgeblich über die Teilnahme an dem FUDIS-System.

Außerdem werden verbindliche Regeln aufgestellt und durch Unterschrift bestätigt. Der Antrag kann von dem Verfahrensverantwortlichen des IT-Verfahrens gestellt werden, welches eine Übermittlung von Daten und/oder eine Teilnahme an der Authentifizierung durch den zentralen Dienst FUDIS der ZEDAT benötigt.

Aus Gründen der Einfachheit und des Textflusses wird durchgehend die männliche Anredeform verwendet. Sie soll kein bestimmtes Geschlecht bevorzugen oder benachteiligen.

2 Ablauf des Antragsverfahren

Das Antragsverfahren soll die folgende Grafik veranschaulichen.

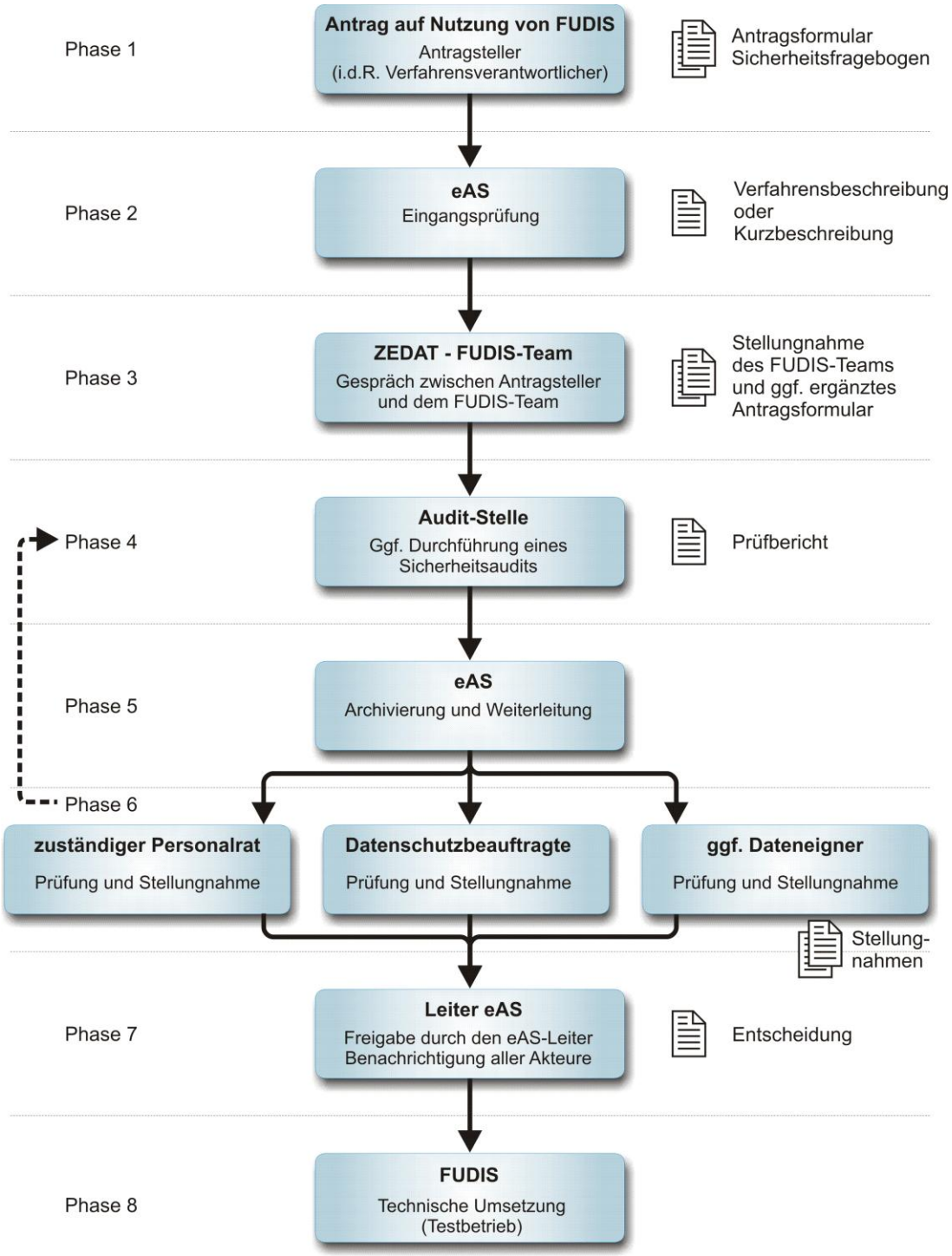

Abbildung 1: Vereinfachte schematische Darstellung des Ablaufs. Auf der rechten Seite wird das (wesentliche) Ergebnis der jeweiligen Phase abgebildet. Der gestrichelte Pfeil soll andeuten, dass entgegen einer ursprünglichen Einschätzung ein Sicherheitsaudit notwendig ist.

Die einzelnen Phasen des Ablaufs werden im Folgenden beschrieben.

2.1 Phase 1 – Antragsstellung

Um die Dienste von FUDIS in Anspruch nehmen zu können, muss das dafür vorgesehene Antragsformular ausgefüllt werden. Zusätzlich ist ein zweiteiliger Fragebogen zu Sicherheitsthemen auszufüllen, der als Grundlage zur Durchführung des Sicherheits-Audits sowie zur Selbsteinschätzung der Sicherheit der anzuschließenden Systeme dient. Darüberhinaus sollen die geforderten Sicherheitsanforderungen als Voraussetzung für den Anschluss aus dem Fragebogen erkennbar werden. Die Beantwortung der Fragen des ersten Teils ist obligatorisch, dass heißt, alle Fragen dieses Teils müssen vom Antragsteller vollständig beantwortet werden. Die Beantwortung der restlichen Fragen ist freiwillig. Der vollständige Fragenkatalog beinhaltet alle Fragen des ggf. später durchzuführenden Sicherheits-Audits und dient somit der Information bzw. der Vorbereitung des Antragsstellers.

Die in dem Antragsformular und dem Fragebogen geforderten Angaben dienen u. a. als Grundlage für das folgende Gespräch mit Vertretern der FUDIS-Gruppe der ZEDAT. Beide Formulare müssen an eAS übermittelt werden.

2.2 Phase 2 – Eingangsprüfung

