

Betriebsordnung der IT-Dienste der Hochschule für Wirtschaft und Umwelt Nürtingen - Geislingen

vom 24. Januar 2013

Aufgrund von § 8 Abs. 5 des Landeshochschulgesetzes (LHG) in der Fassung vom 1. Januar 2005 (GBl. S. 1) in Verbindung mit § 8 der Satzung für das Informationszentrum der Hochschule für Wirtschaft und Umwelt Nürtingen - Geislingen vom 12. Dezember 2011 hat der Senat in seiner Sitzung am 25. Oktober 2012 die nachstehende Betriebsordnung der IT-Dienste beschlossen.

Nach Art. 3 Abs. 2 GG sind Frauen und Männer gleichberechtigt. Alle Personen und Funktionsbezeichnungen in dieser Ordnung gelten für Frauen und Männer in gleicher Weise.

Inhaltsverzeichnis

1. Abschnitt - Allgemeine Bestimmungen	3
§ 1 Geltungsbereich.....	3
§ 2 Gegenstand.....	3
§ 3 Benutzerkreis.....	3
§ 4 Nutzungszweck und Zulassung zur Nutzung.....	3
§ 5 Begriffsbestimmungen.....	3
2. Abschnitt - Rechen- und Kommunikationstechnik	4
§ 6 Zentrale Benutzerkennung	4
§ 7 E-Mail.....	5
§ 8 Webhosting - Inhalte von Internet-Websites	5
§ 9 Software.....	6
§ 10 Wireless LAN.....	6
§ 11 Protokollierung von Verkehrsdaten.....	7
§ 12 Rechte und Pflichten der Nutzer	7
§ 13 Sanktionen bei Missbrauch.....	8
§ 14 Haftung des Nutzers	8
§ 15 Haftung der HfWU	9
§ 16 Rechte und Pflichten des Administrators	9
§ 17 Fernwartung	9
§ 18 Inkrafttreten	10

1. Abschnitt - Allgemeine Bestimmungen

§ 1 Geltungsbereich

Die Betriebsordnung gilt für die Nutzung aller rechen- und kommunikationstechnischen Einrichtungen und Systeme (ausgenommen der Telekommunikationsanlage und der Brandmeldeanlage) der Hochschule für Wirtschaft und Umwelt Nürtingen - Geislingen (nachfolgend HfWU) sowie für die Gesamtheit der Nutzer.

§ 2 Gegenstand

Gegenstand dieser Ordnung ist

1. die Regelung der Nutzungsmöglichkeit und Rechte als auch die verbindlich einzuhaltenden Pflichten für die in § 1 genannten Einrichtungen und Systeme,
2. die Nutzungsbedingungen und Maßnahmen der Pflege, Wartung und Kontrolle mit entsprechenden Aufzeichnungen transparent zu machen,
3. die personenbezogenen Daten der Nutzer zu sichern,
4. der sichere Betrieb der IT - Systeme und des Hochschulnetzes.

§ 3 Benutzerkreis

- (1) Zur Nutzung der IT-Dienste der Hochschule können zugelassen werden
 1. Mitglieder, Angehörige, zentrale Betriebs- und wissenschaftliche Einrichtungen der Hochschule,
 2. Beauftragte der Hochschule zur Erfüllung ihrer Dienstaufgaben,
 3. sonstige staatliche Forschungs- und Bildungseinrichtungen und Behörden sowie in Einzelfällen sonstige andere Personen aufgrund besonderer Vereinbarungen.
- (2) Die Hochschule behält sich vor, jederzeit den Nutzerkreis zu erweitern oder einzuschränken.

§ 4 Nutzungszweck und Zulassung zur Nutzung

- (1) Das Nutzungsrecht der rechen- und kommunikationstechnischen Einrichtungen und Systeme der Hochschule erfolgt per Antrag.
- (2) Den Studierenden wird das Nutzungsrecht mit der Immatrikulation eingeräumt.
- (3) Die Zulassung zur Nutzung erfolgt zu Zwecken von Forschung, Lehre und Studium, der Aus- und Weiterbildung sowie zu Zwecken der Verwaltung von Hochschulangelegenheiten der HfWU.
- (4) Das Betreiben von Servern bedarf der Genehmigung des Bereichsleiters IT-Dienste und ist schriftlich zu beantragen.
- (5) Für die Nutzung von Software gilt § 9.

