IT-Sicherheitsleitlinie

der teilnehmenden
Hochschulen und wissenschaftlichen Einrichtungen
in Schleswig-Holstein

AG IT-Sicherheit

Version 2.0.0

Stand: November 2019

Ausfertigung für die Fachhochschule Kiel

mit Präsidiumsbeschluss der Fachhochschule Kiel vom 20.11.2019


C A U
Christian-Albrechts-Universität zu Kiel


Europa-Universität
Flensburg


Fachhochschule Kiel
Hochschule für Angewandte Wissenschaften


FH Westküste
Wirtschaft und Technik


FHVD
Fachhochschule für Verwaltung
und Dienstleistung


Forschungszentrum Borstel
Leibniz Lungenzentrum


GEOMAR


Helmholtz-Zentrum
Geesthacht
Zentrum für Material- und Küstenforschung


Hochschule
Flensburg
University of
Applied Sciences


ifw
KIEL INSTITUT FÜR
WELTWIRTSCHAFT


musik
hochschule
lübeck


muthesius
kunsthochschule


STUDENTENWERK SH
Wir sind dein Rückenwind


TECHNISCHE
HOCHSCHULE
LÜBECK


UNIVERSITÄT ZU LÜBECK


ZBW
Leibniz-Informationszentrum
Wirtschaft
Leibniz Information Centre
for Economics

Inhaltsverzeichnis

1. Präambel

„Informationssicherheit hat das Ziel, Informationen jeglicher Art und Herkunft zu schützen. Dabei können Informationen auf Papier, in IT-Systemen oder auch in den Köpfen der Benutzer gespeichert sein. IT-Sicherheit als Teilmenge der Informationssicherheit konzentriert sich auf den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.[1]“

In Abgrenzung gegenüber gängigen Standards wie dem BSI-Standard 200-1 „Managementsysteme für Informationssicherheit (ISMS)“ oder der DIN EN ISO/IEC 27001 beschränkt sich diese Leitlinie explizit auf IT-Sicherheit, also den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.

Das vorliegende Dokument wurde von der *Arbeitsgruppe IT-Sicherheit* der oben aufgeführten Hochschulen und wissenschaftlichen Einrichtungen im Land Schleswig-Holstein erstellt. Die *AG IT-Sicherheit* setzt sich aus Mitgliedern der landesweiten Arbeitsgemeinschaft *ITSH-edu* zusammen. In dieser Arbeitsgemeinschaft sind die IT-Beauftragten der staatlichen Hochschulen und wissenschaftlichen Einrichtungen in Schleswig-Holstein vertreten.

Die vorliegende Fassung ersetzt die ITSH-edu IT-Sicherheits*politik* in der Version 1.3 vom 08. Oktober 2010. Sie basiert in wesentlichen Teilen auf dem Papier „Bedeutung der IT-Sicherheit an wissenschaftlichen Einrichtungen“ der Allianz der Wissenschaftsorganisationen[2]. Zielsetzung ist eine schrittweise Verbesserung und dauerhafte Aufrechterhaltung der IT-Sicherheit.

[1] Auszug aus Abschnitt 2 des BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS).

[2] Das Papier wurde im Oktober/November 2014 an die Leitungen der Einrichtungen verteilt.

2. Steckbrief

Dokumenten-Klasse:	Leitlinie
Dokumententitel:	IT-Sicherheitsleitlinie
Dokumentennummer:	2019.2.0
Zielsetzung:	Definition und Aufrechterhaltung der IT-Sicherheit
Geltungsbereich:	Alle Nutzerinnen und Nutzer der IT der Einrichtung
Verantwortlicher:	Leitung der Einrichtung
Letzte Bearbeitung:	04.11.2019
Gültigkeitsdauer:	10 Jahre

3. Bedeutung der IT-Sicherheit an wissenschaftlichen Einrichtungen

Für die Arbeit an wissenschaftlichen Einrichtungen sind Dienstleistungen der Informations- und Kommunikationstechnik (IKT bzw. IT) von existentieller Bedeutung. Damit ist die Abhängigkeit von der Funktionstüchtigkeit der IKT in vielen Bereichen unternehmenskritisch. Das Spektrum der IKT umfasst beispielsweise den Betrieb von IT-Anlagen für die Lehre, für die Arbeit der Verwaltung, der Zentralen Dienste, für die Kommunikation mit externen Partnern und Auftraggebern sowie für die Durchführung von Versuchen und Experimenten, wissenschaftliche Anwendungen und Simulationen. Die Auswirkungen von Störungen oder Ausfällen in diesen verschiedenen Anwendungsgebieten sind von unterschiedlicher Tragweite. Datenverlust an Unautorisierte kann zu Nachteilen im Wettbewerb um Fördermittel und die besten Fachkräfte, zu finanziellen Einbußen und zu Reputationsbeschädigungen führen. Wegen bestehender Abhängigkeiten und zunehmender Bedrohungen durch Cyber-Angriffe werden von Zuwendungsgebern immer häufiger Sicherheitsnachweise gefordert. Aus diesen Gründen ist es insgesamt unerlässlich, eine IT-Sicherheitsstrategie zu formulieren und umzusetzen.