Bei eAS werden die Angaben in den Formularen geprüft. Bei bestehenden IT-Verfahren werden insbesondere die Angaben zum Verfahren mit den bei eAS archivierten Verfahrensdokumentationen abgeglichen. Bei neuen IT-Verfahren ist entweder eine bereits erstellte vollständige Verfahrensdokumentation oder eine kurze Beschreibung des Verfahrens beizufügen, aus dem mindestens folgende Informationen hervorgehen:

- Zweck des IT-Verfahrens und Zielsetzung
- Angaben über die verarbeiteten Daten
- Angaben zu allen verfahrensrelevanten Rollen
- Angaben über die Anzahl und Art von (geplanten) technischen Einrichtungen und Geräten
- Angaben der Schnittstellen zu anderen IT-Verfahren, IT-Systemen und sonstigen Diensten
- Ggf. Zustimmung des Dateneigners zur Nutzung der Daten
- Angaben über betroffene Bereiche, Aufstellungsort
- Zeitplan mit den wesentlichen Meilensteinen für die Einführung des Verfahrens

Insbesondere müssen alle verantwortlichen Rolleninhaber (Verfahrensverantwortlicher, Personen mit administrativen Rechten usw.) und deren Vertreter mit den vollständigen Kontaktdaten (Name, Dienstadresse, dienstliche Telefonnummer, dienstliche E-Mail-Adresse) angegeben werden. Sind externe Personen (Fremdfirmen) involviert, müssen ebenfalls alle Personen mit einer Zugriffsberechtigung auf die Systeme und/oder Daten mit ihren vollständigen Kontaktdaten angegeben werden.

Auf der Grundlage der vorhandenen Informationen wird von eAS und dem FUDIS-Team der

ZEDAT abgeschätzt, ob ein Sicherheitsaudit durchgeführt werden muss. Bei dieser Abschätzung werden vor allem die Art und der Umfang der beantragten Dienste, die Schutzwürdigkeit der Daten und datenschutzrechtliche Aspekte (z.B. Liegen die Einwilligungen der Betroffenen vor?) geprüft. Das Ergebnis kann in einer der folgenden Kategorien fallen:

- Trivial (z.B. nur Affiliation) ⇨ keine weiteren Anforderungen an Antragsteller
- Normal (z.B. Anforderung der Dienstadresse) ⇨ Selbstauskunft anfordern
- Sicherheitskritisch ⇨ Sicherheitsaudit oder Zertifizierung erforderlich
- Untragbar ⇨ Datenübermittlung bzw. Diensterbringung wird verweigert

Die Formulare werden von eAS anschließend an das FUDIS-Team weitergeleitet.