§ 5 Begriffsbestimmungen

- (1) Die **IT-Dienste** haben die Gesamtverantwortung für alle rechen- und kommunikationstechnischen Einrichtungen und Systeme der Hochschule gem. § 1.
- (2) **Administratoren** sind von den IT-Diensten bestellte Personen, die für die rechen- und kommunikationstechnischen Einrichtungen und Systeme in ihrem Aufgabenbereich verantwortlich sind.
- (3) **Systembetreuer** haben Administrationsrechte für Teilbereiche und dürfen nur in Absprache mit den IT-Diensten bestellt werden. Der Bereichsleiter IT-Dienste ist weisungsbefugt und kann die Bestellung jederzeit widerrufen.
- (4) **Benutzer** (Nutzer) sind dem Benutzerkreis zugehörige gem. § 3.
- (5) Zu den **Mitgliedern** der Hochschule zählen die an der Hochschule hauptberuflich Tätigen, die eingeschriebenen Studierenden sowie die Professoren.

- (6) Wer an der Hochschule tätig ist, ohne ihr Mitglied zu sein, ist **Angehöriger** der Hochschule.
- (7) **Server** sind IT-Systeme, die anderen IT-Systemen innerhalb oder außerhalb des Hochschulnetzes Speicherplatz, Dienste oder sonstige Ressourcen zur Verfügung stellen.
- (8) **Personenbezogene Daten** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person.
- (9) **Verkehrsdaten** (Nutzungsdaten) sind technische Informationen, die bei Nutzung der Systeme anfallen, bspw. Beginn und Ende einer Verbindung.
- (10) Ein **Verfahrensverzeichnis** ist ein Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden.
- (11) **Externe Fernwartung** wird durch einen fremden Dritten mit Rechnern, die sich außerhalb des Hochschulnetzes befinden, durchgeführt.
- (12) **Interne Fernwartung** wird durch Administratoren oder Systembetreuer ausschließlich innerhalb des Hochschulnetzes durchgeführt.
- (13) Das Landesdatenschutzgesetz als auch das Bundesdatenschutzgesetz finden ergänzend Anwendung.

2. Abschnitt - Rechen- und Kommunikationstechnik

§ 6 Zentrale Benutzererkennung

- (1) Für die Nutzer der rechen- und kommunikationstechnischen Einrichtungen und Systeme der HfWU wird die Benutzererkennung gem. § 4 vergeben und verwaltet. Für Studierende der HfWU können die IT-Dienste zentrale Benutzerkennungen (Benutzername, Passwort) in automatisierter Form vergeben und verwalten.
- (2) Zusammen mit der Benutzererkennung erhält der Nutzer ein sogenanntes Homeverzeichnis für die zentrale Ablage von Daten. Auf dieses Homeverzeichnis hat allein der Nutzer Zugriff. Jedem Nutzer steht ein maximales Speichervolumen zur Verfügung, dessen Größe auf der Hochschulwebseite (www.hfwu.de) veröffentlicht wird. Regelmäßig gesicherter Speicherplatz mit hoher Verfügbarkeit kann nicht in beliebiger Höhe zur Verfügung gestellt werden.
- (3) Beim Ausscheiden eines Nutzers werden dessen persönliche Daten in den verschiedenen IT-Systemen inkl. Benutzererkennung und E-Mail-Adresse gem. § 7 unverzüglich gelöscht, sobald eine schriftliche Mitteilung durch die Hochschulverwaltung oder eine andere Hochschuleinrichtung gegenüber den IT-Diensten vorliegt. Die Löschung der Benutzerkennungen von Studierenden erfolgt nach Exmatrikulation.
- (4) Die Nutzer sind verpflichtet, ausschließlich mit der Benutzererkennung (Benutzername, Passwort) zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde.
- (5) Die Weitergabe der Benutzererkennung ist unzulässig. Jeder Nutzer hat dafür Sorge zu tragen, dass unberechtigten Personen die Nutzung seiner Benutzungskennung verwehrt wird. Dazu gehören die sorgfältige Wahl eines Passwortes und dessen regelmäßige Änderung. Dem Nutzer ist es untersagt, fremde Benutzerkennungen zu ermitteln und zu nutzen. Die Passwortvergabe sollte den aktuellen Sicherheitsrichtlinien entsprechen (www.hfwu.de).