Dieses Dokument definiert die IT-Sicherheitsleitlinie der teilnehmenden Hochschulen und wissenschaftlichen Einrichtungen in Schleswig-Holstein inklusive der IT-Sicherheitsstrategie. Es stellt die Basis für ein IT-Sicherheitskonzept und daraus folgende Maßnahmen für eine schrittweise Verbesserung und dauerhafte Aufrechterhaltung der Sicherheit im Bereich der Informationstechnik dar.

4. Geltungsbereich

Diese IT-Sicherheitsleitlinie gilt für alle Personen, die Zugriff auf die IKT der Einrichtung haben.

5. Eckpfeiler der IT-Sicherheitsstrategie

Grundlegende Voraussetzung für IT-Sicherheit ist ein Risikomanagement auf Basis des Schutzbedarfes von Daten, Anwendungen und der technischen Infrastruktur. IT-

Sicherheitsziele und Maßnahmen orientieren sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dabei ist der Aufwand für die IT-Sicherheitsmaßnahmen in Relation zu dem angestrebten Sicherheitsniveau zu setzen.

Die Aufrechterhaltung der IT-Sicherheit ist aufgrund dauernd wechselnder Gefährdungen eine permanente Aufgabe. Dieses erfordert personelle und finanzielle Mittel und die Mitwirkung aller Nutzerinnen und Nutzer der IKT.

5.1. Ziele der IT-Sicherheit

IT-Sicherheit umfasst die Verfügbarkeit, Vertraulichkeit und Unversehrtheit von Daten und Anwendungen.

5.1.1. Verfügbarkeit der Informations- und Kommunikationstechnik

Technische Systeme[3] besitzen eine begrenzte Verfügbarkeit. Dabei ist organisatorisch festzulegen, welche Ausfallzeiten akzeptabel und unter dem Gesichtspunkt der Wirtschaftlichkeit vertretbar sind. In Abhängigkeit hiervon sind geeignete Maßnahmen zu ergreifen, die in den akzeptierten zeitlichen Grenzen einen Wiederanlauf ermöglichen. Daten sind so zu sichern, dass nach menschlichem Ermessen ein grundsätzlicher Verlust ausgeschlossen werden kann.

5.1.2. Unversehrtheit (Integrität) von Daten

Unbefugte oder unbemerkte Veränderungen von Daten sollen ausgeschlossen sein, sei es durch Personen, Schadsoftware 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 Unversehrtheit von Daten zu erhalten.

5.1.3. Vertraulichkeit von Daten (Schutz vor unberechtigtem Zugriff)

In wissenschaftlichen Einrichtungen werden unterschiedlichste vertrauliche Informationen verarbeitet. Da nicht ausgeschlossen ist, dass auf die Daten unberechtigt zugegriffen wird, müssen geeignete technische, organisatorische und personelle Maß-

[3] Darunter wird Hard-, Software und Daten verstanden

nahmen in den Anwendungen, dem IT-Netz, den Servern, den Arbeitsplatzcomputern und auf den Übertragungswegen ergriffen werden, die einen möglichst effektiven Zugriffsschutz bewirken.

5.2. Proaktive Maßnahmen

Grundlegend für die Einhaltung der IT-Sicherheitsziele sind proaktive Maßnahmen, die es ermöglichen, dass Bedrohungen zeitnah erkannt und Risiken minimiert werden können. Dazu gehören z.B. die Etablierung von Rechte- und Rollenkonzepten, die Verwendung von Verschlüsselung, ein geeignetes Monitoring der IT-Infrastrukturen, das Filtern des Datenverkehrs nach gefährlichen Inhalten und die Sensibilisierung der Beschäftigten.

6. Aufgabenzuordnung und Rahmenbedingungen

Die Gesamtverantwortung für die IT-Sicherheit liegt bei der Leitung der wissenschaftlichen Einrichtung. Die IT-Sicherheit ist für die Einrichtung ein wesentliches strategisches Ziel.

Die Leitung der wissenschaftlichen Einrichtung bestellt eine oder einen IT-Sicherheitsbeauftragte*n und stellt ihm oder ihr die erforderlichen Ressourcen und Befugnisse zur Verfügung. Der oder die IT-Sicherheitsbeauftragte berichtet an die Leitung und berät hinsichtlich risikomindernder Maßnahmen.

6.1. IT-Sicherheitsbeauftragte*r

Der oder die IT-Sicherheitsbeauftragte ist dafür zuständig, dass die in dieser IT-Sicherheitsleitlinie benannten Ziele konkretisiert, umgesetzt und eingehalten werden. Er oder sie sorgt dafür, dass angemessene IT-Sicherheitsmaßnahmen im Rahmen eines IT-Sicherheitskonzepts realisiert, fortentwickelt und überwacht werden.

Sich hieraus ergebende Regeln sind für alle Nutzerinnen und Nutzer der IKT verbindlich.

6.2. Nutzer*innen der IKT

Alle Nutzer*innen der IKT sind für die Sicherheit und den Schutz der Daten im eigenen Verantwortungsbereich verantwortlich. Alle Nutzer*innen sind verpflichtet, bei der Erfüllung der Aufgabe „IT-Sicherheit“ kooperativ und verantwortungsbewusst mitzuwirken.