Verwaltungs- und Benutzungsordnung des Informationszentrums

Abschnitt II Benutzungsordnung der Abteilung Informationstechnik

Präambel

Diese Benutzungsordnung dient der Sicherheit sowie der verantwortungsbewussten und kostenbewussten Nutzung der informationstechnischen Einrichtungen (IT) der Hochschule Albstadt-Sigmaringen. Sie ist von allen Nutzern einzuhalten. Nutzer sind in der Regel alle Mitglieder und Angehörige der Hochschule.

Sobald ein Nutzer die IT der Hochschule nutzt,

- akzeptiert er diese Benutzungsordnung
- ist er mit der automatischen E-Mail-Filterung zum Unterdrücken von unerwünschten Massenmails (SPAM) einverstanden.

Diese Benutzungsordnung gilt in gleicher Weise für Frauen als auch für Männer, auch wenn hier die männliche Anrede gewählt wurde.

Die Sicherheit und der Fortbestand unserer Hochschule sind in hohem Maße von der fehlerfreien Funktion der technischen Einrichtungen, speziell auch der informationstechnischen Einrichtungen abhängig. Dazu gehören die elektronische Datenverarbeitung (EDV) und die Telefonanlage. Durch Computerviren, Spionage und Sabotage sind diese Einrichtungen besonders gefährdet. Unsachgemäße Nutzung, bewusster und unbewusster Missbrauch der informationstechnischen Einrichtungen erhöhen nicht nur das Gefährdungspotential. Sie verursachen erhebliche Mehrkosten für Wartung und Reparatur, für die Speicherung der anfallenden digitalen Daten, deren tägliche Sicherung und Archivierung und für die ausfallsichere Auslegung der informationstechnischen Komponenten. Außerdem müssen laut Datenschutzgesetz personenbezogene Daten von Mitarbeitern, Studierenden, Kunden und Lieferanten besonders geschützt werden.

Um die Sicherheit und den Schutz der informationstechnischen Einrichtungen sowie der gespeicherten Daten zu gewährleisten und um die Kosten der Informationstechnologie in akzeptablen Grenzen zu halten, ist es notwendig, dass alle Angehörigen unserer Hochschule mit den informationstechnischen Einrichtungen verantwortungsbewusst und kostenbewusst umgehen.

§1 Sicherheitskonzept

Das EDV-Netzwerk der Hochschule wird künftig nach einem Sicherheitskonzept gegliedert. Die dazu erforderlichen technischen Maßnahmen werden baldmöglichst umgesetzt. Zwischen dem internen Netzwerk der Hochschule und dem externen Netz der Belwü wird eine Firewall installiert. Im internen Netz werden verschiedene Zonen mit abgestuften Sicherheitsebenen eingeführt. Die höchste Sicherheitsebene ist dabei mit 100 und die niedrigste Sicherheitsebene mit 0 klassifiziert. Es wird unterschieden zwischen Nutzern und Administratoren. Nutzer dürfen entsprechend den Berechtigungskonzepten der Hochschule die angebotenen EDV-Dienste nutzen. Administratoren können darüber hinaus Rechner und Netzwerkkomponenten verwalten, installieren und konfigurieren.
Administratoren werden von der Abteilung Informationstechnik oder vom jeweiligen Dekan oder vom jeweiligen Leiter einer zentralen Einrichtung benannt. Lokale Administratorenrechte hängen von der Zuordnung zu Sicherheitszonen ab und bedürfen nicht der Zustimmung des Dekans.

Als weitere grundlegende Regeln gelten folgende Definitionen:

(1) Prinzipiell ist ein Übergang von einer niedrigeren auf eine höhere Sicherheitsebene nicht möglich und auch nicht gestattet. Falls Bedarf besteht, von einer niedrigeren Sicherheitsebene auf Ressourcen einer höheren Sicherheitsebene zuzugreifen, muss dies nach vorherigen Sicherheitsmaßnahmen explizit frei geschaltet werden.

(2) Externer Zugriff auf einen Rechner der Hochschule ist nur möglich, wenn sich der Rechner in einer demilitarisierten Zone (DMZ) befindet.

