IT-Strategie und IT-Konzept der Fachhochschule Flensburg

Flensburg, den 10.01.2012

Inhaltsverzeichnis

Inhaltsverzeichnis 1

Einleitung ..... **Fehler! Textmarke nicht definiert.**

1 IT-Organisation in der Hochschule 3

1.1 CIO (Chief Information Office) 4

1.2 Zentrale IT-Dienste 4

1.3 Dezentrale IT-Organisationseinheiten 5

1.4 IT-Kooperationen 5

2 Personalplanung, zentraler und dezentraler Einsatz des IT-Personals 6

2.1 IT-Akteure 6

2.2 Beratung und technische Unterstützung 7

2.3 Entwicklung der IT-Fortbildung 7

3 Kernaussagen zum aktuellen IT-Einsatz in Forschung, Lehre und Verwaltung (Ist-Beschreibung). 8

3.1 Vorgehensweise und Organisation von IT-Projekten und IT-Maßnahmen 8

3.2 Wesentliche IT-Dienste in der Hochschule 8

3.2.1 Basisdienste 8

3.2.2 Forschung 9

3.2.3 Lehre 9

3.2.4 Verwaltung 9

3.3 Einsatz 10

3.4 Hochschulinterne oder hochschulübergreifende IT-Standards 10

3.5 IT-Inventarisierung und Lizenzmanagement 10

4 Kernaussagen zur Strategie des zukünftigen IT-Einsatzes in Beziehung zu den Zielen der Hochschule (Soll-Beschreibung) 11

4.1 Strategische Schwerpunkte für die mittel- und langfristige Ausgestaltung des IT-Einsatzes in Forschung, Lehre und Verwaltung 11

4.2 Handlungsfelder / Schwerpunkte der nächsten fünf Jahre 11

4.2.1 Basisdienste 11

4.2.2 Forschung 12

4.2.3 Studium & Lehre 12

4.2.4 Verwaltung 12

5 Kernaussagen zur nachhaltigen Wirtschaftlichkeit von IT-Maßnahmen 14

5.1 Bedarfsplanung und Kosten 14

5.2 Kosten / Nutzen der Maßnahmen 14

5.3 Finanzierungsplan 14

5.4 Berücksichtigung von Folgekosten 15

6 Grundaussagen zur IT-Sicherheit und Verweise auf das Sicherheitskonzept 16
6.1 Klassifikation der Bereiche in Grundschutz oder erweiterten Schutzbedarf 16
6.2 Festlegung der zu schützenden Ressourcen 16
6.3 Berichtspflichten bei Sicherheitsvorfällen 16
6.4 Maßnahmen bei Sicherheitslücken 16
6.5 Festlegung der Dokumentationspflichten 16

Einleitung

Im Rahmen des Sicherheitskonzeptes der Fachhochschule Flensburg wurde in der IT-Sicherheitsrichtlinie festgelegt, dass die Arbeitsgruppe IT-Sicherheit u.a. die IT-Strategie festzulegen hat und dass entsprechende IT-Konzepte aufzustellen sind. Da die Gremien in der Fachhochschule Flensburg noch nicht implementiert wurden, lege ich als Grundlage die nachstehende IT-Strategie sowie das IT-Konzept mit heutigem Stand zur Weiterentwicklung fest.

Flensburg, 10. Januar 2012

Prof. Dr. Herbert Zickfeld
Präsident

10.01.2012 Änderungen:
Ergänzung um Nr. 3.5, Nr. 5, vorherige Nr. 5 wird Nr. 6, Nr. 6.1 neu

Quellen:

- Organisationsrichtlinie der FU Berlin, Juni 2009 (insb. Adaptiert in Abschnitt 1)
- IT-Konzept der Universität Würzburg, Juni 2006
- Sicherheitsrichtlinie der ITSH-edu (insb. in Abschnitt 5), Oktober 2010
- Leitfaden „IT-Konzept / IT-Strategie“ vom 04.10.2011
- DFG Empfehlungen der Kommission für Infrastruktur (2011-2015): http://www.dfg.de/download/pdf/foerderung/programme/wgi/empfehlungen_kfr_2011_2015.pdf

1 IT-Organisation in der Hochschule

Dieser Abschnitt beschreibt die (aktuelle und geplante) IT-Organisation in der Fachhochschule Flensburg und die Zuständigkeiten und Aufgaben der beteiligten IT-Organisationseinheiten und benennt beteiligte IT-Gremien und IT-Akteure (zu den IT-Akteuren s. Abschnitt 2.1). Eine verbindliche Organisationsrichtlinie mit genauen Rollenbeschreibungen wird derzeit erarbeitet.

Um die Zusammenarbeit und Abstimmung zwischen den zentralen und dezentralen IT-Organisationseinheiten zu intensivieren, ist durch das Präsidium der Fachhochschule Flensburg geplant, ein strategisch ausgerichtetes CIO (Chief-Information Office)-Gremiums (s. Abschnitt 1.1) zu gründen. Das Ziel des Gremiums ist wesentlich IT-strategische Fragen gemeinsam und unter Beteiligung der zentralen operativen Einheiten zu diskutieren, festzulegen und umzusetzen.