§ 7 E-Mail

- (1) Die Nutzer sind dazu verpflichtet die Funktionalität des E-Mail-Accounts sicherzustellen, insbesondere ausreichend Speicherplatz durch regelmäßiges Löschen von E-Mails, vorzuhalten.
- (2) Die IT-Dienste bilden die E-Mail-Adressen für die Mitglieder und Angehörigen an der HfWU mit Ausnahme der Studierenden aus Vorname.Nachname@hfwu.de.
- (3) Für die Studierenden werden die E-Mail-Adressen aus Nachname sowie dem Anfangsbuchstaben des Vornamens gebildet, bspw. Max Mustermann - mustermannm@stud.hfwu.de. Die schriftliche Einwilligung des betroffenen Nutzers hierfür ist nicht gesondert erforderlich. Bei Gleichnamigkeit der E-Mail-Adressen für Studierende, werden zugunsten der Eindeutigkeit weitere Buchstaben des Vornamens hinzugefügt, bspw. mustermannma@stud.hfwu.de.
- (4) Auf schriftlichen Antrag kann eine personenneutrale E-Mail-Adresse bestehend aus Struktureinheit@hfwu.de, Funktionseinheit@hfwu.de oder Institutname@hfwu.de vergeben werden. Diese Vergabe unterliegt strengen Kriterien um eine missbräuchliche Nutzung dieser personenneutralen E-Mail-Adressen zu verhindern.
- (5) Wird eine Benutzerkennung zeitweilig durch die IT-Dienste gesperrt, werden E-Mails an die damit verbundenen E-Mail-Adressen weiterhin angenommen und in der zur Benutzerkennung gehörende Mailbox gespeichert, sofern ausreichend Speicherplatz vorhanden ist. Nach erfolgter Entsperrung kann der Benutzer auf diese E-Mails zugreifen. Ist eine Benutzerkennung endgültig gelöscht, werden E-Mails an die damit verbundenen E-Mail-Adressen abgewiesen.
- (6) Die Bildung und Nutzung von automatisch generierten E-Mail-Verteilerlisten ist nur zulässig, soweit dies zur Durchführung des Dienst- oder Arbeitsverhältnisses, zur Durchführung organisatorischer Maßnahmen sowie für Ausbildungs-, Prüfungs- oder wissenschaftliche Zwecke erforderlich ist. Die E-Mail-Verteilerlisten werden unter Mitwirkung der personalverwaltenden Stelle und des Studierendensekretariats verwaltet.
- (7) E-Mails werden auf SPAM, Schadsoftware sowie auf ausführbare Dateien überprüft. Weiterführende Informationen finden sich auf der Hochschulwebseite (www.hfwu.de).
- (8) Jedem Nutzer steht ein maximaler E-Mail-Speicherplatz zur Verfügung. Regelmäßig gesicherter Speicherplatz mit hoher Verfügbarkeit kann nicht in beliebiger Höhe zur Verfügung gestellt werden. Aus diesem Grund ist auch die maximal zulässige Größe von E-Mails (inkl. Anhängen) begrenzt. Die aktuellen Werte dieser Beschränkungen sind auf der Hochschulwebseite (www.hfwu.de) veröffentlicht.
- (9) Weiterführende Hinweise zu verteilerbasierten Rundmails finden sich bei den IT-Diensten auf der Hochschulwebseite (www.hfwu.de).