(3) Alle Rechner, die sich mit dem Netzwerk der Hochschule verbinden, dürfen nur benutzt werden, wenn eine aktuelle Antiviren- und Antispyware-Software darauf eingesetzt ist und wenn die aktuellen Updates installiert sind. Die Administratoren haben dafür zu sorgen, dass diese Bedingung für Rechner der Hochschule erfüllt wird.

(4) Nutzer dürfen keine Änderungen an der existierenden Verkabelung vornehmen. Insbesondere ist das Aus- und Umstecken von Netzwerkgeräten untersagt.

(5) Die Abt. Informationstechnik kann die Einhaltung des Sicherheitskonzeptes überprüfen.

§2 Zonen und Sicherheitsebenen

(1) Management (Sicherheitsebene 100)
Hier sind die administrativen Schnittstellen von aktiven Netzwerkkomponenten und Servern angesiedelt, welche von der Abteilung Informationstechnik betrieben werden.
Der Zugriff erfolgt nur über ein Management-VPN.
Administratoren sind ausschließlich benannte Mitarbeiter der Abt. Informationstechnik.

(2) Verwaltung Server (Sicherheitsebene 100)
In diesem Segment befinden sich die Server der Verwaltung sowie die Kommunikationskomponenten mit höchstem Sicherheitsbedarf.
Administratoren sind ausschließlich benannte Mitarbeiter der Abteilung Informationstechnik.

(3) Mitarbeiter Clients (Sicherheitsebene 90)
In dieser Zone befinden sich die Clients von Mitarbeitern, die ungehindert Zugriff auf Verwaltungsdaten brauchen. Zugriff auf die Forschung und Lehre Server ist ebenfalls ungehindert möglich.

Der Zugang zu dieser Zone erfolgt entweder kabelgebunden oder über ein speziell dafür konfiguriertes WLAN.

Lokale Administrationsrechte sind nicht möglich. Der Zugang zum Internet erfolgt ausschließlich über einen Proxy-Server. Dienste können nicht veröffentlicht werden. Administratoren sind ausschließlich benannte Mitarbeiter der Abteilung Informationstechnik. Clients in diesem Segment müssen an den zentralen Sicherheitsmassnahmen teilnehmen.

(4) Forschung und Lehre Server (Sicherheitsebene 80)
Diese Zone beinhaltet das Active Directory sowie den zentralen Exchange Server. Gemeinsame Ressourcen zwischen Verwaltung, Lehrenden sowie Studierenden werden hier angesiedelt. Die hier befindlichen Server können nicht aus dem Internet erreicht werden.

Administratoren sind ausschließlich benannte Mitarbeiter des jeweiligen Studiengangs oder der Abteilung Informationstechnik.

(5) Forschung und Lehre Clients (Sicherheitsebene 50)
Diese Zone dient für alle Pool PCs sowie für die Clients, für die eine lokale Administration notwendig ist.

Aus dieser Zone ist der Zugriff auf Verwaltungsdaten nur mit zusätzlichen Sicherheitsmassnahmen wie Verschlüsselung, 2-Faktor Authentisierung und Terminaldiensten möglich.

Zugriff auf Forschung und Lehre Server ist ungehindert möglich. Lokale Administrationsrechte sind möglich. Diese Systeme müssen zwingend an den zentral angebotenen Sicherheitsmaßnahmen der Abteilung Informationstechnik teilnehmen.

Bei Systemen, die aus technischen Gründen nicht an den zentralen Sicherheitsmassnahmen teilnehmen können, muss in den Fachbereichen ein Administrator benannt werden, der für einen sicheren Zustand und Betrieb der Clients verantwortlich zeichnet.

Administratoren sind gleichzeitig benannte Mitarbeiter des jeweiligen Studiengangs und der Abteilung Informationstechnik.