Ein wesentlicher nächster organisatorischer Schritt ist die stärkere Einbeziehung dezentraler IT-Organisationseinheiten, vor allem der Fachbereiche, hinunter bis auf die Abteilungsebene. Ziel ist es, Strukturen zu etablieren, die IT-Zuständigkeiten in den dezentralen Bereichen *einheitlich* regeln in Bezug auf Rollendefinition, Berichtswesen und IT-Konzept-Abstimmung. Besonders die IT-Akteure sind dezentral nicht einheitlich festgelegt.

IT-Organisationseinheiten und IT-Gremien:

- CIO (Chief Information Office)-Gremium
- Zentraler IT-Servicebereich (Abteilung IT-Services & Network Security)
- Dezentrale IT-Organisationseinheiten

IT-Akteure (s.a. Abschnitt 2.1):

- Zentraler IT-Leiter in der Hochschulverwaltung
- Leiter der Einrichtungen
- IT-Sicherheitsbeauftragte
- IT-Beauftragte
- IT-Verfahrensverantwortliche
- Datenschutzbeauftragte
- IT-Systemadministrator/innen
- IT-Applikationsbetreuer/innen
- IT-Anwenderbetreuer/innen
- IT-Key User/innen
- IT-Anwender/innen
- Personalvertretungen

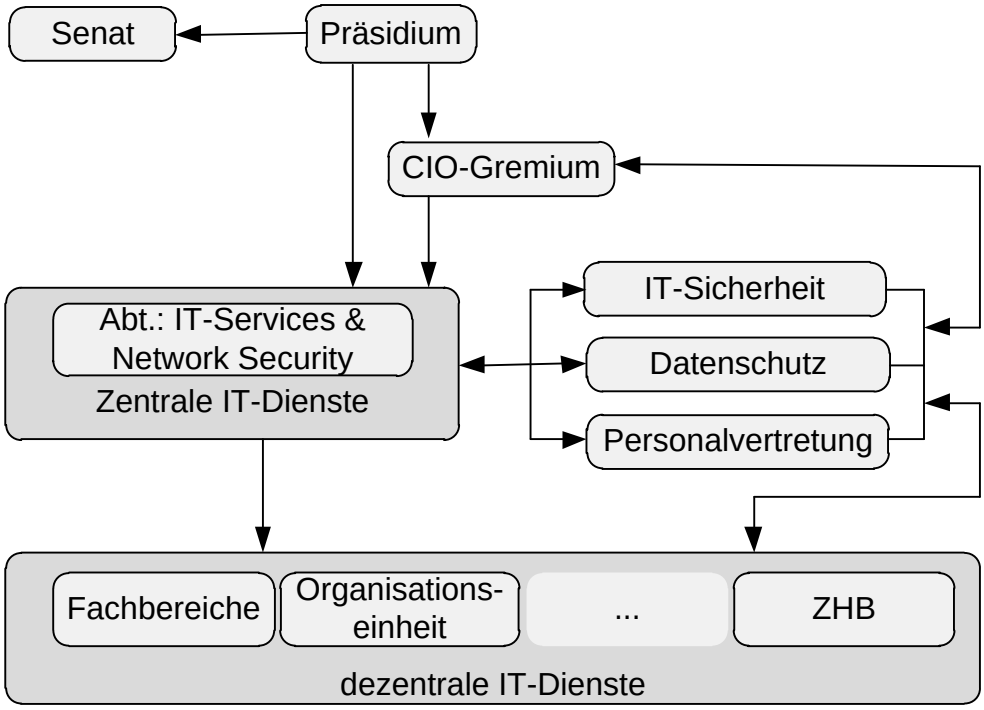

Abb. 1: Darstellung der IT-Organisationsstruktur der Fachhochschule Flensburg.

1.1 CIO (Chief Information Office)

Das Präsidium der Fachhochschule Flensburg plant die Gründung eines CIO-Gremiums.

Das CIO-Gremium soll im Auftrag des Präsidiums die Aufgaben für strategische Informations- und Kommunikations- (IuK) Fragen der Fachhochschule Flensburg wahrnehmen. Geplante Aufgaben des CIO-Gremiums:

- die Erstellung und laufende Fortschreibung einer IuK-Konzeption für die gesamte Hochschule
- Überwachung der Implementierungsprojekte
- Überprüfung dezentraler luK-Planungen und -Entwicklungskonzepte auf Vereinbarkeit mit der zentralen luK-Strategie und deren Genehmigung
- Festlegung von Schnittstellen zwischen verschiedenen Prozessen
- luK-Fragen, die von außen an das Präsidium herangetragen werden (z. B. Ministerien) oder Fragen der regionalen und/oder überregionalen Zusammenarbeit
- Abgabe von Empfehlungen gegenüber den Gremien (Präsidium, Senat) für Beschlüsse zur Umsetzung strategischer Maßnahmen im Rahmen der luK-Strategie.

Das CIO wird vom Präsidium benannt und setzt sich zusammen aus einem Präsidiumsmitglied, dem IT-Sicherheitsbeauftragtem, dem IT-Leiter IT-Services & Network Security, den IT-Beauftragten der Fachbereiche, den Dekanen sowie dem Datenschutzbeauftragten als ständigem Gast. Alle folgenden IT-Einrichtungen und IT-Akteure sind dem CIO gegenüber direkt oder indirekt berichts- bzw. informationspflichtig.

1.2 Zentrale IT-Dienste

Die Abteilung IT-Services & Network Security sorgt für zentrale IT-Infrastrukturen und -dienste im Bereich der Informations- und Kommunikationstechniken und ist verantwortlich für die hard- und

softwaretechnische Bereitstellung und Weiterentwicklung der benötigten IT- und Netzinfrastruktur. Die Abteilung erbringt zentrale Server- und Datensicherungsdienste, Authentifizierungsdienste, PC-Support für die Hochschulverwaltung sowie zentrale Versorgung von eMail und Content-Management.

