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

Vom 2. Juni 2026

Aufgrund von § 8 Abs. 5 des Landeshochschulgesetzes (LHG) in der Fassung vom 1. Januar 2005, zuletzt geändert durch Artikel 5 des Gesetzes vom 11. Dezember 2025 (GBl. 2025 Nr. 139), hat der Senat in seiner Sitzung am 21.05.2026 die nachstehende Betriebsordnung der IT-Dienste beschlossen.

Inhaltsverzeichnis

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*innen.

§ 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 transparent zu machen,
3. die personenbezogenen Daten der Nutzer*innen zu schützen,
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 der Leitung der 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) ***Administrator*innen*** sind von den IT-Diensten bestellte Personen, die für die rechen- und kommunikationstechnischen Einrichtungen und Systeme in ihrem Aufgabenbereich verantwortlich sind.

(3) ***Systembetreuer*innen*** haben Administrationsrechte für Teilbereiche und dürfen nur in Absprache mit den IT-Diensten bestellt werden. Die Leitung der IT-Dienste ist weisungsbefugt und kann die Bestellung jederzeit widerrufen.

(4) **Nutzer*innen** sind dem Benutzerkreis zugehörige gem. § 3.

(5) Die Begriffsbestimmung der **Mitglieder** und **Angehörigen** der Hochschule finden sich in der aktuellen Grundordnung.

(6) **Lehrbeauftragte** im Sinne dieser Ordnung sind Gastwissenschaftler*innen als auch Gastprofessor*innen sowie nebenberuflich Lehrende.

(7) ***Server*** sind IT-Systeme, die anderen IT-Systemen innerhalb oder außerhalb des Hochschulnetzes Speicherplatz, Dienste oder sonstige Ressourcen zur Verfügung stellen.

(8) ***Verkehrsdaten*** (Nutzungsdaten) sind technische Informationen, die bei Nutzung der Systeme anfallen, bspw. Beginn und Ende einer Verbindung.

(9) ***Externe Fernwartung*** wird durch einen fremden Dritten mit Rechnern, die sich außerhalb des Hochschulnetzes befinden, durchgeführt.

(10) ***Interne Fernwartung*** wird durch Administrator*innen oder Systembetreuer*innen ausschließlich innerhalb des Hochschulnetzes auf hochschuleigenen Geräten durchgeführt.

2. Abschnitt - Rechen- und Kommunikationstechnik

§ 6 Zentrale Benutzerkennung

(1) Für die Nutzer*innen der rechen- und kommunikationstechnischen Einrichtungen und Systeme der HfWU wird die Benutzerkennung 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 Benutzerkennung erhalten Studierende, Professor*innen (ausgenommen Lehrbeauftragte) sowie Mitarbeitende ein sogenanntes Homeverzeichnis für die zentrale Ablage von Daten. Auf dieses Homeverzeichnis hat allein die/der Nutzer*in Zugriff. Allen Nutzer*innen steht jeweils ein maximales Speichervolumen zur Verfügung, dessen Größe auf den internen Plattformen veröffentlicht wird. Regelmäßig gesicherter Speicherplatz mit hoher Verfügbarkeit kann nicht in beliebiger Höhe zur Verfügung gestellt werden.

(3) Beim Ausscheiden von Nutzer*innen werden die persönlichen Daten in den verschiedenen IT-Systemen inkl. Benutzerkennung und E-Mail-Konto (gem. § 7) nach einer definierten Karenzzeit nach dem Austrittsdatum gelöscht. Professor*innen bleibt beim Übergang in den Ruhestand der Zugang zum Hochschulnetz sowie die Nutzung des Mailsystems weiterhin erhalten, sofern die geforderten Informationssicherheitsschulungen erfolgreich absolviert wurden. Eine Löschung erfolgt dann nur auf Antrag der/des Professors*in. Die Löschung der Benutzerkennungen von Studierenden erfolgt nach den Vorgaben der DatenschutzS der HfWU.

(4) Alle Nutzer*innen sind verpflichtet, ausschließlich mit der Benutzerkennung zu arbeiten, deren Nutzung im Rahmen der Zulassung gestattet wurde.

(5) Die Benutzerkennung sowie die rechen- und kommunikationstechnischen Einrichtungen und Systeme der HfWU sind ausschließlich für Hochschulzwecke zu verwenden (bspw. Lehr-, Forschungs- und Dienstaufgaben). Die Nutzung für private Zwecke ist untersagt, es sei denn, eine Privatnutzung ist ausdrücklich zugelassen (Anlage 1).

