Leseabschrift

Benutzungsrahmenordnung (Satzung) für die Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck

vom 29. November 2016 (NBl. HS MSGWG Schl.-H. S. 101)

geändert durch:
Satzung vom 29. August 2017 (NBl. HS MBWK Schl.-H. S. 76)
Satzung vom 14. März 2018 (NBl. HS MBWK Schl.-H. S. 18)
Satzung vom 13. Juni 2018 (NBl. HS MBWK Schl.-H. S. 43)
Satzung vom 12. Oktober 2020 (NBl. HS MBWK Schl.-H. S. 83)
Satzung vom 20. März 2025 (NBl. HS MBWFK Schl.-H. S. 15)

Präambel

Diese Benutzungsrahmenordnung soll die möglichst störungsfreie, ungehinderte und sichere Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck und der ihr angeschlossenen Einrichtungen unter Wahrung der geltenden datenschutzrechtlichen Bestimmungen gewährleisten. Die Benutzungsrahmenordnung sichert die gesetzlich festgelegten Aufgaben der Universität zu Lübeck sowie ihr Mandat zur Wahrung der akademischen Freiheit. Sie stellt Grundregeln für einen ordnungsgemäßen Betrieb der Infrastruktur auf und regelt so das Nutzungsverhältnis zwischen den einzelnen Nutzungsberechtigten und dem Datenverarbeitungsinfrastrukturbetreiber (im Folgenden DV-Betreiber genannt).

§ 1
Geltungsbereich

Diese Benutzungsrahmenordnung gilt für die Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck und der ihr angeschlossenen Einrichtungen. Die Kommunikations- und Datenverarbeitungsinfrastruktur besteht aus den Datenverarbeitungsanlagen, Kommunikationssystemen - einschließlich Telekommunikations-systemen - und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung der Universität zu Lübeck und der ihr angeschlossenen Einrichtungen.

§ 2
Aufgaben des DV-Betreibers

(1) Dem DV-Betreiber obliegen insbesondere folgende Aufgaben:

1. Planung, Realisierung und Betrieb der Kommunikationsinfrastruktur der Universität zu Lübeck für Aufgaben in Forschung, Lehre und Studium, Verwaltung und Krankenversorgung,

2. Koordination der Beschaffung der Kommunikationsinfrastruktur, insbesondere Stellungnahme zu Investitionsmaßnahmen, Nutzungsanalyse vorhandener Systemkomponenten und Bedarfsplanung,

3. Bereitstellung und Aufrechterhaltung eines störungsfreien und möglichst ununterbrochenen Betriebes der Kommunikationsinfrastruktur,

4. Verwaltung der Adress- und Namensräume,

5. Bereitstellung von Kommunikationsdiensten und zentralen Servern,

6. Unterstützung der Nutzungsberechtigten bei der Anwendung der Dienste.

(2) Zur Gewährleistung eines ordnungsgemäßen Betriebes der Kommunikationsinfrastruktur kann der DV-Betreiber weitere Regeln zur Nutzung der Kommunikationsinfrastruktur erlassen, wie z.B. die Nutzung des WLAN, Zugänge zum Datennetz über 802.1x oder technisch organisatorische Vorgaben zum Betrieb der Kommunikationsinfrastruktur.

§ 3
Nutzungsberechtigte

(1) Zur Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur können zugelassen werden:

1. Mitglieder und Angehörige der Universität zu Lübeck nach § 13 HSG,

2. Beauftragte der Universität zu Lübeck zur Erfüllung ihrer Dienstaufgaben,

3. Mitglieder und Angehörige von Einrichtungen, die der Universität zu Lübeck angegliedert sind,

4. Mitglieder und Angehörige des UKSH,

5. Mitglieder und Angehörige anderer Hochschulen aufgrund besonderer Vereinbarung,

6. sonstige staatliche Forschungs- und Bildungseinrichtungen und Behörden des Landes Schleswig-Holstein und der Bundesrepublik Deutschland aufgrund besonderer Vereinbarung,

7. Studentenwerk Schleswig-Holstein.

(2) Andere Personen und Einrichtungen können zu wissenschaftlichen Zwecken oder zur Erfüllung der Aufgaben der Hochschulen des Landes zur Nutzung oder zum Angebot von Diensten durch den DV-Betreiber zugelassen werden, sofern hierdurch die Belange der in Absatz 1 genannten Nutzungsberechtigten nicht beeinträchtigt werden.

(3) Auftragnehmer der Universität zu Lübeck (z.B. Fremdfirmen) können zur Erfüllung ihrer vertraglichen Aufgaben zum Angebot von Diensten durch den DV-Betreiber zugelassen werden, sofern hierdurch die Belange der in Absatz 1 genannten Nutzungsberechtigten nicht beeinträchtigt werden. Hiervon ausgenommen sind private Nutzungen.

