IT-Sicherheitspolitik

der teilnehmenden Hochschulen und Forschungseinrichtungen in Schleswig-Holstein

AG IT-Sicherheit

Version 1.3

Stand: 08.Oktober 2010

Teilnehmende Institutionen

Fachhochschule Flensburg

Universität Flensburg

Christian-Albrechts-Universität

IFM-GEOMAR

Fachhochschule Kiel

Muthesius Kunsthochschule

Fachhochschule Lübeck

Universität Lübeck

Musik-Hochschule Lübeck

Fachhochschule Westküste

Inhalt

Präambel

1. Bedeutung der Informations- und Kommunikationstechnik

2. IT-Sicherheitsziele

2.1 Verfügbarkeit der Informations- und Kommunikationstechnik

2.2 Integrität von Daten

2.3 Vertraulichkeit von Daten

2.4 Einhaltung gesetzlicher Auflagen

3. Aufgabenzuordnung

4. IT-Sicherheitsrichtlinie und IT-Maßnahmenkatalog

Präambel

Für die Aufgabenerfüllung von Hochschulen und Forschungseinrichtungen sind Dienstleistungen der Informations- und Kommunikationstechnik (IKT bzw. IT) von zunehmender Bedeutung. Damit nimmt auch die Abhängigkeit dieser von der Funktionstüchtigkeit einer IKT stetig zu. Es ist daher unerlässlich, umfassende Schutzmaßnahmen zu ergreifen. Dieses Papier definiert die IT-Sicherheitspolitik der Hochschulen und Forschungseinrichtungen. Es stellt die Basis für eine IT-Sicherheitsrichtlinie und daraus folgender Maßnahmen für eine schrittweise Verbesserung und dauerhafte Aufrechterhaltung der Sicherheit im Bereich der Informationstechnik dar.

Dabei sollte berücksichtigt werden:

> **Der Aufwand für die IT-Sicherheitsmaßnahmen ist in Relation zu dem erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter zu setzen.**

IT-Sicherheitsziele und Maßnahmen orientieren sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

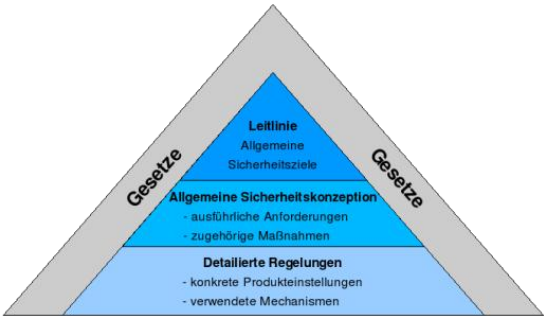
IT-Sicherheit umfasst die Verfügbarkeit, Integrität und Vertraulichkeit von Daten und Anwendungen. Technische Systeme verfügen über eine begrenzte Verfügbarkeit und bieten Möglichkeiten der Manipulation und des Vertraulichkeitsverlustes. Gegen diese Bedrohungen sind geeignete Maßnahmen zu ergreifen.

Aufgrund der Bedeutung der IKT wird die Realisierung und Einhaltung der IT-Sicherheit durch die Präsidien/Direktorien unterstützt.

Die folgenden Ausführungen stecken den Rahmen der IT-Sicherheitspolitik der Hochschulen und Forschungseinrichtungen ab. Die IT-Sicherheitspolitik ist die Basis für die IT-Sicherheitsrichtlinie, welche Detailmaßnahmen beschreibt. Bei dauernd wechselnden Gefährdungen ist die Aufrechterhaltung der IT-Sicherheit eine permanente Aufgabe. Dieses erfordert personelle und finanzielle Mittel und die Mitwirkung jedes Einzelnen.

Die Geltungsdauer dieses und der folgenden Dokumente beträgt:

- IT-Sicherheitspolitik (10 Jahre)
- IT-Sicherheitsrichtlinie (5 Jahre)
- IT-Organisationsrichtlinie (individuell je Institution)



Quelle: BSI

2. Bedeutung der Informations- und Kommunikationstechnik

Die Informations- und Kommunikationstechnik ist von zentraler Bedeutung für die Aufgabenerfüllung der Hochschulen und Forschungseinrichtungen. Das Spektrum der IT-Anwendungen umfasst die rechnergestützte Informationsverarbeitung für Forschung, Lehre, Studium und Verwaltung sowie die Kommunikation mit externen Partnern und Auftraggebern. Die Bedeutung der Informationstechnik für die unterschiedlichen Anwendungsgebiete ist unterschiedlich hoch. Dementsprechend sind die Auswirkungen von Störungen oder Ausfällen in den verschiedenen Anwendungsgebieten von unterschiedlicher Tragweite.