1.3 Dezentrale IT-Organisationseinheiten

Dezentrale IT-Organisationseinheiten sind jene Bereiche in den Fachbereichen, Organisationseinheiten und der ZHB, die nicht bei den zentralen IT-Servicebereichen angesiedelt sind und die dezentrale IT-Services erbringen. Die Aufgaben und Zuständigkeiten der IT-Akteure in den dezentralen IT-Organisationseinheiten werden in der in Arbeit befindlichen Organisationsrichtlinie beschrieben (s.a. Abschnitt 2.1).

1.4 IT-Kooperationen

Die Abteilung IT-Services & Network Security kooperiert mit dem ZIMT der Universität Flensburg. Es existieren gemeinsame VLANs und WLANs. Ein Internetanschluss beim Provider DFN wird als Cluster genutzt.

Weiterhin ist die Fachhochschule Flensburg vertreten mit dem IT-Leiter der zentralen Organisationseinheit, den IT-Sicherheitsbeauftragten und dem Datenschutzbeauftragtem der anderen Hochschulen des Landes Schleswig-Holstein im ITSH-edu.

2 Personalplanung, zentraler und dezentraler Einsatz des IT-Personals

2.1 IT-Akteure

Über die Rollenbeschreibungen der IT-Akteure in den zentralen und dezentralen Organisationseinheiten werden gleichsam Zuständigkeiten und Aufgaben der einzelnen IT-Akteure geregelt (Details zu Aufgaben, Zuständigkeiten, Berichtsweg und Dokumentationspflicht regelt die Organisationsrichtlinie, die derzeit erstellt wird). Eine Person kann u.U. mehrere Rollen gleichzeitig wahrnehmen.

Zur Verbesserung der Lesbarkeit der folgenden Rollenbeschreibungen wird nur die männliche Form verwendet.

Zentraler Leiter: Der Leiter der zentralen IT-Organisationseinheit trägt die Verantwortung für die Bereitstellung der zentralen IT-Dienste und beteiligt sich über seine Mitgliedschaft im CIO an strategischen IT-Planungen und berichtet dem CIO.

Leiter der Einrichtungen (z.B. Dekane, Professoren): Die Leitung einer Organisationseinheit trägt die Verantwortung für den IT-Einsatz in ihrem Aufgabenbereich und ist zuständig für alle bereichsinternen IT-Planungen sowie für den laufenden internen IT-Betrieb und die Umsetzung hochschulweiter IT-Richtlinien. Die Bereichsleitung kann einen IT-Beauftragten benennen und somit die Umsetzung der IT-Planungen und IT-Richtlinien in ihrem Bereich delegieren.

IT-Beauftragte: Die IT-Beauftragten werden von den Leitern der Einrichtungen bestellt und unterstützen diese in der Umsetzung allgemeiner Richtlinien und Konzepte. Ihnen kommt eine wichtige operative Rolle abseits der zentralen IT-Organisationseinheiten zu.

IT-Verfahrensverantwortliche: Der IT-Verfahrensverantwortliche ist für ein bestimmtes IT-Verfahren verantwortlich und ist i.d.R. in der Fachabteilung angesiedelt, dessen Arbeit durch das Verfahren unterstützt wird (z.B. Zeiterfassung = Personalabteilung). Der IT-Verfahrensverantwortliche arbeitet eng mit dem für das Verfahren zuständigen IT-Administrator zusammen.

IT-Systemadministrator: Der Systemadministrator ist für die Konfiguration und den ordnungsgemäßen Betrieb der IT-Systeme verantwortlich, die in seinem Zuständigkeitsbereich liegen. Er ist auch ganz oder teilweise für die Erstellung und Einhaltung eines Betriebs- und Datensicherungskonzepts zuständig.

IT-Applikationsbetreuer: Der IT-Applikationsbetreuer parametrisiert und konfiguriert Anwendungssoftware und verwaltet festgelegte Benutzerrechte und sorgt für einen reibungslosen Betrieb aus anwendungsbezogener Sicht. Damit stellt die Applikationsbetreuung eine fachliche Ergänzung der Systemadministration dar.

IT-Anwenderbetreuer: Der Anwenderbetreuer installiert und wartet Endgeräte (Arbeitsplatz-IT) inkl. der Administration bestimmter Software wie z.B. Betriebssysteme und Office-Anwendungen und ist erste Anlaufstelle für Endanwender bei IT-Problemen (First-Level-Support). Der Anwenderbetreuer übernimmt auch die weitere Hilfestellung (Problemlösung durch Aktivierung des Second-Level-Supports).

IT-Key-User: IT-Key-User sind Experten für fachliche Anwendung und geben ihre besonderen Kenntnisse als Multiplikatoren an die Anwender weiter und sind erste Ansprechpartner für diese bei aufgabenbezogenen, fachlichen Fragen und Problemen des IT-Einsatzes. IT-Key-User sind Schnittstelle zwischen Anwendern und Applikationsbetreuern und sind eingebunden in die Organisation des Betriebs des jeweiligen Systems.

IT Anwender: IT-Anwender sind Personen, die im Rahmen der ihnen zugewiesenen Berechtigungen die IT-Ressourcen der Fachhochschule Flensburg verantwortlich nutzen.