(6) Die Weitergabe der Benutzerkennung ist unzulässig. Alle Nutzer*innen haben dafür Sorge zu tragen, dass unberechtigten Personen die Nutzung ihrer persönlichen Benutzungskennung verwehrt wird. Dazu gehört die sorgfältige Wahl eines komplexen Passwortes. Es ist untersagt, fremde Benutzerkennungen zu ermitteln und zu nutzen. Die Passwortvergabe sollte den aktuellen Sicherheitsrichtlinien entsprechen (diese werden auf den internen Plattformen veröffentlicht).

(7) Auf schriftlichen Antrag kann ein personenneutraler Account bestehend für Struktureinheiten, Funktionseinheiten oder Institute vergeben werden. Diese Vergabe unterliegt strengen Kriterien um eine missbräuchliche Nutzung dieser personenneutralen Accounts zu verhindern.

§ 7 E-Mail

(1) Die Nutzer*innen 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 und Lehrbeauftragten aus Vorname.Nachname@hfwu.de. Sollte der Benutzername einen Umfang von 17 Buchstaben überschreiten, wird dieser ausschließlich aus dem Nachnamen gebildet. Bei Gleichnamigkeit der E-Mail-Adressen, wird zugunsten der Eindeutigkeit eine Nummer hinzugefügt, bspw. Max.Mustermann1@hfwu.de.

(3) Die IT-Dienste bilden die E-Mail-Adressen für die Lehrbeauftragen aus Vorname.Nachname@lb.hfwu.de. Sollte der Benutzername einen Umfang von 17 Buchstaben überschreiten, wird dieser ausschließlich aus dem Nachnamen gebildet. Bei Gleichnamigkeit der E-Mail-Adressen, wird zugunsten der Eindeutigkeit eine Nummer hinzugefügt, bspw. Max.Mustermann1@lb.hfwu.de.

(4) Für die Studierenden werden die E-Mail-Adressen aus dem Kürzel „st“ sowie einer fortlaufenden 8-stelligen-Nummer gebildet, bspw. –st80000000@stud.hfwu.de. Die schriftliche Einwilligung der Nutzer*innen ist hierfür nicht gesondert erforderlich.

(5) Für personenneutrale Accounts wird die E-Mail-Adresse wie folgt gebildet: Struktureinheit@hfwu.de, Funktionseinheit@hfwu.de oder Institutname@hfwu.de.

(6) 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/die Nutzer*in auf diese E-Mails zugreifen. Ist eine Benutzerkennung endgültig gelöscht, werden E-Mails an die damit verbundenen E-Mail-Adressen abgewiesen.

(7) 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 des Rektorats organisiert.

(8) E-Mails werden auf Spam-/Phishing-Mails, Schadsoftware sowie gefährdende Anhänge überprüft und ggf. gefahrenabwendende Maßnahmen ergriffen. Weiterführende Informationen werden auf den internen Plattformen veröffentlicht.

(9) Den Nutzer*innen steht jeweils 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 werden auf den internen Plattformen veröffentlicht.

§ 8 Externe Systeme

Die Nutzung von rechen- und kommunikationstechnischen Einrichtungen und Systeme Dritter (bspw. Cloudsysteme), die eine Verbindung zu IT-Systemen der Hochschule herstellen, bedürfen der vorherigen Zustimmung durch die Leitung der IT-Dienste.

§ 9 Software

(1) Die IT-Dienste stellen den Professor*innen und Mitarbeitenden, die einen Rechner von ihrer Organisationseinheit erhalten, eine Grundinstallation bereit.

(2) 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 Softwareprodukts.

(3) Alle für die dienstliche Nutzung benötigten Softwareprodukte, sind von den Nutzer*innen selbst mit einem Softwareantrag und gemäß den aktuellen Beschaffungsvorgaben über die IT-Dienste zu beschaffen. Der Softwareantrag ist sowohl bei kostenfreien als auch kostenpflichtigen Cloud-Diensten und Installations-Software notwendig.

(4) Die private Nutzung der für dienstliche Zwecke erworbenen Software setzt voraus, dass diese Nutzungsform in Vertrags- oder Lizenzbestimmungen oder vom Hersteller ausdrücklich genehmigt ist.

(5) Eine dienstliche Nutzung von Hochschul-Software auf privater Hardware muss in den Lizenzrechtsbestimmungen gestattet sein.

(6) 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.

(7) Die Nutzung von privat erworbener Software für dienstliche Zwecke muss durch die Lizenzbestimmungen abgedeckt sein und bedarf der schriftlichen Zustimmung der Leitung der IT-Dienste.

(8) Je nach Softwarevertrag erhält der/die Nutzer*in 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.

(9) Verwendung von Software, die auf Basis der Peer-to-Peer Technologie arbeitet, ist nicht gestattet. Dies betrifft insbesondere Filesharing-Technologien (wie bspw. Tauschbörsen für Musik und Videos).