§ 8 Webhosting - Inhalte von Internet-Websites

- (1) Unter Webhosting wird die Bereitstellung von Webspace für den in § 3 genannten Benutzerkreis auf Webservern der HfWU verstanden.
- (2) Der Nutzer verpflichtet sich zur Einhaltung der gesetzlichen Bestimmungen des Telemediengesetzes, insbesondere der Informationspflicht auf Internet-Websites. Er stellt die HfWU von allen Ansprüchen frei, die auf einer Verletzung der vorgenannten Pflichten beruhen.
- (3) Der Nutzer darf durch die Internetseiten nicht gegen Gesetze, gesetzliche Regelungen, die guten Sitten und Rechte Dritter (Marken-, Namens-, Urheber-, Datenschutzrechte usw.) verstoßen.
- (4) Die HfWU ist nicht verpflichtet, die Internet-Präsenz des Nutzers auf eventuelle Rechtsverstöße zu überprüfen. Nach dem Erkennen von Rechtsverstößen oder von Inhalten, welche gemäß dieser Betriebsordnung unzulässig sind, ist die HfWU berechtigt, die Website ohne Warnung zu sperren (§ 13 Sanktionen bei Missbrauch). Über die Sperrung wird der betreffende Betreiber unverzüglich informiert.

§ 9 Software

- (1) Die Zulassung von Software erfolgt ausschließlich zu Zwecken von Forschung, Lehre und Studium, der Aus- und Weiterbildung sowie zu Zwecken der Verwaltung von Hochschulangelegenheiten. Es gelten insbesondere die Lizenzbestimmungen oder die Verträge für das jeweilige Softwareprodukt.
- (2) Alle für die dienstliche Nutzung zu beschaffenden Software-Produkte, die vom Hersteller für den beabsichtigten Verwendungszweck kostenpflichtig zur Verfügung gestellt werden, sind vom Nutzer über die IT-Dienste zu bestellen.
- (3) Die private Nutzung der für dienstliche Zwecke erworbenen Software setzt voraus, dass diese Nutzungsform in Vertrags- oder Lizenzbestimmungen oder vom Hersteller ausdrücklich genehmigt ist.
- (4) Eine dienstliche Nutzung von Hochschul-Software auf privater Hardware muss in den Lizenzrechtsbestimmungen gestattet sein. Zugleich bedarf es der Meldung an den für das Lizenzmanagement verantwortlichen IT-Dienste Mitarbeiter.
- (5) Die Nutzung von privat erworbener Software für dienstliche Zwecke muss durch die Lizenzbestimmungen abgedeckt sein und bedarf der Zustimmung des Bereichsleiters der IT-Dienste.
- (6) Je nach Softwarevertrag erhält der Nutzer das zeitlich unbefristete oder zeitlich befristete Nutzungsrecht. Ist die Nutzung zeitlich befristet, so ist nach Ablauf dieser Nutzungsfrist die Software ohne Aufforderung der IT-Dienste zu deinstallieren. Zudem sind die Sicherungskopien unverzüglich zu vernichten. Ist der Verbleib einer Sicherungskopie für Archivierungszwecke dringend erforderlich, so ist die Genehmigung des Herstellers diesbezüglich einzuholen.
- (7) Ist nach den Lizenzbestimmungen die Installation von Software auf privaten Rechnern erlaubt, so darf diese nur im Zeitraum der Hochschulangehörigkeit oder Hochschulmitgliedschaft genutzt werden. Danach muss unverzüglich, ohne Aufforderung der IT-Dienste, die Software deinstalliert werden.
- (8) Verwendung von Software, die auf Basis der Peer-to-Peer Technologie arbeitet, ist nicht gestattet. Dies betrifft neben Filesharing-Technologien (wie bspw. Tauschbörsen für Musik und Videos) auch die Verwendung von Kommunikationssystemen (wie bspw. Skype).