IT-Sicherheitsbeauftragter: Das Präsidium der Fachhochschule Flensburg beauftragt einen Mitarbeiter mit der Wahrnehmung der Aufgaben des IT-Sicherheitsbeauftragten. Zu den Aufgaben des IT-Sicherheitsbeauftragten gehören, den Sicherheitsprozess zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken, die Leitungsebene bei der Erstellung der IT-Sicherheitsrichtlinie zu unterstützen, die Erstellung der IT-Sicherheitsrichtlinie, des Notfallkonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren. Zur Unterstützung empfiehlt sich die Benennung eines stellvertretenden Sicherheitsbeauftragten.

Datenschutzbeauftragter: Die Fachhochschule Flensburg bestellt einen Datenschutzbeauftragten, der u.a. in allen Fragen des Datenschutzes Informations-, Beratungs- und Kontrollfunktion wahrnimmt und ein Verfahrensverzeichnis zu führen hat. Bestellung und Aufgaben des Datenschutzbeauftragten ist im Landesdatenschutzgesetz Schleswig-Holsteins (LDSG-SH) §10, Behördliche Datenschutzbeauftragte, geregelt. Der Datenschutzbeauftragte ist ständiger Gast im CIO-Gremium.

Personalvertretung: Die Personalräte der Fachhochschule Flensburg werden vor allem bei mitbestimmungspflichten IT-Verfahren mit einbezogen. Die Funktion ist im Mitbestimmungsgesetz Schleswig-Holstein MBG-SH) geregelt.

2.2 Beratung und technische Unterstützung

Für den Aufbau, Ausbau und Betrieb einer bedarfsorientierten Supportstruktur hat die Fachhochschule Flensburg ein Netz aus zentralen und dezentralen Beratungs- und Unterstützungsangeboten, die auf der Ebene der IT-Anwendung sowohl operativer als auch technischer Natur sind. Die Zuständigkeit ergibt sich aus der für ein bestimmtes IT-Verfahren zuständigen IT-Organisationseinheit bzw. zuständigem IT-Akteur (s. Abschnitt 0 und 2.1). Im Bereich des PC-Arbeitsplatzsupports etwa bietet die nächstzuständige IT-Organisationseinheit den First-Level-Support, die nächsthöhere den Second-Level-Support an.

Die zentrale IT-Organisationseinheit bietet Beratung in der Auswahl, der Einführung und der Nutzung von IT-Systemen und ist zuständig für die technische Unterstützung zur Einführung, Umsetzung und Nutzung von zentralen IT-Systemen.

2.3 Entwicklung der IT-Fortbildung

Eine festgeschriebene Integration von IT-Fortbildungen im Rahmen des Personalentwicklungskonzeptes (PE) der Fachhochschule Flensburg sowie die gezieltere Auswahl von Mitarbeitern bei Neuanstellung auch hinsichtlich ihrer IT-Kenntnisse ist aus Sicht der IT-Organisationseinheiten wünschenswert. Hierbei spielt nicht nur die Anwendung von IT-Systemen eine Rolle, sondern auch Aspekte der IT-Sicherheit und des Datenschutzes am Arbeitsplatz.

3 Kernaussagen zum aktuellen IT-Einsatz in Forschung, Lehre und Verwaltung (Ist-Beschreibung)

3.1 Vorgehensweise und Organisation von IT-Projekten und IT-Maßnahmen

Die Vorgehensweise oder Organisation von IT-Projekten und IT-Maßnahmen ist nicht standardisiert, sondern hängt von der jeweiligen Größe des Projektes bzw. der Dimension der Auswirkungen seiner Einführungen ab. Die IT-Projekte, die Auswirkung auf bestehende Arbeitsabläufe oder Änderungen in der Datenhaltung und dem Datenzugriff, speziell bei personenbezogenen Daten haben, werden durch das Präsidium begleitet. Dabei ist darauf zu achten, alle wesentlichen Gruppen, die von der Einführung eines bestimmten Systems betroffen sein werden, mit einzubeziehen, da mit der Einführung eines neuen IT-Systems oft eine Veränderung der Arbeitsprozesse einhergeht. Die Projektorganisation entspricht einer Matrixorganisation mit Personal- und Fachverantwortung. Je nach Größe und Komplexität können externe Experten hinzugezogen werden.

Auswahl
Für die Einführung neuer IT-Systeme wird i.d.R. die zuständige IT-Organisationseinheit beauftragt, Anforderungen zu formulieren und in Frage kommende Systeme zu evaluieren (inkl. Testbestrieb) und dem nächsthöheren Entscheidungsgremium eine Empfehlung auszusprechen.

Entscheidung
Das Präsidium fällt auf Empfehlung der zuständigen IT-Organisationseinheit eine Entscheidung über die Einführung von IT-Systemen bzw. den Start und Umfang von IT-Projekten.

Abschluss
Ein IT-Projekt gilt als abgeschlossen, wenn das neue System im Live-Betrieb ist, alle Nutzergruppe mit dem neuen System arbeitsfähig und evtl. vorher bestehende Systeme vollständig abgelöst sind.

3.2 Wesentliche IT-Dienste in der Hochschule

Die wesentlichen IT-Dienste der Fachhochschule Flensburg werden von der zentralen IT-Organisationseinheit erbracht und dienen der Optimierung des Arbeitsalltags von Studierenden, Wissenschaftlern, Lehrenden und administrativen Mitarbeiter/innen. Die Dienste teilen sich auf in Basisdienste für alle Hochschulangehörigen und zielgruppenspezifische IT-Verfahren für Forschung, Studium & Lehre und Verwaltung.