(4) Jede und jeder Nutzungsberechtigte im Sinne der Absätze 1 bis 3 ist dazu verpflichtet, den Datenschutz-Selbstlernkurs mit Erhalt der IDM-Zugangsdaten spätestens innerhalb von zwei Wochen nach deren Erhalt zu absolvieren. Der Datenschutz-Selbstlernkurs steht zur Verfügung unter https://weiterbildung.uni-luebeck.de/course/view.php?name=Awareness-DS.

§ 4
Zulassung und Nutzung von Internet und E-Mail

(1) Die Zulassung erfolgt grundsätzlich automatisiert nach Einstellung oder Immatrikulation. Andernfalls auf Antrag mit Formblatt „Antrag auf Zugang zur Datenverarbeitungsinfrastruktur der Universität zu Lübeck".

(2) Die Nutzungserlaubnis ist auf die Zeit des Studiums, der Tätigkeit oder des beantragten Vorhabens an der Universität zu Lübeck und der ihr angeschlossenen Einrichtungen befristet.

(3) Die Zulassung zur Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur erfolgt grundsätzlich ausschließlich zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, für Zwecke der universitären Verwaltung, der Aus- und Weiterbildung sowie zur Erfüllung sonstiger gesetzlicher Aufgaben der Universität zu Lübeck.

(4) Die private nichtkommerzielle Nutzung der Internetdienste wird durch die Universität zu Lübeck mit Ausnahme der Personengruppe unter § 3 Absatz 3 gestattet, wenn sie nur geringfügig ist und die Zweckbestimmung der Kommunikations- und Datenverarbeitungsinfrastruktur sowie die Belange und Rechte der anderen Nutzungsberechtigten nicht beeinträchtigt werden.

(5) Zum Schutz der IT-Systeme vor Viren und Trojanern und ähnlichen Bedrohungen ist es nicht gestattet, mit dienstlich genutzten Endgeräten Dateien aus dem Internet und E-Mail-Anhänge zu privaten Zwecken herunterzuladen, zu öffnen und zu speichern. Unzulässig ist die Internetnutzung für Glücksspiele, Wetten und ähnliche Internetaktivitäten, die ein Suchtpotential und damit gesundheitliches Gefährdungspotential für Nutzungsberechtigte besitzen.

(6) Die Gestattung der privaten Nutzung des Internetzugangs nach den Vorgaben dieser Benutzungsrahmenordnung erfolgt jedoch ausschließlich gegenüber denjenigen, die zuvor ihre Einwilligung gemäß der Anlage 1 erklärt haben. Die Abgabe der Einwilligungserklärung ist freiwillig und für die Zukunft frei widerruflich. Soweit die Einwilligung jedoch nicht erteilt wird, so ist nur eine dienstliche/studentische Nutzung zulässig. Die Einräumung der privaten Nutzungsmöglichkeit in diesem Umfang ist eine rein freiwillige Leistungsausweitung der Universität zu Lübeck und unter Angaben von konkreten Gründen widerruflich. Mit der

Erlaubnis zur privaten Nutzung des Internetzugangs ist kein Anspruch auf Verfügbarkeit des Dienstes und Betreuung begründet.

(7) Die Nutzung von E-Mail-Konten der Universität zu Lübeck ist ausschließlich für dienstliche/studentische Zwecke zulässig. Somit ist es untersagt, den dienstlichen/studentischen E-Mail-Account für privaten E-Mail-Verkehr zu nutzen.

(8) Der lesende und schreibende Zugriff auf ein privates, bei einem externen Dienstanbieter geführten E-Mail-Postfach (Web-Mail) ist den Beschäftigten/Studierenden gestattet, soweit dienstliche/studentische Interessen nicht entgegenstehen und dazu keine zu dienstlichen Zwecken zur Verfügung gestellten E-Mail-Programme verwendet werden.

(9) Wenn bei einer eingehenden E-Mail die absendende Stelle, der Inhalt oder die Anlage zweifelhaft erscheint, ist unverzüglich das IT-Service-Center zu informieren. Dieses entscheidet über die weitere Behandlung und informiert ggf. das Präsidium.

(10) Eine E-Mail mit vertraulichem Inhalt oder mit personenbezogenen Daten darf extern (außerhalb des Datennetzes der Universität zu Lübeck) nur versandt werden, wenn die Nachricht verschlüsselt ist und die Empfängerin oder der Empfänger zur Entschlüsselung der E-Mail in der Lage ist. Sicher gekoppelte andere Verwaltungsnetze (z.B. über VPN – Virtual Private Network) gelten in diesem Sinne als intern.

(11) Der DV-Betreiber kann die Zulassung zur Nutzung von vorhandenen Kenntnissen über die Benutzung der Kommunikations- und Datenverarbeitungsinfrastruktur abhängig machen. Die Kenntnisse können zu Beginn der Tätigkeit/des Studiums an der Universität zu Lübeck durch Teilnahme an einer Einführungsveranstaltung erworben werden.

(12) Zur Gewährleistung eines ordnungsgemäßen und störungsfreien Betriebes kann der DV-Betreiber die Nutzungserlaubnis überdies mit einer Begrenzung der Onlinezeit sowie mit anderen nutzungsbezogenen Bedingungen und Auflagen verbinden.