§ 10 Wireless LAN

(1) Die Nutzung des Wireless Local Area Network (nachfolgend WLAN) der HfWU ist dem in § 3 dieser Benutzerordnung festgelegten Benutzerkreis vorbehalten.

(2) Die Anmeldung erfolgt mit der Benutzerkennung.

(3) Eine Verschlüsselung der WLAN-Kommunikation erfolgt nach aktuellem technischen Standard.

(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. Alle Nutzer*innen sind dazu verpflichtet, dafür zu sorgen, dass das eigene genutzte System aktuellen Sicherheitsvorkehrungen entspricht bspw. durch einen aktuellen Virenscanner 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 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*innen sind hierüber zu informieren.

(4) Protokolle werden nicht zur Verhaltens- und Leistungskontrolle verwendet.

(5) Der Zugriff der Protokolle ist auf die Administrator*innen begrenzt. Protokolle und Protokolldaten werden regelmäßig 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*innen

(1) Die Nutzer*innen 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) Die Nutzer*innen verpflichten 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. in den Räumen der Hochschule den Weisungen des IT-Dienste-Personals Folge zu leisten,
4. die eigene Nutzungsberechtigung auf Verlangen nachzuweisen,
5. Störungen, Beschädigungen und Fehler der rechen- und kommunikationstechnischen Einrichtungen und Systeme den Mitarbeiter*innen der IT-Dienste unverzüglich zu melden und auf Nachfrage Auskunft darüber zu erteilen,
6. ohne ausdrückliche schriftliche Einwilligung der IT-Dienste keine Eingriffe in die rechen- und kommunikationstechnischen Einrichtungen und Systeme sowie des Netzwerks vorzunehmen und die Konfiguration zu verändern (bspw. Anschluss privater Zusatzgeräte),
7. keine privaten Rechner mit dem Hochschulnetzwerk zu verbinden, von dieser Regelung ausgeschlossen ist die WLAN-Nutzung gem. § 10 Wireless LAN,
8. zur Sicherung einer sach- und ordnungsgemäßen Funktion der Datenverarbeitungsanlagen der Leitung der IT-Dienste oder dessen Mitarbeiter*innen auf Verlangen unter Beachtung der Vertraulichkeit Auskünfte über Programme und benutzte Methoden sowie Einsicht in die Programme zu gewähren (insbesondere selbstentwickelte Programme),
9. selbst für die Sicherung der auf den lokalen Festplatten gespeicherten Daten und Programme von Dienstgeräten zu sorgen, und zwar abhängig vom Volumen
    a. durch eine geeignete Übernahme auf zentral bereitgestellte Verzeichnisse (Anlage 2) oder
    b. durch separat zu beschaffenden externen Speichermedien, die nach Maßgabe der IT-Dienste angeschlossen und mittels von den IT-Diensten bereitgestellter Datensicherungssoftware betrieben werden (Anlage 2).
10. gesetzliche Regelungen, die guten Sitten und Rechte Dritter (Marken-, Namens-, Urheber-, Datenschutzrechte usw.) zu beachten,
11. Handlungen zum unberechtigten Erlangen von fremden Programmen, Systemen und Informationen (bspw. Passwörtern) zu unterlassen.

§ 13 Sanktionen bei Missbrauch

(1) Nutzer*innen 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 entstehen.

(2) Maßnahmen nach Abs. 1 sollen grundsätzlich erst nach vorheriger Anhörung des/r Betroffenen erfolgen. Dies gilt nicht bei Gefahr in Verzug. Hierüber ist der/die Betroffene, wenn möglich, unverzüglich zu informieren. Auf Wunsch des/r Betroffenen oder der Leitung der IT-Dienste können Mitarbeitervertretung, Datenschutzbeauftragte oder Hochschulleitung hinzugezogen werden.

(3) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein Verhalten nach Abs. 1 gegeben ist, können die zuständigen Administrator*innen 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/r Nutzer*in

(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/die Nutzer*in 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/Die Nutzer*in haftet auch für Schäden, die im Rahmen der ihm/ihr 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 den internen Plattformen.

(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 der Administrator*innen und Systembetreuer*in

(1) Die Administrator*innen sowie die Systembetreuer*innen wurden über ihre weiteren Rechte und Pflichten in Kenntnis gesetzt. Systembetreuer*innen haben diese anhand einer Verpflichtungserklärung mit Unterzeichnung anerkannt.

(2) Bei Gefahr sind die Administrator*innen 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 Nutzer*innen werden, wenn möglich, nachträglich darüber informiert.

§ 17 Fernwartung

(1) Externe Fernwartung erfolgt nur mit Unternehmen, die einen Dienstleistungsvertrag mit der HfWU abgeschlossen oder in Ausnahmefällen einen Einzelauftrag erhalten haben. Ein Einzelauftrag ist von den Administrator*innen mit ihren Vorgesetzten abzuklären.