Entscheidend für alle IT-Dienste und Daten sind Sicherheit, Integrität, Vertraulichkeit, Zuverlässigkeit und hohe Verfügbarkeit. Voraussetzung ist daher ein im Rahmen einer Sicherheitsrichtlinie leistungsstarkes, hochverfügbares, möglichst offenes und sicheres Hochschulnetz mit Zugriff auf die vorhandenen IT-Ressourcen.

3.2.1 Basisdienste

Die wesentlichen Basisdienste werden an der Fachhochschule Flensburg durch die Abteilung IT-Services & Network Security betrieben.

Die Basisdienste beinhalten:

- Netzwerkinfrastruktur und Netzwerkzugang,
- Server- und Archivierungsdienste
- File- und Backup-Dienste (sofern nicht dezentral organisiert)
- Softwareversorgung, insbesondere Campuslizenzen
- Verzeichnisdienst für Rechte- und Rollenmanagement,
- Authentifizierungsdienste
- E-Mail-Server
- Druckdienste für die Hochschulverwaltung
- Content-Management-System (sofern nicht dezentral organisiert)
- IT-Sicherheitsdienste
- PC-Support für die Hochschulverwaltung
- Helpdesk
- eduroam

3.2.2 Forschung

Wissenschaftliches Rechnen **(dezentrale Organisationseinheiten)**

3.2.3 Lehre

Studierendenverwaltung

Anwendungsbereich	**Softwaresystem**
Bewerbung und Zulassung	HISinOne
Immatrikulation, Rückmeldung, Exmatrikulation	SOS-GX, in Vorbereitung HISinOne
Veranstaltungsplanung	Sked, Eigenentwicklung
Prüfungsverwaltung	Eigenentwicklung Prinz, in Vorbereitung HISinOne
Alumni	Eigenentwicklung, in Vorbereitung HISinOne
Lehrevaluation	EvaSys

e-Learning

Anwendungsbereich	**Softwaresystem**
Lernmanagementsystem / Lernplattform	Stud.ip
Virtual Classroom	Videokonferenz
Vorlesungsaufzeichnung / -Streaming	Livestream

3.2.4 Verwaltung

Anwendungsbereich	**Softwaresystem**
Personalmanagement	HIS SVA, Excel
Haushaltsmanagement	SAP
Drittmittel-DB	Excel, SAP
Inventarisierung	SAP, LanDesk, Eigenentwicklung
Gebäudemanagement	HIS BAU
Raummanagement	EIB, Simons & Voss Schliessanlage

3.3 Einsatz

Die Fachabteilung trägt Fachverantwortung und hat i.d.R. eine/n Verfahrensbeauftragte/n sowie eine/n IT-Key-User für das jeweilige Hauptsystem (z.B. SAP), die/der als Schnittstelle zwischen der zentralen IT-Organisationeinheit und den Endnutzern in der Fachabteilung (z.B. Sachbearbeiter/innen in der Haushaltsabteilung) fungiert.

Die zentrale IT-Organisationseinheit stellt die Sicherheit und Verfügbarkeit der IT-Systeme sicher und leistet Support bei Zugriffs- oder technischen Problemen.

Die zentrale IT-Organisationseinheit leistet etwaige notwendige Anpassungen des Systems an die Belange der Fachabteilung, sofern diese Leistung nicht durch Dritte erbracht wird bzw. werden kann.

3.4 Hochschulinterne oder hochschulübergreifende IT-Standards

Derzeit sind diverse Dokumente zur hochschulweiten Definition, Orientierung und Umsetzung von IT-Standards im Entstehungs- und Entscheidungsprozess, Teile davon in einer hochschulübergreifenden Kooperation (ITSH-edu – AG IT-Konzept). Jede Richtlinie muss die Entscheidungs- und Kontrollgremien der Fachhochschule Flensburg durchlaufen (s.a. Abschnitt 0).

Dokument	**Status**
IT-Sicherheitspolitik	fertig
IT-Konzept	fertig
IT-Sicherheitsrichtlinie nach BSI Grundschutz	fertig
IT-Organisationsrichtlinie	in Arbeit
IT-Schutzbedarfsanalyse	In Vorbereitung
IT-Risikoanalyse	in Vorbereitung
Allgemeine Datenschutzrichtlinie	in Vorbereitung
Verfahrensverzeichnis /-beschreibungen	in Arbeit
IT-Betreuungskonzept	in Vorbereitung
IT-Personalentwicklungsrichtlinie	in Vorbereitung
Internet-Nutzungsvereinbarung	fertig

3.5 IT-Inventarisierung und Lizenzmanagement

Für die Inventarisierung wird die Anlagenbuchhaltung des SAP-Verfahrens genutzt.

Um eine einheitliche hochschulweite Inventarisierung zu ermöglichen, wird geprüft, ob das System FRÄDI der Fachhochschule Kiel auch an der Fachhochschule Flensburg eingesetzt werden kann oder eine anderes von der hochschulübergreifenden Arbeitsgruppe ITSH.edu empfohlenes Inventarisierungsverfahren sinnvoller ist.