2.3 Phase 3 – Gespräch mit dem FUDIS-Team

In diesem Gespräch sollen technische und organisatorische Fragen geklärt werden. Unter anderem sollen folgende Aspekte besprochen werden:

- Vollständigkeit der Angaben im Antrag
- Spezifikation der benötigten Daten
- Möglichkeiten der Datenübertragung
- Fragen zur Sicherheit

Ergeben sich aus dem Gespräch weitere Informationen, werden diese dem Antragsformular hinzugefügt. Das Gespräch bildet die wesentliche Grundlage für eine Stellungnahme der FUDIS-Gruppe. Die FUDIS-Gruppe leitet ihre Stellungnahme sowie ggf. die ergänzte Fassung des Antragsformulars an eAS weiter.

2.4 Phase 4 – Ggf. Durchführung eines Sicherheits-Audits

Das im Antrag angegebene IT-Verfahren bzw. die betroffenen IT-Systeme werden entsprechend der Einschätzung in Phase 2 einem Sicherheits-Audit unterzogen. Das Audit wird von der Audit-Stelle der Freien Universität Berlin durchgeführt. Die Datenschutzbeauftragte wird über den vereinbarten Audit-Termin in Kenntnis gesetzt und zu dem Audit eingeladen. Das Ergebnis des Audits wird dokumentiert und an eAS übermittelt.

In Vorbereitung des Auditierungsprozesses muss vom Antragsteller zunächst (bei Antragsstellung; siehe Abschnitt 2.1 Phase 1 – Antragsstellung) ein Fragebogen zu Sicherheitsthemen ausgefüllt werden. Zweck dieser „Vor-Audit-Phase“ ist eine Selbsteinschätzung der Systemsicherheit seitens des Betreibers und stellt eine erste Grundlage für weitere Sicherheitsbetrachtungen dar. Für die eigentliche Prüfung der Systeme sind drei verschiedene Auditphasen vorgesehen.

Vor der erstmaligen Nutzung der FUDIS-Dienste wird ggf. ein Initial-Audit durchgeführt. Ergeben sich bei diesem ersten Audit Mängel an den Systemen bzw. werden Sicherheitslücken aufgedeckt, wird dem Antragsteller eine Frist zur Behebung der erkannten Mängel eingeräumt. Erklärt der Antragsteller, dass nunmehr alle Mängel behoben sind, wird – in Abhän-

gigkeit der Schwere der Mängel – ein Follow-up-Audit durchgeführt, bei dem die beanstandeten Sicherheitsprobleme erneut geprüft werden.

Das Follow-up-Audit wird immer dann durchgeführt, wenn während des ersten Audits schwerwiegende Mängel festgestellt wurden. Das Antragsverfahren wird solange angehalten, bis die Beseitigung der Mängel von der Audit-Stelle festgestellt wurde. Bei kleineren Mängeln kann eine (schriftliche) Erklärung des Antragstellers über deren Beseitigung ausreichen. In diesem Fall läuft das Antragsverfahren weiter. Die Mängel müssen vom Antragsteller bis spätestens vor der Phase 7 – Entscheidung, beseitigt sein. Über die Durchführung eines Follow-up-Audits entscheidet die Audit-Stelle in Abhängigkeit der Schwere der festgestellten Mängel. Einzelheiten zum Ablauf des initialen Audits werden in Kapitel 3 „Kriterienkatalog zum Sicherheits-Audit“ beschrieben.

Alle an FUDIS angeschlossenen Systeme werden in unregelmäßigen Abständen einem Revisions-Audit unterzogen. Die Auswahl der Systeme, die einem Revisions-Audit unterzogen werden, richtet sich zum einen nach dem Zufallsprinzip, zum anderen werden auch Häufungen von Sicherheitsproblemen bei der Auswahl berücksichtigt. Die Betreiber der zur Revision ausgewählten Systeme werden fünf Werktage vor dem Revisions-Audit über dessen Durchführung informiert.