3. IT-Sicherheitsziele

Lösungen zur Erreichung von Sicherheitszielen sollen das Restrisiko verkleinern, müssen angemessen und wirtschaftlich vertretbar sein.

3.1. Verfügbarkeit der Informations- und Kommunikationstechnik

Technische Systeme besitzen eine begrenzte Verfügbarkeit. Dabei ist organisatorisch festzulegen, welche Ausfallzeiten akzeptabel und unter dem Gesichtspunkt der Wirtschaftlichkeit vertretbar sind. In Abhängigkeit dieser Forderungen sind geeignete Maßnahmen zu ergreifen, die in den akzeptierten zeitlichen Grenzen einen Wiederanlauf ermöglichen. Daten sind in mehrstufigen Verfahren so zu sichern, damit nach menschlichem Ermessen ein grundsätzlicher Verlust ausgeschlossen werden kann.

3.2. Integrität von Daten

Unbefugte oder unbemerkte Veränderungen von Daten sollen ausgeschlossen sein, sei es durch Personen oder technische Fehler. Es wird erwartet, dass Daten weder irrtümlich noch mutwillig manipuliert werden. Je nach Anwendung sind deshalb geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Integrität von Daten zu erhalten.

3.3. Vertraulichkeit von Daten

Die Hochschulen und Forschungseinrichtungen verarbeiteten unterschiedlichste vertrauliche Informationen. Da nicht ausgeschlossen ist, dass auf die Daten unberechtigt zugegriffen wird, müssen geeignete technische, organisatorische und personelle Maßnahmen in den Anwendungen, dem IT-Netz, den Arbeitsplatzcomputern und auf den Übertragungswegen ergriffen werden, die einen möglichst effektiven Zugriffsschutz bewirken.

3.4. Einhaltung gesetzlicher Auflagen

Die Hochschulen und Forschungseinrichtungen haben eine Vielzahl gesetzlicher Auflagen wie Datenschutz, Arbeitssicherheit, etc. zu erfüllen. IT-Systeme und die dazu erlassenen organisatorischen Regelungen müssen so ausgelegt sein, dass die gesetzlichen Bestimmungen eingehalten werden.

4. Aufgabenzuordnung

4.1 IT-Sicherheitsbeauftragte

Die Gesamtverantwortung für die IT-Sicherheit liegt bei dem Präsidium/Direktorium.

Diese bestellt einen IT-Sicherheitsbeauftragten und stellt ihm die erforderlichen Ressourcen und Befugnisse zur Verfügung.

Der IT-Sicherheitsbeauftragte ist dafür zuständig, dass die in dieser IT-Sicherheits-Politik benannten Ziele umgesetzt werden. Er sorgt dafür, dass angemessene IT-Sicherheitsmaßnahmen realisiert, fortentwickelt und überwacht werden.

Sich hieraus ergebende Regeln sind für alle Nutzer der IT-Infrastruktur verbindlich.

4.2 Datenschutzbeauftragter

Das Präsidium/Direktorium bestellt einen Datenschutzbeauftragten und stellt ihm die erforderlichen Ressourcen und Befugnisse zur Verfügung.

Ein Datenschutzbeauftragter muss bestellt werden, wenn personenbezogene Daten (z. B. Arbeitnehmerdaten in der Personalabteilung, Kunden- und Interessentendaten) automatisiert verarbeitet werden.

4.3 Geltungsbereich

Jeder Benutzer der Informations- und Kommunikationstechnik ist für die Sicherheit und den Schutz der Daten in seinem Verantwortungsbereich verantwortlich. Alle Angehörigen der Hochschulen und Forschungseinrichtungen sind verpflichtet, bei der Erfüllung der Aufgabe „IT-Sicherheit“ kooperativ und verantwortungsbewusst mitzuwirken.

5. IT-Sicherheitsrichtlinie und IT-Maßnahmenkatalog

Der IT-Sicherheitsbeauftragte sorgt in Kooperation mit der AG IT-Sicherheit der teilnehmenden Institutionen für die Erstellung und Pflege der IT-Sicherheitsrichtlinie und Umsetzung der dort aufgeführten Maßnahmenkataloge.