(13) Wenn die Kapazitäten der Kommunikations- und Datenverarbeitungsinfrastruktur nicht ausreichen, um allen Nutzungsberechtigten gerecht zu werden, können die Betriebsmittel für die einzelnen Nutzungsberechtigten entsprechend kontingentiert werden, da die Zulassung nur im Rahmen der verfügbaren Kapazitäten erfolgen kann.

(14) Die Nutzungserlaubnis kann vom DV-Betreiber ganz oder teilweise versagt, widerrufen oder nachträglich beschränkt werden, insbesondere wenn

1. kein ordnungsgemäßer Antrag vorliegt oder die Angaben im Antrag nicht oder nicht mehr zutreffen,

2. die Voraussetzungen für eine ordnungsgemäße Benutzung der Kommunikations- und Datenverarbeitungsinfrastruktur nicht oder nicht mehr gegeben sind,

3. die nutzungsberechtigte Person nach § 7 von der Benutzung ausgeschlossen worden ist,

4. das geplante Vorhaben der Nutzungsberechtigten nicht mit den Aufgaben der Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck und den in § 4 Absatz 3 bis 10 genannten Zwecken vereinbar ist,

5. die vorhandene Kommunikations- und Datenverarbeitungsinfrastruktur für die beantragte Nutzung ungeeignet oder für besondere Zwecke reserviert ist,

6. die Kapazität der Ressourcen, deren Nutzung beantragt ist, wegen einer bereits bestehenden Auslastung für die geplante Nutzung nicht ausreicht,

7. die zu benutzenden DV-Komponenten an ein Netz angeschlossen sind, das besonderen Datenschutzerfordernissen genügen muss und kein sachlicher Grund für die geplante Nutzung ersichtlich ist,

8. zu erwarten ist, dass durch die beantragte Nutzung andere berechtigte Vorhaben in unangemessener Weise beeinträchtigt werden.

§ 5
Nutzung privater mobiler Endgeräte

(1) Für die Durchführung dienstlicher Kommunikation (Video-, Webkonferenz- und Telefonietool) und dienstlichen E-Mail-Verkehrs ist die Nutzung eines privaten mobilen Endgeräts zulässig. Ein Anspruch besteht nicht. Bei der Nutzung von privaten mobilen Endgeräten sind folgende Grundsätze zu beachten:

1. Betriebssysteme sind stets aktuell zu halten; Sicherheitspatches sind umgehend einzuspielen.

2. Ein lokaler Virenschutz und/oder eine lokale Firewall ist stets aktuell zu halten und eingeschaltet zu lassen.

3. Eine verschlüsselte Kommunikation mit der Universität zu Lübeck ist vorzuziehen.

4. Zu bearbeitende Daten sind auf IT-Systemen der Universität zu Lübeck oder ihrer Institute zu speichern. Das Speichern von personenbezogenen Daten der Universität zu Lübeck auf lokalen privaten (NAS) Systemen und/oder privaten USB-Sticks oder -Systemen ist untersagt.

5. Für das Speichern von personenbezogenen Daten in einer Cloud ist ausschließlich die Nutzung der universitären Cloud gestattet.

(2) Dienstliche Kommunikation und dienstlicher E-Mail-Verkehr im Sinne von Absatz 1 Satz 1 ist als informeller Austausch zu verstehen, nicht als mobiles Arbeiten. Das Bearbeiten von dienstlichen Dokumenten von mobilen privaten Endgeräten via VPN, Cloud oder SSL-Gate-Techniken ist nur mit dienstlichen Endgeräten gestattet. Der informelle Austausch ist als Lesen und Beantworten von Chats und E-Mails sowie als Einsichtnahme in Kalender und deren Benachrichtigungen zu verstehen.

(3) Die Berechtigung zur Nutzung privater mobiler Endgeräte zu dienstlichen Zwecken umfasst auch die Nutzung von auf dem jeweiligen Endgerät installierten Diensten und Anwendungen, soweit sie für die dienstliche Tätigkeit notwendig sind (z.B. 2-Faktor-Authentifizierung). Ein Anspruch auf Verfügbarkeit der Dienste und Anwendungen besteht nicht.

(4) Berechtigt zur Nutzung privater mobiler Endgeräte sind alle Nutzungsberechtigten im Sinne des § 3.

(5) Zwischen privaten und dienstbezogenen Daten ist zu trennen. Die oder der Nutzungsberechtigte ist verpflichtet,

1. dienstbezogenen Daten umgehend zu löschen (z.B. im Download-Ordner), sobald sie nicht mehr benötigt werden,

2. dienstbezogene Daten gegen den Zugriff Dritter zu sichern (z.B. durch gesperrte Smartphones/Tablets mit PIN, Muster, Fingerabdruck, Gesichtserkennung).