(6) Forschung und Lehre Projekte und Praktika (Sicherheitsebene 45)
Diese Zone dient der Aufnahme aller Clients aus dem Forschung und Lehre Bereich auf denen Studierende für Praktika oder Projektarbeiten mit Root- oder Administratorrechten arbeiten können. Damit werden diese Clients von den als sicher zu betrachtenden FuL Clients separiert. Für die Studiengänge wird jeweils ein IP Subnetz in dieser Zone eingerichtet. Sollte ein Studiengang darüber hinaus Bedarf haben, sich gegen die anderen Studiengänge in dieser Zone abzuschotten, liegt dies in der eigenen Verantwortung des Studiengangs.

(7) DMZ RAS (Sicherheitsebene 40)
In dieser Zone befindet sich die private Schnittstelle der VPN ASA und ggf. anderer Remote Access Geräte. Auf diese Weise wird der über VPN in das Netz kommende Verkehr reglementiert. Administratoren sind ausschließlich benannte Mitarbeiter der Abteilung Informationstechnik.

(8) DMZ Restriktiv (Sicherheitsebene 30)
In dieser Zone finden sich zentrale Server, die von Außen (Internet, BelWü) erreichbar sind oder dort hin kommunizieren.

Die Kommunikation unterliegt einem Regelwerk.

Administratoren sind ausschließlich benannte Mitarbeiter der Abteilung Informationstechnik.

(9) DMZ Forschung und Lehre (Sicherheitsebene 20)
Diese DMZ dient zur Aufnahme der Server, die von den Fakultäten betrieben werden und die externe Kommunikationsbeziehungen benötigen. Eine Kommunikation mit den Zonen der Verwaltung ist nicht möglich.

Die in das Internet ausgehende Kommunikation ist ungehindert möglich. Die eingehende Kommunikation unterliegt einem Regelwerk.

Administratoren sind ausschließlich benannte Mitarbeiter des jeweiligen Studiengangs oder der Abteilung Informationstechnik.

(10) Public Internet (Sicherheitsebene 10)
Diese Zone dient der Aufnahme aller übrigen Clients. Der Anschluss an das Hochschulnetz erfolgt dabei entweder per WLAN oder durch Anschluss an spezielle, von der Abt. Informationstechnik bereitgestellte Netzwerkdosen. Die Kommunikation aus dieser Zone auf das Internet und auf die Zonen der Forschung und Lehre erfolgt über eine Software, welche Vertraulichkeit und Authentizität der Kommunikation sicherstellt.

Aus dieser Zone ist der Zugriff auf Verwaltungsdaten nur mit zusätzlichen Sicherheitsmassnahmen wie Verschlüsselung, 2-Faktor Authentisierung und Terminaldiensten möglich. Direkter Zugriff auf Fileshares der Verwaltung ist nicht möglich.

Administratoren sind die jeweiligen Besitzer und/oder Inhaber der Rechner.

(11) Externe Partner (Sicherheitsebene 15)
In dieser Zone sind Rechner externer Partner, z.B. des Studentenwerks angesiedelt. Diese Rechner haben keinen Zugriff auf das Hochschulnetz.

(12) Outside (Sicherheitsebene 0)
Hier findet der Übergang nach Außen (Internet, Belwü) sowie der Transfer zwischen Albstadt und Sigmaringen statt.

(13) Über die genannten Kommunikationsbeziehungen hinausgehende Anforderungen müssen individuell mit den Verantwortlichen unter Berücksichtigung von Kosten und Nutzen abgestimmt werden.

§ 3 Installation und Einsatz von Software

(1) Im EDV-Netzwerk der Hochschule und besonders auf allen Servern, Computern und Laptops der Hochschule dürfen nur Softwareprodukte installiert und genutzt werden, die rechtmäßig lizenziert wurden.

(2) Ausführbare Programme (binäre Dateien) auf den Rechnern der Hochschule dürfen nur durch die Administratoren installiert werden. Dies bezieht sich insbesondere auf folgende Punkte:

- Installation von Betriebssystemen, Anwendungsprogrammen, Updates, Hotfixes und auch Bildschirmschoner, Demoprogramme, Computerspiele oder Utilities.
- Herunterladen von ausführbaren Programmen (binäre Dateien) aus dem Internet oder Installation auf einem anderen Weg, beispielsweise von externen Datenträgern auf Computern.
- Direktes Starten von ausführbaren Programmen (binäre Dateien) direkt aus dem Internet oder aus E-Mail-Anhängen heraus.