§ 10 Wireless LAN

- (1) Die Nutzung des Wireless Local Area Network (nachfolgend WLAN) der HfWU ist ausschließlich dem in § 3 dieser Benutzerordnung festgelegten Benutzerkreis vorbehalten.
- (2) Eine Verschlüsselung der WLAN Kommunikation erfolgt nach aktuellem technischen Standard.
- (3) Die Anmeldung erfolgt mit der Benutzerkennung (§ 6 Zentrale Benutzerkennung).
- (4) Das Angriffsrisiko bei Nutzung von WLAN ist gegenüber einem kabelgebundenem Netzwerk erheblich höher. Die HfWU übernimmt keine Haftung für Zugriffe, Abhör- oder Aufzeichnungsversuche durch Dritte. Jeder Nutzer ist verpflichtet, dass sein genutztes System aktuellen Sicherheitsvorkehrungen entspricht bspw. durch einen aktuellen Virens Scanner und eine aktivierte Firewall. Wird ein System, durch automatische Sicherheitsscans als infiziert erkannt, kann dieses von der Nutzung des Netzwerkzugangs ausgeschlossen werden.
- (5) Die von der HfWU angebotenen kommunikationstechnischen Systeme stehen über das WLAN gem. § 1 nicht in vollem Umfang zur Verfügung.
- (6) Im Übrigen gilt § 13 Sanktionen bei Missbrauch.

§ 11 Protokollierung von Verkehrsdaten

- (1) Bei der Nutzung der rechen- und kommunikationstechnischen Einrichtungen werden von den Systemen automatisch Verkehrsdaten (bspw. Benutzername, IP-Adresse, Datum, Uhrzeit oder E-Mail-Empfänger/Absender) erfasst und in Protokolldateien gespeichert.
- (2) Protokolle werden ausschließlich zu Zwecken der Analyse und Korrektur technischer Fehler, zur Beseitigung von technischen Störungen, zur Gewährleistung der Systemsicherheit, Optimierung des Netzes und statistischer Feststellung des Gesamtnutzungsvolumens verwendet.
- (3) In begründeten Fällen von Missbrauch oder beim Verdacht strafbarer Handlungen kann unter Einbezug des Datenschutzbeauftragten eine weitergehende Einsicht in die Protokolldateien vorgenommen werden. Die betroffenen Nutzer sind hierüber zu informieren.
- (4) Protokolle werden nicht zur Verhaltens- und Leistungskontrolle verwendet.
- (5) Der Zugriff der Protokolle ist auf die Administratoren begrenzt. Protokolle und Protokolldaten werden nach spätestens 45 Tage gelöscht, sofern nicht aufgrund des Verdachtes eines schwerwiegenden Verstoßes gegen diese Betriebsordnung ein Speichern der Protokolle und der Protokolldaten bis zur Klärung die Frist verlängert werden muss.

§ 12 Rechte und Pflichten der Nutzer

- (1) Die Nutzer haben das Recht, die rechen- und kommunikationstechnischen Einrichtungen und Systeme der Hochschule sowie die von den IT-Diensten angebotenen Dienstleistungen unter den Vorgaben dieser Betriebsordnung in Anspruch zu nehmen.
- (2) Der Nutzer verpflichtet sich mit Ingebrauchnahme dieser Einrichtungen
 1. die Vorschriften der Betriebsordnung einzuhalten, insbesondere alles zu unterlassen, was den ordnungsgemäßen Betrieb der IT-Dienste stört,
 2. die zu benutzenden rechen- und kommunikationstechnischen Einrichtungen und Systeme sorgfältig und schonend zu behandeln,
 3. seine Nutzungsberechtigung auf Verlangen nachzuweisen,
 4. Störungen, Beschädigungen und Fehler der rechen- und kommunikationstechnischen Einrichtungen und Systeme den Mitarbeitern der IT-Dienste unverzüglich zu melden und auf Nachfrage Auskunft darüber zu erteilen,
 5. keine privaten Rechner mit dem Hochschulnetzwerk zu verbinden, von dieser Regelung ausgeschlossen ist die WLAN-Nutzung gem. § 10 Wireless LAN,
 6. zur Sicherung einer sach- und ordnungsgemäßen Funktion der Datenverarbeitungsanlagen dem Bereichsleiter IT-Dienste oder dessen Mitarbeitern auf Verlangen unter Beachtung der Vertraulichkeit Auskünfte über Programme und benutzte Methoden sowie Einsicht in die Programme zu gewähren (insbesondere selbstentwickelte Programme),
 7. selbst für die Sicherung der auf den lokalen Festplatten gespeicherten Daten und Programme zu sorgen,
 8. Gesetze, gesetzliche Regelungen die guten Sitten und Rechte Dritter (Marken, Namens-, Urheber-, Datenschutzrechte usw.) zu beachten,
 9. Handlungen zum unberechtigten Erlangen von fremden Programmen und Informationen (bspw. Passwörtern) zu unterlassen.