(6) Die oder der Nutzungsberechtigte trägt alle im Zusammenhang mit der Anschaffung und dem Betrieb des privaten mobilen Endgeräts anfallenden Kosten. Dazu zählen insbesondere

1. die Kosten für das private mobile Endgerät selbst sowie Zubehör und Anwendungen, die nicht von der Universität zu Lübeck zur Verfügung gestellt werden,

2. sämtliche Kosten, die im Zusammenhang mit der Nutzung des privaten mobilen Endgeräts anfallen (inklusive Kosten für Datenverbindungen).

(7) Die Universität zu Lübeck haftet nicht für Verlust oder Beschädigung des privaten mobilen Endgeräts. Dies gilt auch für installierte Anwendungen, private Daten und sonstige Inhalte. Für den Fall des Verlusts, des Diebstahls, der Zerstörung, der dauerhaften Überlassung an einen Dritten oder der Pfändung des privaten mobilen Endgeräts, hat die oder der Nutzungsberechtigte unverzüglich, spätestens innerhalb von 24 Stunden (auch an Wochenenden), das IT-Service-Center der Universität zu Lübeck zu unterrichten und mitzuteilen, ob aufgrund dieses Ereignisses die Gefahr der Verletzung des Schutzes personenbezogener Daten besteht. Bei Weitergabe, Veräußerung oder dauerhafter Überlassung des privaten mobilen Endgeräts an einen Dritten sind geeignete Maßnahmen zum Schutz der Daten zu treffen, sie beispielsweise die Rückstellung auf Werkseinstellungen und die sichere Löschung der Festplatten.

(8) Absatz 1 bis 7 gilt nicht für die Nutzung privater mobiler Endgeräte für die Erreichbarkeit im Rahmen einer Havarie oder des Krisenmanagements der Universität zu Lübeck, soweit arbeitsvertraglich nichts anderes geregelt ist. Absatz 1 bis 7 gilt auch nicht für die Nutzung privater mobiler Endgeräte bei der Entgegennahme dienstlicher Kommunikation oder dienstlichen E-Mailverkehrs außerhalb der Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck, es sei denn, der Empfänger hat den Zugang hierfür eröffnet.

§ 6
Nutzung von Voice-over-IP (VoIP) und Collaboration-Dienst

(1) Das VoIP-System dient ausschließlich der Nachrichtenübermittlung. Die Nutzung des VoIP-Systems und der damit verbundenen Kommunikationsdienste werden in der „Richtlinie über den Betrieb und die Nutzung eines auf Voice-over-IP basierenden Telekommunikationssystems der Universität zu Lübeck“ geregelt.

(2) Der Collaboration-Dienst dient ausschließlich der Nachrichtenübermittlung. Die Nutzung des Collaboration-Dienstes und der damit verbundenen Kommunikationsdienste werden in der „Richtlinie über den Betrieb und die Nutzung einer funktionsübergreifenden Kommunikationsplattform der Universität zu Lübeck“ geregelt.

§ 7
Rechte und Pflichten der Nutzungsberechtigten

(1) Die nutzungsberechtigten Personen (Nutzungsberechtigte) haben das Recht, die Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck im Rahmen der Zulassung und nach Maßgabe dieser Benutzungsrahmenordnung zu nutzen. Eine hiervon abweichende Nutzung bedarf einer gesonderten Zulassung durch den DV-Betreiber.

(2) Die Nutzungsberechtigten sind verpflichtet,

1. die Vorgaben dieser Benutzungsrahmenordnung zu beachten,

2. alle im Rahmen ihrer Beschäftigung für die Universität zu Lübeck erzeugten Daten nach Maßgabe der jeweiligen Bereichsleitung in universitären Verzeichnissen (z.B. Teamlaufwerk, etc.) zu sichern,

3. alles zu unterlassen, was den ordnungsgemäßen Betrieb der Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck stört,

4. alle Datenverarbeitungsanlagen, Informations- und Kommunikationssysteme und sonstigen Einrichtungen der Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck und der ihr angeschlossenen Einrichtungen sorgfältig und schonend zu behandeln,

5. ausschließlich mit den Benutzungskennungen zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde,

6. dafür Sorge zu tragen, dass keine anderen Personen Kenntnis von den Benutzerpasswörtern erlangen, sowie Vorkehrungen zu treffen, damit unberechtigten Personen der Zugang zu der Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck verwehrt wird; dazu gehört auch der Schutz des Zugangs durch ein geheim zu haltendes und geeignetes, d.h. nicht einfach zu ermittelndes Passwort (siehe IT-Sicherheitsrichtlinie),

7. fremde Benutzerkennungen und Passwörter weder zu ermitteln noch zu nutzen,

8. keinen unberechtigten Zugriff auf Informationen anderer Nutzungsberechtigter zu nehmen und bekannt gewordene Informationen anderer Nutzungsberechtigter nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern,

9. bei der Benutzung von Software, Dokumentationen und anderen Daten die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten von der Universität zu Lübeck zur Verfügung gestellt werden, zu beachten,