2.5 Phase 5 – Archivierung und Weiterleitung

eAS leitet die Dokumente

- Kurzbeschreibung (im Falle von neuen, noch nicht fertig dokumentierten IT-Verfahren)
- Antrag
- Stellungnahme des FUDIS-Teams
- ggf. Ergebnis des Sicherheits-Audits

an die folgenden Stellen weiter:

- Zuständiger Personalrat (die anderen Personalräte werden über den aktuellen Stand informiert)
- Datenschutzbeauftragte

Wenn ein Sicherheits-Audit durchgeführt wird, wird das Ergebnis auch an das FUDIS-Team der ZEDAT übermittelt. (Die anderen Dokumente sind bereits dem FUDIS-Team bekannt.)

2.6 Phase 6 – Stellungnahme des zuständigen Personalrats, der Datenschutzbeauftragten und ggf. des Dateneigners

Auf Grundlage der überreichten Unterlagen nehmen der zuständige Personalrat und die Datenschutzbeauftragte Stellung. Insbesondere werden von dem Personalrat mitbestimmungsrelevante Aspekte und von der Datenschutzbeauftragten Aspekte des Datenschutzes betrachtet. Falls schützenswerte, insbesondere personenbezogene Daten von FUDIS bezogen

werden sollen, werden die Antragsunterlagen auch an den/die Dateneigner bzw. den betroffenen Verfahrensverantwortlichen mit der Bitte um Stellungnahme weiter geleitet.

Wenn nicht alle Fragen auf Basis der vorhandenen Unterlagen geklärt werden können, besteht die Möglichkeit für die genannten Akteure weitere Auskünfte einzuholen. Die Stellungsnahmen werden innerhalb von 14 Tagen an eAS übermittelt.

Entgegen der in Phase 2 erfolgten Abschätzung über die Notwendigkeit zur Durchführung eines Sicherheitsaudits kann eine prüfende Stelle zu einer abweichenden Beurteilung kommen. In diesem Fall wird über die Durchführung eines Sicherheitsaudits gemeinsam mit dem FUDIS-Team der ZEDAT und der eAS beraten.

2.7 Phase 7 – Entscheidung

Nachdem die Stellungnahmen des FUDIS-Teams, des zuständigen Personalrats, der Datenschutzbeauftragten, ggf. des Dateneigners sowie ggf. das Ergebnis des Sicherheitsaudits vorliegen, wird vom Leiter des Bereichs eAS nach Rücksprache mit dem Leiter der ZEDAT entschieden, ob die FUDIS-Dienste im gewünschten Umfang genutzt werden dürfen. Falls der eAS-Leiter eine Entscheidung nicht herbei führen kann, informiert er das CIO-Gremium. Das CIO-Gremium entscheidet über das weitere Vorgehen. Die Entscheidung wird vom verantwortlichen eAS-Leiter an eAS IT-S übermittelt. eAS IT-S archiviert den Beschluss und informiert alle Akteure.

2.8 Phase 8 – Technische Umsetzung

Im Falle einer positiven Entscheidung schafft das FUDIS-Team der ZEDAT die notwendigen technischen Voraussetzungen zur Nutzung der FUDIS-Dienste. In der Regel wird vor Aufnahme des Routinebetriebs die Funktionsfähigkeit des gewünschten Services zusammen mit dem Antragsteller getestet.

3 Kriterienkatalog zum Sicherheits-Audit

In diesem Kapitel werden die einzelnen Schritte zur Durchführung der Sicherheits-Audits von IT-Systemen beschrieben, die an FUDIS angeschlossen werden sollen.

3.1 Durchführung

Wesentliche Grundlage zur Durchführung der unten beschriebenen Sicherheitsaudits ist die IT-Sicherheitsrichtlinie der Freien Universität Berlin. Die Beachtung bzw. Umsetzung der relevanten IT-Grundschutzmaßnahmen bildet die notwendige Grundlage für den Betrieb aller IT-Systeme an der Freien Universität Berlin. Bei der Durchführung des Audits wird in erster Linie der Grad der Umsetzung der für das betreffende System relevanten Maßnahmen überprüft.