In der Hochschulverwaltung wird das Lizenzmanagementsystem LANDesk eingesetzt. Der Einsatz eines hochschulweiten Lizenzmanagementsystems wird geprüft.

4 Kernaussagen zur Strategie des zukünftigen IT-Einsatzes in Beziehung zu den Zielen der Hochschule (Soll-Beschreibung)

4.1 Strategische Schwerpunkte für die mittel- und langfristige Ausgestaltung des IT-Einsatzes in Forschung, Lehre und Verwaltung

Die zukünftige IT-Strategie soll sich nicht nur an den Zielen der Hochschule orientieren sondern helfen, diese zu ermöglichen. Dies betrifft insbesondere die Möglichkeiten des vernetzten, kooperativen Arbeitens sowie eines (flexiblen) integrierten Arbeitsplatzes unter ökologisch vernünftigen Rahmenbedingungen. Zentrales Anliegen dabei ist die Verbesserung und Effektivierung der IT-Dienste für Forschung, Studium & Lehre und Verwaltung. Die mittel- und langfristige Ausgestaltung des IT-Einsatzes wird sich auf fünf wesentliche Bereiche konzentrieren:

a. Einbeziehung ökologischer Strategien in das IT-Konzept
b. Zusammenfassung bestehender und zukünftiger IT-Dienste in zielgruppenorientierte Webportale (Studium, Forschung, Verwaltung) und damit integrierter Zugang zu allen spezifischen Diensten und Daten über ein Portal.
c. Ausbau eLearningbasierter Dienste
d. Aufbau eines integrierten Campus-Management-Systems
e. IT-gestützte Optimierung von Abläufen

Aus der Verzahnung dieser Schwerpunkte ergibt sich eine IT-Landschaft, die eine effektive Umsetzung der strategischen Ziele der Fachhochschule Flensburg unterstützt und fördert.

4.2 Handlungsfelder / Schwerpunkte der nächsten fünf Jahre

Auf Basis der breiten Angebotspalette an IT-Diensten wird die Fachhochschule Flensburg in den nächsten Jahren das zielgruppenorientierte Angebot ausbauen und modernisieren. Die wesentlichen Handlungsfelder lassen sich auch hier nach Basisdiensten sowie Diensten für Forschung, Studium & Lehre und Verwaltung kategorisieren.

Neben der Konsolidierung und andauernden Modernisierung der bestehenden IT-Infrastruktur und IT-Dienste sind folgende Schwerpunkte für die nächsten Jahre geplant:

4.2.1 Basisdienste

Handlungsfeld	Beschreibung
Server Virtualisierung Storage Archivierung	Eine virtualisierte Serverumgebung und der Einsatz eines Storage- und Archivierungssystems erlaubt die effektive Nutzung vorhandener Hardware, steigert die Ausfallsicherheit und reduziert den Wartungs- und Energieaufwand. Dies ist in vielen Serverbereichen der Fachhochschule Flensburg sinnvoll umsetzbar.
Webtechnologien	Portale, Webapplikationen, Webservices ermöglichen die Verknüpfung verschiedener Dienste sowie einen integrierten und zusammengefassten Zugang
Cloud Computing	Cloud Computing verbindet Virtualiserung und Webtechnologie zu einer dynamischen und bedarfsorientierten Nutzung der IT-Infrastruktur
IT- und Datensicherheit	Nach den Erfahrungen des Brandes im Rechenzentrum der CAU im Frühjahr 2010 wird versucht, einen zweiten auf dem

	Campus Flensburg gelegenen Serverraum mit allen üblichen Sicherheitsvorkehrungen einzurichten, in dem alle wesentlichen Daten und Dienste gespiegelt werden.
Identity Management (IDM)	Mit Aufbau von HISinOne geplant
EduRoam SSID mit Einschränkung Gast-SSID	Ausbau und Ergänzung des campusweiten WLAN-Einsatzes
Contentmanagement	Ausbau und Ergänzung des Content-Management-System (CMS)

4.2.2 Forschung

Handlungsfeld	Beschreibung
Supercomputing	
Forschungsdaten-management	
Publikations-management	
Forschungsdatenbank	
Drittmittelbewirt-schaftung	*--- in Planung ---*
Webportal für Forschungsdienste	

4.2.3 Studium & Lehre

Handlungsfeld	Beschreibung
Integriertes Campus-Management (mit HISinOne)	Abbildung des Student-Life-Cycles (Bewerbung, Zulassung Immatrikulation, Rückmeldung, Exmatrikulation, Prüfungs- und Veranstaltungsmanagement, Alumni) und Abschaltung aller bisher verwendeten HIS-Module zur Studierendenverwaltung (s.a. Abschnitt 3.2). Die Fachhochschule Flensburg ist Pilotanwender.
Lernmanagement-system	Weiterentwicklung und Anpassung zentralen Lernplattform (stud.ip) sowie Anbindung an IDM und Veranstaltungsmanagement
Studierendenportal	Integration aller für Studierende relevanten Dienste in einem individualisierbarem Portal

4.2.4 Verwaltung

Handlungsfeld	Beschreibung
Workflow- und DMS	in Planung
Report-System	Ergänzung und Weiterentwicklung der SAP-Reports
Inventarisierung	Automatisierte Erfassung von IT-Geräten, SAP Anlagenbuchhaltung
Trennungsrechnung	SAP
Zeiterfassung	campusweite Einführung von Novatime ab August 2011
Zugangskontrolle	Software von Siemens & Voss
Einbruchsicherung	Software Honeywell WINMAGplus ab November 2011
Brandmeldeanlage	Esser ITQ8 Control und Esser Net seit März 2011