10. die bereitgestellte Software, Dokumentationen und Daten weder zu kopieren noch an Dritte weiterzugeben, sofern dies nicht ausdrücklich erlaubt ist, noch zu anderen als den erlaubten Zwecken zu nutzen,

11. Störungen, Sicherheitsbedenken, Beschädigungen und Fehler an der Kommunikations- und Datenverarbeitungsinfrastruktur nicht selbst zu beheben, sondern dem DV-Betreiber oder den zuständigen Administratoren unverzüglich und ausschließlich zu melden,

12. keine unautorisierten Eingriffe in die Hardwareinstallation von zur Nutzung bereitgestellter Kommunikations- und Datenverarbeitungsinfrastruktur vorzunehmen und die Konfiguration der Betriebssysteme, der Systemdateien, der systemrelevanten Nutzerdateien und des Datennetzes nicht zu verändern,

13. dem DV-Betreiber und der oder dem Datenschutzbeauftragten auf Verlangen in begründeten Einzelfällen – insbesondere bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung – zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu erteilen sowie Einsicht in die Programme zu gewähren, mit Ausnahme der unter das Telekommunikations- und Datengeheimnis fallenden Nutzerdaten,

14. eine Verarbeitung personenbezogener Daten mit dem DV-Betreiber und der oder dem Datenschutzbeauftragten abzustimmen und – unbeschadet der eigenen datenschutzrechtlichen Verpflichtungen der Nutzungsberechtigten – die vom DV-Betreiber erlassenen Datenschutz- und Datensicherheitsvorkehrungen strikt einzuhalten.

(3) Auf die folgenden Straftatbestände wird besonders hingewiesen:

1. Ausspähen von Daten (§ 202a StGB),

2. Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB),

3. Computerbetrug (§ 263a StGB),

4. Verbreitung pornographischer Darstellungen (§§ 184 ff. StGB), insbesondere Verbreitung, Erwerb und Besitz kinderpornographischer Schriften (§ 184b StGB) und die Verbreitung pornographischer Darbietungen durch Rundfunk, Medien- oder Teledienste (§ 184c StGB),

5. Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB),

6. Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB),

7. strafbare Urheberrechtsverletzungen, z.B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG).

(4) Zudem wird auf folgende zusätzlich einzuhaltende Vorschriften hingewiesen:

1. Allgemeines Persönlichkeitsrecht (APR), das sich auf Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz stützt und die Individual-, Privat-, Intimsphäre einem besonderen Schutz unterstellt,

2. Kunsturheberrechtsgesetz (KUG), das das Recht am eigenen Bild regelt (§ 22 KUG),

3. Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG), die den rechtlichen Rahmen für so genannte Telemedien in Deutschland setzen,

4. Benutzungsordnung des Deutschen Forschungsnetzes (DFN, http://www.dfn.de),

5. Richtlinie des Präsidiums der Universität zu Lübeck zur Nutzung der EDV-Pools.

6. Für die Beschäftigten der Universitätsverwaltung (ZUV, Zentrale Einrichtungen): „Dienstanweisung über die Erreichbarkeit am Arbeitsplatz“, die die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz regelt.

§ 8
Einschränkung und Ausschluss von der Nutzung

(1) Nutzungsberechtigte können vorübergehend oder dauerhaft in der Benutzung der Kommunikations- und Datenverarbeitungsinfrastruktur beschränkt oder hiervon ausgeschlossen werden, wenn

1. sie schuldhaft gegen diese Benutzungsrahmenordnung, insbesondere gegen die in § 4 aufgeführten Pflichten, verstoßen, bspw.

   a) Missachtung der Benutzungsrahmenordnung,
   b) Störung des ordnungsgemäßen Betriebs,
   c) Arbeit mit nicht zugelassener Benutzungskennung,
   d) fehlende Vorkehrung gegen unberechtigten Zugang zur Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck,
   e) Ermittlung sowie Nutzung fremder Benutzerkennungen und Passwörter,
   f) unberechtigte Zugriffe auf Informationen anderer Nutzungsberechtigter sowie deren weiterer Gebrauch,
   g) Verstoß gegen gesetzliche Vorgaben, z.B. Urheberrechtsschutz,
   h) unerlaubte Nutzung, Kopie und Weitergabe von bereitgestellter Software, Dokumentationen und Daten,

i) unautorisierte Eingriffe in die Hardwareinstallation sowie Veränderung der Konfiguration der Betriebssysteme, der Systemdateien, der systemrelevanten Nutzerdateien der Kommunikations- und Datenverarbeitungsinfrastruktur,
j) Verarbeitung personenbezogener Daten ohne Abstimmung mit dem DV-Betreiber und/oder der oder dem Datenschutzbeauftragten

oder

2. sie die Kommunikations- und Datenverarbeitungsinfrastruktur für strafbare Handlungen missbrauchen oder

3. der Universität zu Lübeck, der ihr angeschlossene Einrichtungen oder deren Angehörigen durch sonstiges rechtswidriges Nutzerverhalten Nachteile entstehen oder

4. sie die erforderliche Einwilligungserklärung zur privaten Nutzung des Internetzugangs nicht unterzeichnet haben. In diesem Fall ist die private Internetnutzung untersagt.