Der Auditierungsprozess umfasst folgende Schritte:

Schritt 1: Der Antragsteller führt eine „Selbstauskunft“ durch

Schritt 2: Die vorhandenen Dokumente werden geprüft

Schritt 3: Das Audit wird beim Antragsteller durchgeführt

Direkter Ansprechpartner für alle durchzuführenden Schritte ist der Verfahrensverantwortliche des FUDIS nutzenden Systems. Dieser hat alle notwendigen Informationen bezüglich der Systeme und Applikationen bereitzustellen.

Schritt 1: Selbstauskunft durch den Antragsteller

In dem Dokument „Audit_Fragenkatalog“ sind alle Fragen enthalten, die im Rahmen des Audit beantwortet bzw. geklärt werden müssen. Die Fragen sind in zwei Gruppen unterteilt. Die Fragen der ersten Gruppe, Kapitel 2 „Grundlegende Fragestellungen (Selbstauskunft)“, behandeln allgemeine Kriterien wie zum Beispiel Typ des Betriebssystems, Aufstellung der Systeme, Verantwortlichkeiten etc. Diese Fragen müssen vom Antragsteller vorab, d.h. vor der Durchführung des eigentlichen Audits, beantwortet werden. In der Regel wird der Verfahrensverantwortliche zusammen mit den entsprechenden Rolleninhabern (Systemadministrator, Applikationsbetreuer usw.) die Fragen bearbeiten. Der vollständig ausgefüllte Fragenkatalog wird dann vom Antragsteller an eAS weitergeleitet. Der Fragenkatalog muss mindestens 5 Werktage vor dem Audit-Termin bei eAS eingegangen sein.

Die Fragen der zweiten Gruppe, Kapitel 3 „Audit“ im Fragenkatalog, beziehen sich auf die einzelnen Grundschutzmaßnahmen und werden im Rahmen des Audit gemeinsam mit den Auditoren und dem Antragsteller sowie dessen Mitarbeiter bearbeitet. Der Antragsteller kann auch die Fragen der zweiten Gruppe ganz oder teilweise vorab beantworten. Im Unterschied zu den Fragen der ersten Gruppe ist die Beantwortung dieser Fragen im Rahmen der Selbstauskunft freiwillig.

Schritt 2: Dokumentenprüfung

In diesem Schritt werden alle vorhandenen Dokumente gesichtet, auf Vollständigkeit überprüft und bewertet, die das an FUDIS anzuschließende System betreffen. Sollte sich in diesem Schritt herausstellen, dass keine Dokumentation vorhanden, falsch oder vollständig veraltet ist, so wird das Sicherheits-Audit nicht durchgeführt. Zusammen mit dem Verfahrensverantwortlichen wird dann ein Zeitraum abgestimmt, in dem die notwendige Dokumentation erstellt werden kann. Danach wird erneut der Schritt 2 „Dokumentenprüfung“ durchgeführt.

Schritt 3: Durchführung des Audit

In diesem Schritt werden u.a. die technischen Angaben verifiziert, die in der Dokumentation zu den anzuschließenden Systemen enthalten sind. Außerdem wird mit Hilfe der Fragen im zweiten Teil des Fragenkatalogs der Umsetzungsgrad der für die anzuschließenden Systeme relevanten Grundschutzmaßnahmen überprüft.

Die Ergebnisse der Dokumentenprüfung und des Audits werden in einem Abschlussbericht zusammengefasst. Auf Basis der Klassifizierungsmatrix der FUDIS-Produkte werden die nicht oder nur teilweise umgesetzten Maßnahmen bewertet und gewichtet. In der Klassifizierungsmatrix sind die Schutzklassen der einzelnen FUDIS-Produkte festgelegt. (Die Klassifizierungsmatrix befindet sich zusammen mit den FUDIS-Produkten im Anhang zum Antrag.) Als Gesamtergebnis wird eine Risikobewertung der an FUDIS anzuschließenden Systeme abgegeben. Darin enthalten sind mögliche Empfehlungen zur Minimierung von evtl. bestehenden Sicherheitsrisiken und in Abstimmung mit dem Antragsteller ggf. zeitliche Fristen für eine Nachprüfung (Follow-up-Audit).