§ 13 Sanktionen bei Missbrauch

- (1) Nutzer können vorübergehend oder dauerhaft in der Benutzung eingeschränkt oder ganz ausgeschlossen werden, wenn diese:
 1. schuldhaft gegen diese Betriebsordnung verstoßen (missbräuchliches Verhalten),
 2. die Rechen- und Kommunikationstechnik sowie Software der HfWU für strafbare Handlungen missbrauchen oder
 3. der HfWU durch sonstiges rechtswidriges Nutzerverhalten Nachteile zufügen.
- (2) Maßnahmen nach Abs. 1 sollen grundsätzlich erst nach vorheriger Anhörung des betroffenen Nutzers erfolgen. Auf Wunsch des betroffenen Nutzers oder der Leitung der IT-Dienste können Mitarbeitervertretung, der Datenschutzbeauftragte und/oder die Hochschulleitung hinzugezogen werden.
- (3) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein Verhalten nach Abs. 1 gegeben ist, kann der zuständige Administrator die weitere Nutzung unterbinden, bis die Sach- und Rechtslage hinreichend geklärt ist.
- (4) Vorübergehende Nutzungseinschränkungen sind aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet ist.
- (5) Auf die folgenden Straftatbestände wird besonders hingewiesen:
 1. Ausspähen von Daten (§ 202 a StGB),
 2. Abfangen von Daten (§ 202 b StGB),
 3. Vorbereiten des Ausspähens und Abfangens von Daten (§202 c StGB),
 4. Datenveränderung (§ 303 a StGB) und Computersabotage (§ 303 b StGB),
 5. Computerbetrug (§ 263 a StGB),
 6. Verbreitung pornographischer Darstellungen (§ 184 b StGB),
 7. Abruf oder Besitz kinderpornographischer Darstellungen (§ 184 b StGB),
 8. Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB),
 9. Ehrdelikte wie Beleidigung oder Verleumdung (§ 185 ff. StGB),
 10. Strafbare Urheberrechtsverletzungen, z. B. durch lizenz- und urheberrechtswidrige Nutzung, Vervielfältigung und Weitergabe (§ 106 ff. UrhG).

§ 14 Haftung des Nutzers

- (1) Die Haftung ergibt sich aus den gesetzlichen Bestimmungen. Hingewiesen wird insbesondere auf zivilrechtliche Schadensersatzansprüche sowie das Marken-, Namens-, Urheber-, und Datenschutzrecht. Weiterhin kommt eine strafrechtliche Verantwortlichkeit in Betracht.
- (2) Der Nutzer haftet für alle Nachteile, die der HfWU durch die missbräuchliche oder rechtswidrige Verwendung, durch schuldhaft verursachte Schäden der Rechen- und Kommunikationstechnik/Software oder durch Nichteinhaltung seiner Verpflichtungen aus dieser Betriebsordnung entstehen.
- (3) Der Nutzer haftet auch für Schäden, die im Rahmen der ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Nutzung Dritter entstanden sind, wenn er deren Nutzung zu vertreten hat.