(2) Maßnahmen nach Absatz 1 erfolgen erst nach vorheriger Ermahnung. Betroffenen ist Gelegenheit zur Stellungnahme zu geben.

(3) Vorübergehende Nutzungseinschränkungen sind aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet ist.

(4) Eine dauerhafte Nutzungseinschränkung oder der vollständige Ausschluss der Nutzungsberechtigten von der weiteren Nutzung kommt nur bei schwerwiegenden oder wiederholten Verstößen im Sinne des Absatzes 1 in Betracht. Die Entscheidung über den dauerhaften Ausschluss trifft die Hochschulleitung.

§ 9
Rechte und Pflichten des DV-Betreibers

(1) Der DV-Betreiber dokumentiert die erteilten Benutzungsberechtigungen sowie E-Mail-Adressen der zugelassenen Nutzungsberechtigten.

(2) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutz der Nutzerdaten erforderlich ist, kann der DV-Betreiber die Nutzung seiner Ressourcen vorübergehend einschränken oder einzelne Nutzerkennungen oder Netzzugänge vorübergehend sperren. Sofern möglich, sind die betroffenen Nutzungsberechtigten hierüber im Voraus zu unterrichten.

(3) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass Nutzungsberechtigte rechtswidrige Inhalte zur Nutzung im Datennetz bereitstellen, kann der DV-Betreiber die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.

(4) Der DV-Betreiber ist berechtigt, die Sicherheit der System-/Benutzerpasswörter und der Nutzerdaten durch regelmäßige automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen zu ergreifen, z.B. Änderungen leicht zu erratender Passwörter

durchzuführen, um die Kommunikations- und Datenverarbeitungsinfrastruktur und Benutzerdaten vor unberechtigten Zugriffen Dritter zu schützen. Bei erforderlichen Änderungen der Benutzerpasswörter, der Zugriffsberechtigungen auf Nutzerdateien und sonstigen nutzungsrelevanten Schutzmaßnahmen sind die Nutzungsberechtigten hiervon unverzüglich in Kenntnis zu setzen.

(5) Der DV-Betreiber ist nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der Kommunikations- und Datenverarbeitungsinfrastruktur durch die einzelnen Nutzungsberechtigten zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist

1. zur Gewährleistung eines ordnungsgemäßen Systembetriebs,

2. zur Ressourcenplanung und Systemadministration,

3. zum Schutz der personenbezogenen Daten anderer Nutzungsberechtigter,

4. für das Erkennen und Beseitigen von Störungen sowie

5. zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

(6) Unter den Voraussetzungen des Absatzes 5 ist der DV-Betreiber auch berechtigt, unter Beachtung des Datengeheimnisses Einsicht in Programme und Dateien von Nutzungsberechtigten zu nehmen, soweit dies zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Missbräuchen erforderlich ist und sofern hierfür tatsächliche Anhaltspunkte vorliegen. Eine Einsichtnahme in die Nachrichten- und E-Mail- Postfächer ist jedoch nur zulässig, soweit dies zur Behebung aktueller Störungen im Nachrichtendienst unerlässlich ist. In jedem Fall ist die Einsichtnahme zu dokumentieren, und die betroffenen Nutzungsberechtigten sind unverzüglich zu benachrichtigen.

(7) Unter den Voraussetzungen des Absatzes 5 können auch Verkehrs- und Nutzungsdaten im Nachrichtenverkehr, insbesondere der E-Mail-Nutzung, dokumentiert werden. Es dürfen jedoch nur die näheren Umstände der Telekommunikation – nicht aber die nichtöffentlichen Kommunikationsinhalte – erhoben, verarbeitet und genutzt werden. Die Verkehrs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Telemediendiensten, die der DV-Betreiber zur Nutzung bereithält oder zu denen der DV-Betreiber den Zugang zur Nutzung vermittelt, sind frühestmöglich, spätestens am Ende der jeweiligen Nutzung zu löschen.

(8) Die gesetzlichen Regelungen nach der Europäischen Datenschutzgrundverordnung (EU-DSGVO) sowie nach dem Schleswig-Holsteinischen Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -) in der jeweils geltenden Fassung werden eingehalten.

§ 10
Protokollierung und Kontrolle

(1) Eine Protokollierung der Nutzung der Dienste (Nutzungs-, Verkehrs- und Inhaltsdaten) erfolgt, soweit unbedingt erforderlich

1. aus Gründen der Daten- und Systemsicherheit,
2. aus Gründen der Systemtechnik (z.B. zur Fehlerverfolgung) und
3. aus Gründen der Arbeitsorganisation (z.B. zur Feststellung von Art und Umfang der Nutzung),
4. zur Missbrauchskontrolle (sofern sich bei der stichprobenartigen Auswertung der Daten Hinweise auf unzulässige Zugriffe oder Überschreitung der erlaubten Nutzung ergeben).