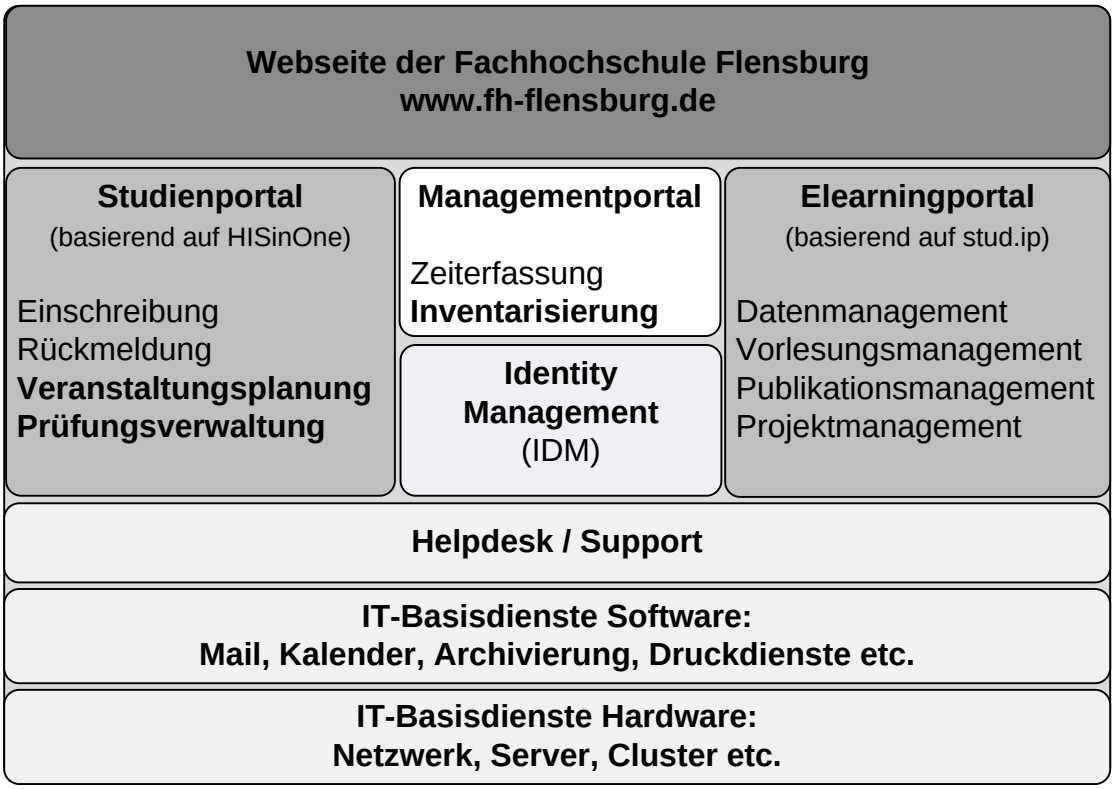

Abb. 2: Überblick zur Planung zukünftiger Dienstbereitstellung über zielgruppenorientierte Portale.

5 Kernaussagen zur nachhaltigen Wirtschaftlichkeit von IT-Maßnahmen

5.1 Bedarfsplanung und Kosten

Alle relevanten IT-Bereiche erstellen eine jährliche, mit Ihrem Zuständigkeitsbereich abgestimmte, Bedarfsplanung für Ersatz und Erweiterungen sowie neue IT-Maßnahmen (s.a. 5.3. Finanzplan). Diese finden sich in den Mittelzuweisungen, z.B. im Rahmen von Zielvereinbarungen, für die Bereiche wieder. Die oberste Instanz für die Mittelzuweisung ist der zentrale Haushalts- und Planungsausschuss (ZHP).
Der Re-Investitionsbedarf orientiert sich an den Empfehlungen der DFG und richtet sich nach der Anzahl der Studierenden/Fachbereich bzw. der Anzahl der zu betreuenden Arbeitsplatzrechner und zu betreuenden Systeme. Bei den Planungen sollte berücksichtigt werden, dass aktive Komponenten der Netze nach circa. 5 Jahren ersetzt werden müssen. Auf Grund der Kurzlebigkeit vieler IT-Systeme ist ein Erneuerungszyklus von 3 – 5 Jahren anzustreben.
Es wird erwartet, dass (hochschulweite) Jahresplanungen Optimierungsstrategien enthalten, die die Steigerungsrate der IT-Kosten senken und zu einem effizienteren Einsatz von IT-Infrastrukturen führen. Maßnahmen können sein: Abbau dezentraler Strukturen, verstärkter Einsatz von Thin-Clients oder Desktopvirtualisierung, Vereinheitlichung bestehender IT-Dienste, Energieeffizienz. Die Optimierungsziele werden von dem CIO-Gremium vorgegeben.
Den Bereichen werden künftig Regeln zur Nachhaltigen IT-Beschaffung in Form einer IT-Planungs- und Projektrichtlinie bereitgestellt, anhand derer zukünftige IT-Planungen abgeglichen und ggfs. geprüft werden können.