Ausführbare Programme dürfen dann durch Nutzer installiert werden, wenn die Nutzer durch einen Administrator dazu aufgefordert werden.

(3) Alle Datenbestände, die von außerhalb des Campusgeländes (z.B. auf externen Datenträgern wie mobilen Festplatten, Disketten, CDs, DVDs, Memory-Sticks oder über das Internet oder als E-Mail-Anhang) in das Hochschulnetz importiert werden, müssen durch das aktuelle Antivirenprogramm der Hochschule überprüft werden, bevor sie im Netz der Hochschule verwendet werden.

(4) Beim Kopieren von Software sind die Lizenzbedingungen einzuhalten.

§ 4 Datenschutz

(1) Zugangsdaten, wie z.B. Accountnamen oder Passwörter dürfen nicht offen einsehbar hinterlegt werden, weder schriftlich als Notiz noch als unverschlüsselte Datei auf Computern oder Datenträgern. Passwörter dürfen unter keinen Umständen an Dritte weitergegeben werden.

(2) Die Vergabe von Berechtigungen für den Zugriff auf Daten und Programme erfolgt nach Berechtigungskonzepten der Hochschule.

(3) Hochschulinterne Daten, welche nicht Zwecken der Lehre und Forschung dienen, dürfen nur mit Beauftragung der Hochschulleitung Dritten zugänglich gemacht werden. Dies bezieht sich insbesondere auf Adressdaten, personenbezogene Daten oder Produktdaten.

(4) Jeder Nutzer ist verpflichtet, alle ihm im Rahmen des Vertragsverhältnisses und seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente über die Angelegenheiten der Hochschule, ihrer Mitarbeiter, Lieferanten, Kunden und sonstigen Kontakte zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich zu behandeln und geheim zu halten. Er darf derartige Informationen Dritten nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben, außer in Erfüllung seiner vertraglichen Pflichten. Zieht der Mitarbeiter

im Auftrage der Hochschule Dritte zur Mitarbeit hinzu, ist er verpflichtet, diesen die gleiche Verschwiegenheitspflicht aufzuerlegen.

(5) Daten müssen generell so gespeichert werden, dass bei Ausfall eines Mitarbeiters dessen Vertretung oder der Vorgesetzte auf diese Daten zugreifen kann. Die Vereinbarungen der jeweiligen Organisationseinheit über die Ablage von Daten sind zu beachten.

(6) Der Nutzer darf nicht versuchen, in Netzbereiche vorzudringen, die nicht für den Nutzer und sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Rechtevergabe oder technische Mängel möglich ist. Über derartige fehlerhafte Rechtevergabe oder technische Mängel ist der Vorgesetzte oder die IT-Abteilung ohne Verzug zu informieren.

§ 5 Datensicherung

(1) Jeder Nutzer ist dafür verantwortlich, dass er von ihm erzeugte oder verwendete Daten dort speichert, wo sie von der zentralen Datensicherung der Hochschule erfasst werden.

(2) Jeder Nutzer ist angehalten, nicht mehr benötigte Dateien und E-Mails regelmäßig zu löschen und damit dazu beizutragen, dass die Datenbestände und deren Strukturen überschaubar bleiben und die Kosten der Datenhaltung und Datensicherung in vertretbaren Grenzen bleiben.

(3) Mitarbeiter, die mit der Datensicherung beauftragt sind, haben diese Aufgaben mit besonderer Sorgfalt durchzuführen und müssen ihren Vorgesetzten unverzüglich informieren, wenn Probleme aufgetreten sind oder Gefahr im Verzug ist.

§ 6 Allgemeine Regelungen

(1) Die informationstechnischen Einrichtungen der Hochschule dürfen nicht missbräuchlich genutzt werden. Sie dürfen ausschließlich für dienstliche Zwecke oder im Rahmen des Studiums benutzt werden. Darüber hinausgehende Regelungen für Beschäftigte können in einer Betriebsvereinbarung geregelt werden. Darüber hinausgehende Regelungen für Studierende können von der jeweiligen Studiengangsleitung geregelt werden. Eine kommerzielle Nutzung darf nur mit Zustimmung der Hochschulleitung erfolgen.