(2) Für die Nutzung des Internets werden folgende Informationen protokolliert:

1. Datum/Uhrzeit,
2. Quell-IP-Adresse,
3. Ziel-IP-Adresse,
4. Übertragene Datenmenge.

(3) Ein- und ausgehende E-Mails werden mit folgenden Informationen protokolliert:

1. Datum/Uhrzeit,
2. Absender- und Empfängeradresse,
3. Message-ID,
4. Nachrichtengröße,
5. EventID (z.B. Redirect, Transfer, Receive),
6. Quell-IP-Adresse,
7. Ziel-IP-Adressen,
8. MessageInfo.

(4) Die Protokolldaten der Absätze 2 und 3 werden ausschließlich zu Zwecken der Analyse und Korrektur technischer Fehler, Gewährleistung der Systemsicherheit, Optimierung des Netzes und Datenschutzkontrolle verwendet. Die Protokolldaten werden nur so lange aufbewahrt, wie es für die Zweckerreichung erforderlich ist, und nach max. 60 Tagen gelöscht. Die Einhaltung aller datenschutzrechtlichen Bestimmungen ist zu gewährleisten. Bei Vorliegen eines auf zu dokumentierende tatsächliche Anhaltspunkte begründeten Missbrauchsverdachts bei der Internet- oder E-Mail-Nutzung dürfen die Protokolldaten der Absätze 2 und 3 personenbezogen ausgewertet werden. Die Protokolldaten sind zu löschen, sobald feststeht, dass sich der Verdacht als begründet oder unbegründet erwiesen hat, sofern sie nicht noch für die Zwecke nach Absatz 1 benötigt werden.

(5) Personal, das Zugang zu den Protokollinformationen hat, wird besonders auf die Sensibilität dieser Daten hingewiesen und auf die Einhaltung des Datenschutzes verpflichtet.

(6) Eine Auswertung von Protokolldaten muss die Grundsätze einer datenschutzgemäßen Kontrolle berücksichtigen, insbesondere den Grundsatz der Verhältnismäßigkeit. Eine

individuelle Verhaltens- und Leistungskontrolle durch eine Auswertung der Protokolldaten ist unzulässig. Auswertungen von Protokolldaten erfolgen grundsätzlich zunächst anonymisiert.

(7) Zur Analyse von deutlich über dem üblichen Nutzungsverhalten liegenden, auffälligen Häufungen im Kommunikationsverhalten und/oder bei extensivem Anstieg von Übertragungsvolumina bzw. besonders hohen Übertragungsvolumina bestimmter Internet- oder externen E-Mail-Domänen können die Daten durch das ITSC monatlich oder aus gegebenem Anlass gesichtet und ausgewertet werden.

(8) Ergeben sich dabei eindeutige Hinweise auf unzulässige Zugriffe oder auf eine deutliche Überschreitung der erlaubten privaten Nutzung (Stufe 1), ist der betroffene Kreis der Nutzungsberechtigten grundsätzlich zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hinzuweisen (Stufe 2). Zugleich wird darüber unterrichtet, dass bei Fortdauer der Verstöße zukünftig eine gezielte Kontrolle (Stufe 3) oder eine arbeitsplatzspezifische Kontrolle (Stufe 4) nach dem in der Anlage 2 beschriebenen Verfahren stattfinden kann.

(9) Die Anlage 2 ist Bestandteil dieser Benutzungsrahmenordnung.

§ 11
Haftung der Nutzungsberechtigten

(1) Die Nutzungsberechtigten haften für alle Nachteile, die der Universität zu Lübeck und der angeschlossenen Einrichtungen sowie deren Angehörigen durch missbräuchliche oder rechtswidrige Verwendung der Kommunikations- und Datenverarbeitungsinfrastruktur und der Nutzungsberechtigung oder dadurch entstehen, dass die Nutzungsberechtigten schuldhaft ihren Pflichten aus dieser Benutzungsrahmenordnung nicht nachkommen.

(2) Die Nutzungsberechtigten haften auch für Schäden, die im Rahmen der ihnen zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn sie diese Drittnutzung zu vertreten haben, insbesondere im Falle einer Weitergabe der Benutzerkennung an Dritte.

(3) Die Nutzungsberechtigten haben die Universität zu Lübeck von allen Ansprüchen freizustellen, wenn Dritte die Universität zu Lübeck wegen eines missbräuchlichen oder rechtswidrigen Verhaltens der Nutzungsberechtigten auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen. Die Universität zu Lübeck wird den Nutzungsberechtigten den Streit verkünden, sofern Dritte in Folge missbräuchlichen oder rechtswidrigen Verhaltens der Nutzungsberechtigten gegen den DV-Betreiber gerichtlich vorgehen.

§ 12
Haftung der Universität zu Lübeck

(1) Die Universität zu Lübeck übernimmt keine Garantie dafür, dass das System fehlerfrei und jederzeit ohne Unterbrechung läuft. Eventuelle Datenverluste infolge technischer Störungen

sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.