5.2 Kosten / Nutzen der Maßnahmen

Alle geplanten Maßnahmen, insbesondere neue und/oder große IT-Maßnahmen werden einer angemessenen Wirtschaftlichkeitsberechnung unterzogen. Diese Betrachtungen sollten eine Gegenüberstellung der einmaligen Kosten (z.B. Lizenzen), des Einführungsaufwands (z.B. Beratung, Installation) und der jährlichen Kosten (Lizenz, Wartung, Support, Hardware, etc.) zu dem erwarteten Ergebnis (in Form von reduziertem Personalaufwand, gestiegener Transparenz, benötigte technologiebedingte Mehrwerte wie Ubiquität und Mobilität, etc.) erbringen. Ergebnis der Abschätzung ist eine Reflektion des Aufwandes mit dem zu erwartenden Nutzen, ggfs. mit einer bezifferbaren Nutzenschwelle (*break-even point*), etwa möglich bei Themen wie dem Umstieg auf Lizenzmodelle wie Microsoft Campus oder der Einführung eines Client-Management -Systems.

5.3 Finanzierungsplan

Finanzierungspläne dienen der nachhaltigen Bewirtschaftung der IT-Maßnahmen. Hierzu sind vergangene Ausgaben für die Vorausplanung zu berücksichtigen, etwa Entwicklung der Hardware- oder Softwarekosten, abschätzbare Steigerungen der Wartungskosten etc.
Finanzierungpläne sind immer unter dem Vorbehalt einer leichten Wachstumsrate zu betrachten. Schwer vorhersagbare Entwicklungen, wie sprunghafte Steigerung der Studierendenzahlen oder ein starker Anstieg von Drittmittelprojekten und damit auch Personalstellen (z.B. Exzellenzinitiative, Hochschulpakt Lehre, etc.) müssen gesondert kalkuliert werden.
Finanzierungpläne sollten folgende Kategorien enthalten: Hardware und Software, Dienstleistung (Wartung / Support), Verbrauchsmittel, Neue Maßnahmen (inkl. 5.2) und Personal.

5.4 Berücksichtigung von Folgekosten

Die in 5.1.-5.3. beschriebenen Maßnahmen müssen Folgekostenkonzepte beinhalten, die insbesondere die Kategorien Stromkosten, Baumaßnahmen, Wartung / Support, Re-Investition und qualifiziertes Personal berücksichtigen. Dabei sind auch bei dezentralen Planungen zentrale Strukturen (zentrale IT-Dienste) und Maßnahmen (z.B. Umweltmanagement) zu berücksichtigen.

6 Grundaussagen zur IT-Sicherheit und Verweise auf das Sicherheitskonzept

Mit der hochschulübergreifenden IT-Sicherheitsrichtlinie, die für die Fachhochschule am 18.11.10 als verbindlich erklärt wurde, werden Grundlagen und Werkzeuge bereitgestellt, mit deren Hilfe die angestrebte Sicherheit gewährleistet und so Schritt für Schritt ein ausreichendes Sicherheitsniveau erreicht werden kann. Dies ist ein kontinuierlicher Prozess, der die konstruktive Zusammenarbeit aller Beteiligten erfordert.

6.1 Klassifikation der Bereiche in Grundschutz oder erweiterten Schutzbedarf

In der IT-Sicherheitsrichtlinie erfolgt eine Klassifikation des Grundschutzes und des erweiterten Schutzbedarfes.

6.2 Festlegung der zu schützenden Ressourcen

Die zu schützenden Ressourcen werden, sofern noch nicht geschehen, anhand der Schutzbedarfsanalyse (IT-Sicherheitsrichtlinie, Kapitel 3) neu festgelegt und bewertet. Jedes IT-Verfahren soll dieser Schutzbedarfsanalyse unterzogen werden, ein Prozess, der für die gesamte Fachhochschule Flensburg (zentral und dezentral) viel Zeit in Anspruch nehmen wird. Die Sicherheitsbedarfsanalyse bezieht alle relevanten Verfahrensbestandteile und Rahmenbedingung mit ein, wie Schutz der Serverräume, Archivierung, Software, Zugangsschutz, etc.

6.3 Berichtspflichten bei Sicherheitsvorfällen

Die Berichtspflicht bei Sicherheitsvorfällen entspricht der in der derzeit in Arbeit befindlichen IT-Organisationsrichtlinie der Fachhochschule Flensburg festgelegten Rollenbeschreibung von IT-Akteuren und deren Berichtspflichten (siehe Abschnitt 2.1). Grundsätzlich ist bei Sicherheitsvorfällen der IT-Sicherheitsbeauftragte der Fachhochschule Flensburg einzuschalten und zu informieren. Im Falle übergeordneter bzw. weitreichender Sicherheitsprobleme, z.B. aufgrund höherer Gewalt, werden das Präsidium und die zentrale IT-Organisationseinheit informiert.

6.4 Maßnahmen bei Sicherheitslücken

Die Feststellung von Sicherheitslücken führt zu einer sofortigen Einleitung geeigneter Schutzmaßnahmen gemäß der IT-Sicherheitsrichtlinie. Details regelt Abschnitt 2.2.2 „Organisation von IT-Sicherheit“ der IT-Sicherheitsrichtlinie.

6.5 Festlegung der Dokumentationspflichten

Die Dokumentationspflicht wird ebenfalls in Abschnitt 2.2.2 der IT-Sicherheitsrichtlinie festgelegt. Dies beinhaltet die Beschreibung von IT-Verfahren, die Dokumentation von IT-Verfahren bezüglich der IT-Sicherheit sowie die Dokumentation von Ereignissen und Fehlern.