§ 15 Haftung der HfWU

- (1) Die HfWU übernimmt keine Garantie dafür, dass die Rechen- und Kommunikationstechnik sowie die an der HfWU eingesetzte Software fehlerfrei und jederzeit ohne Unterbrechung verfügbar sind. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.
- (2) Aufgrund wichtiger und regelmäßiger Wartungsarbeiten kann es zu kurzfristigen Ausfällen oder zu einer Nichterreichbarkeit der IT-Systeme kommen. Weiterführende Informationen finden sich auf der Hochschulwebseite (www.hfwu.de).
- (3) Die HfWU übernimmt keine Verantwortung für die zur Verfügung gestellte Software. Weiterhin haftet die HfWU nicht für den Inhalt, insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang zur Nutzung vermittelt.
- (4) Die HfWU übernimmt keine Haftung für Schäden, die durch die Nutzung von den durch die IT-Dienste zur Verfügung gestellten Leistungen auf privaten rechen- und kommunikationstechnischen Einrichtungen entstehen können.

§ 16 Rechte und Pflichten des Administrators

- (1) Die Administratoren sowie die Systembetreuer wurden über ihre weiteren Rechte und Pflichten in Kenntnis gesetzt und haben diese anhand einer Verpflichtungserklärung mit Unterzeichnung anerkannt. Weiterführende Informationen sind auf der Hochschulwebseite zu finden (www.hfwu.de).
- (2) Bei Gefahr sind die Administratoren der IT-Dienste befugt, auf den rechen- und kommunikationstechnischen Einrichtungen und Systeme der Hochschule, ohne zusätzliche Erlaubnis des Benutzers, alle erforderlichen Maßnahmen zum Schutz zu ergreifen. Die betroffenen Benutzer werden wenn möglich nachträglich darüber informiert.

§ 17 Fernwartung

- (1) Externe Fernwartung erfolgt nur mit Unternehmen, die einen Dienstleistungsvertrag (inkl. Verpflichtung der Mitarbeiter des externen Unternehmens auf den Datenschutz) mit der HfWU abgeschlossen oder in Ausnahmefällen einen Einzelauftrag erhalten haben. Ein Einzelauftrag kann nur von zwei Administratoren der IT-Dienste gemeinsam erteilt werden. Dies wird im Fernwartungsprotokoll entsprechend dokumentiert.
- (2) Jede externe Fernsteuerungsverbindung muss von den Administratoren der IT-Dienste aktiv mitgetragen werden (bspw. durch Einschalten der Fernsteuerungssoftware auf der Benutzerseite).
- (3) Eine externe Fernwartungssitzung wird ausschließlich mittels zeitlich begrenzter Freischaltung durch einen Administrator ermöglicht. Über jede externe Fernwartungssitzung wird ein Protokoll mit folgendem Inhalt erstellt:
 1. Name des Administrators oder der/des Systembetreuers
 2. Grund der Fernwartung
 3. Datum
 4. Beginn
 5. Ende
 6. Name des Unternehmens und der Person, die die Fernwartung durchführt
 7. betroffene Systeme
- (4) Bei interner Fernwartung werden die Funktionsweise der Fernwartungssoftware und der Grund für die Installation sowie den Einsatz den Nutzern der Rechen- und Kommunikationstechnik nachvollziehbar dargelegt.
- (5) Jede interne Fernsteuerungsverbindung muss von dem betroffenen Nutzer aktiv durch Einschalten der Fernsteuerungssoftware auf der Benutzerseite mitgetragen werden.

- (6) Vor jeder neuen Fernsteuerungsverbindung muss der betroffene Nutzer sein Einverständnis erklären.

§ 18 Inkrafttreten

- (1) Diese Satzung tritt am Tag nach ihrer Bekanntmachung in Kraft.
- (2) Mit Inkrafttreten dieser Satzung tritt die Verwaltungs- und Benutzungsordnung für das Rechenzentrum der Fachhochschule Nürtingen vom 26. November 2002 sowie die Betriebsordnung des Rechenzentrums der Hochschule für Wirtschaft und Umwelt Nürtingen - Geislingen vom 04. April 2005 außer Kraft.

Nürtingen, den 24. Januar 2013



Prof. Dr. Werner Ziegler
Rektor

Bekanntmachung:

Durch Anschlag bekannt gemacht (Standort Nürtingen, Verwaltungsgebäude V I, Neckarsteige 8, EG)

angeschlagen am: 28.01.2013 we

abgenommen am: 12.02.2013 we

Für die Richtigkeit:



R. Bosch
Kreuzlingen