(2) Bei Verdacht auf Virengefahr, Datenspionage oder anderer Umstände, die die Sicherheit der Informationstechnologie der Hochschule betreffen, ist unverzüglich ein Vorgesetzter oder die IT-Abteilung der Hochschule zu informieren.

(3) Der Zugriff auf pornografische oder politisch radikale Internetinhalte ist verboten. Die Verbreitung von gewaltverherrlichenden, pornographischen, rassistischen und volksverhetzenden Darstellungen in Bild, Ton und Schrift ist untersagt. Auf die Vorschriften der §§ 130, 131 und 184 des StGB wird ausdrücklich verwiesen. Gleiches gilt für Inhalte, die das körperliche, geistige oder seelische Wohl von Kindern und Jugendlichen beeinträchtigen können.

(4) Jeder Nutzer ist angehalten, die technischen Einrichtungen pfleglich zu behandeln und mit den informationstechnischen Ressourcen sparsam umzugehen. Das betrifft auch den Verbrauch von Speicherplatz auf den Servern und von Verbrauchsmaterialien wie Druckerpapier, Druckfolien, Druckerpatronen usw.

(5) Störungen und Defekte an informationstechnischen Einrichtungen und auftretende Fehler in der Software sind unverzüglich den dafür verantwortlichen Personen zu berichten.

(6) Zentrale IT-Räume, wie z.B. Serverräume oder Netzwerkverteiler und Büros mit IT-Einrichtungen müssen jederzeit auch physikalisch so geschützt werden, dass kein Unbefugter Zutritt erhält.

(7) Die Zugangsberechtigungen zu zentralen IT-Räumen, wie z.B. Serverräume oder Netzwerkverteiler, werden nach einem Zugangskonzept der Hochschule vergeben. Wartungsarbeiten durch externe Firmen dürfen nur unter Aufsicht erfolgen.

(8) Der Nutzer erklärt sich ausdrücklich damit einverstanden, dass die Hochschule personenbezogene Daten erheben, verarbeiten und nutzen kann, soweit dies zur Erfüllung ihrer Aufgaben bzw. der Einhaltung der gesetzlichen Bestimmungen erforderlich ist. Die Weitergabe an Dritte ist hierbei ausgeschlossen. Das Einverständnis bezieht sich sowohl auf solche Daten, die erforderlich sind, um Dienste der IT-Abteilung in Anspruch zu nehmen (Nutzungsdaten, z.B. IP-Adresse oder genutzte Dienste) als auch auf Daten, die zur inhaltlichen Ausgestaltung des Benutzungsverhältnisses erforderlich sind (Bestandsdaten, z.B. Name oder Telefonnummer).

(9) Folgende Vorschriften und Gesetze sind von allen Angehörigen der Hochschule einzuhalten:
- Bundes- und Landesdatenschutzgesetz (BDSG und LDSG)
- Ausspähen von Daten (§ 202a StGB)
- Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB)
- Computerbetrug (§ 263a StGB)
- Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB)
- Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB)
- Strafbare Urheberrechtsverletzungen, z.B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG)
- Datengeheimnis (§ 5 BDSG)

(10) Sollten betriebsbedingte Anforderungen weitere Regelungen erfordern, die in dieser Benutzungsordnung nicht enthalten sind, so sind diese mit der Abt. Informationstechnik abzustimmen.

(11) Verstöße gegen eine oder mehrere Regeln dieser Benutzungsordnung können zum Entzug der Nutzungsberechtigung für die IT-Einrichtungen führen und personal- und strafrechtliche Konsequenzen nach sich ziehen.

§ 7 Evaluation

Nach Einführung des Sicherheitskonzeptes wird diese Benutzungsordnung nach einem Jahr überprüft.

Sigmaringen, 03.03.2009

Prof. Dr. Günter Rexer
Rektor

Nachweis der öffentlichen Bekanntmachung:

Ausgehängt am: 05.03.2009
Abgehängt am: 31.03.2009

Zur Beurkundung

Bernadette Boden
Verwaltungsdirektorin