(2) Jede externe Fernsteuerungsverbindung muss von den Administrator*innen der IT-Dienste aktiv mitgetragen werden (bspw. durch Einschalten der Fernsteuerungssoftware auf der Benutzerseite).

(3) Bei interner Fernwartung werden die Funktionsweise der Fernwartungssoftware und der Einsatzzweck den Nutzer*innen der Rechen- und Kommunikationstechnik nachvollziehbar dargelegt. Jede interne Fernsteuerungsverbindung muss aktiv durch Einschalten der Fernsteuerungssoftware auf der Benutzerseite mitgetragen werden.

(4) Vor jeder neuen Fernsteuerungsverbindung muss der/die betroffene Nutzer*in das Einverständnis erklären.

§ 18 Inkrafttreten

(1) Diese Satzung tritt am Tag nach ihrer Bekanntmachung in Kraft.

(2) Mit Inkrafttreten dieser Satzung tritt die Betriebsordnung der IT-Dienste der Hochschule für Wirtschaft und Umwelt Nürtingen - Geislingen vom 24. Januar 2013 außer Kraft.

Nürtingen, den 2. Juni 2026

gez.
Prof. Dr. Andreas Frey
Rektor

Anlage 1

Zum Schutz der hochschulspezifischen Informationen sowie zur Sicherstellung der Verfügbarkeit ist die private Nutzung aller rechen- und kommunikationstechnischen Einrichtungen und Systeme der Hochschule mit folgenden Ausnahmen zugelassen:

1. Private Nutzung mit Dienstgeräten

a) Internet-Nutzung mit Dienstgeräten

Die private Internetnutzung ist geringfügig mit aktuellem Browser (Edge, Chrome, Firefox) möglich. Dabei ist mit „geringfügig" eine gelegentliche Nutzung von kurzer Dauer, die nur wenig Datenverkehr verursacht und wenig Speicherplatz in Anspruch nimmt, gemeint. Beispiele hierfür:

- der Aufruf von Webseiten, um Öffnungszeiten, Telefonnummern, die aktuelle Verkehrslage oder allgemeine Informationen zu erfahren

Nicht in diesem Sinne geringfügig sind beispielsweise:
- die Nutzung von Internet-Telefonie und Streaming-Diensten,
- das Herunterladen von großen Dateien

b) Aufgaben mit dienstlichem Bezug

Die Nutzung der Dienstgeräte ist auch für Aufgaben gestattet, die einen wesentlichen dienstlichen Bezug haben (z.B. Zugang zu Dienstaufgaben außerhalb der Arbeitszeit, Erstellung einer Dissertation)

2. Internet- und E-Mail-Nutzung mit Privatgeräten über Eduroam

- Internetnutzung ist erlaubt (ebenso die Nutzung von Internet-Telefonie und Streaming-Diensten)
- Versandt und Empfang von privaten E-Mails ist erlaubt
- das Herunterladen von großen privaten Dateien ist erlaubt

3. Nutzung von Privatgeräten für Dienstaufgaben

a) Dienstliche E-Mail-Nutzung auf Privatgeräten

Der Zugriff über das bereitgestellte Webfrontend (Outlook Web Access) auf das E-Mail-Konto ist zulässig.

Unter bestimmten Rahmenbedingungen ist der Zugriff über private Geräte mit Hilfe eigenständiger Apps auf dienstliche E-Mails gestattet:

- Absicherung des Privatgerätes durch Zugangsbeschränkung (PIN/PW)
- Nur zulässig als Exchange-Postfach oder IMAP
- Und Mails die nicht älter als 14 Tage sind

Die von Microsoft zugelassene Outlook-App ist nicht zulässig (da der Zugriff über diese nicht nach den obigen Vorgaben entsprechend abgesichert werden kann).

b) Nutzung von Authentifikatoren im Zusammenhang mit der Multifaktorauthentifizierung (MFA)

Anlage 2

Bis zu einem Volumen von max. 8 GB erfolgt das Backup der persönlichen Daten der lokalen Festplatten über ein Skript auf das H: Laufwerk. Sollte das bereitgestellte Volumen nicht ausreichen, wendet sich der Anwender an die ITD um über seine Kostenstelle ein externes Speichermedium zu beschaffen, welches über eine von den ITD bereitgestellte Software (derzeit Veeam) die Datensicherung vornimmt.

Das Skript bzw. das Programm liefert einen entsprechenden Hinweis, sofern der Platz auf dem Zielsystem nicht ausreicht. In diesem Fall wendet sich der/die Nutzer*in ebenfalls an die ITD.