(2) Die Universität zu Lübeck übernimmt keine Verantwortung für die Richtigkeit der zur Verfügung gestellten Programme. Die Universität zu Lübeck haftet auch nicht für den Inhalt, insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang zur Nutzung vermittelt.

(3) Im Übrigen haftet die Universität zu Lübeck nur bei Vorsatz und grober Fahrlässigkeit ihrer Mitarbeiter und -innen, es sei denn, dass eine schuldhafte Verletzung wesentlicher Kardinalpflichten vorliegt. In diesem Fall ist die Haftung der Universität zu Lübeck auf typische, bei Begründung des Nutzungsverhältnisses vorhersehbare Schäden begrenzt, soweit nicht vorsätzliches oder grob fahrlässiges Handeln vorliegt.

(4) Mögliche Amtshaftungsansprüche gegen die Universität zu Lübeck bleiben von den vorstehenden Regelungen unberührt.

Anlage 1

Einwilligungserklärung
zur privaten Nutzung des Internetzugangs der Universität zu Lübeck

Ich möchte von dem Angebot Gebrauch machen, den Internetzugang in geringfügigem Umfang auch für private nichtkommerzielle Zwecke zu nutzen.

- Ich habe die Benutzungsrahmenordnung für die Kommunikations- und Datenverarbeitungsinfrastruktur der Universität zu Lübeck in der jeweils geltenden Fassung zur Kenntnis genommen und willige ein, dass mir die private Nutzung des Internets in geringfügigem Umfang für nichtkommerzielle Zwecke gestattet ist. Dies gilt nur, sofern dadurch die dienstliche/studentische Aufgabenerfüllung und die Verfügbarkeit der IT-Systeme für dienstliche/studentische Zwecke und die Belange der anderen Nutzungsberechtigten nicht beeinträchtigt werden.
- Ich willige ein, dass auch meine privaten – also nicht nur die dienstlichen/studentischen – Internetzugriffe im Rahmen der Benutzungsrahmenordnung unter Einhaltung der datenschutzrechtlichen Bestimmungen verarbeitet und protokolliert sowie gemäß § 9 der Benutzungsrahmenordnung personenbezogen ausgewertet werden können.
- Ich willige zudem ein, dass die Nutzung von E-Mail-Konten der Universität zu Lübeck ausschließlich für dienstliche/studentische Zwecke zulässig ist. Somit ist es mir untersagt, den dienstlichen/studentischen E-Mail-Account für private Zwecke zu nutzen. Hiervon ausgenommen ist die Nutzung der universitären E-Mail-Adresse zum Erhalt von studentischen Sonderkonditionen.

Mir ist bewusst, dass ich hierdurch auf den Schutz des Fernmeldegeheimnisses gemäß § 88 Telekommunikationsgesetz (TKG) verzichte.

Ich bin mir darüber im Klaren, dass eine missbräuchliche oder unerlaubte Nutzung neben rechtlichen ggf. arbeitsrechtlichen Konsequenzen auch strafrechtliche Folgen haben kann und dass darüber hinaus ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen kann.

Mir ist bewusst, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, mit der Folge, dass ich ab dem Zeitpunkt des Widerrufs das Internet nicht mehr privat nutzen darf.

Name, Vorname (bitte in Blockbuchstaben)	Matrikelnummer bei Studierenden
Ort, Datum	Unterschrift der/des Nutzungsberechtigten

Anlage 2

Verfahrensbeschreibung zur Überprüfung der gezielten (Stufe 3) und arbeitsplatzspezifischen (Stufe 4) Kontrolle gemäß § 10 Absatz 8 der Benutzungsrahmenordnung

An der Festlegung dieses Verfahrens und Auswertung von Protokolldaten sind die zuständigen Personalvertretungen, das ITSC, die oder der behördliche Datenschutzbeauftragte, ggf. die Gleichstellungsbeauftragte und ggf. die Schwerbehindertenvertretung zu beteiligen. Das Verfahren ist den betroffenen Nutzungsberechtigten bekanntzugeben.

Die Überprüfungen sollten in regelmäßigen Abständen durchgeführt werden. Das geschieht in gemeinsamer Absprache mit den zuständigen Personalvertretungen, dem ITSC, der oder dem behördlichen Datenschutzbeauftragten, ggf. der Gleichstellungsbeauftragten und ggf. der Schwerbehindertenvertretung.

Der Ablauf einer Überprüfung empfiehlt sich wie folgt:

Verfahrensbeschreibung:

1. Einladung der zuständigen Mitgliedervertretung, der oder des behördlichen Datenschutzbeauftragten, einer ITSC-Vertretung, ggf. der Gleichstellungsbeauftragten und ggf. der Schwerbehindertenvertretung durch das Präsidium zu einem Vorbereitungsgespräch des Überprüfungstermins.

2. An diesem Termin werden drei Personen nach dem Zufallsprinzip aus einer Liste ermittelt. Es dürfen nicht alle Nutzungsberechtigten überwacht werden.

3. Diskurs über die Eignung der ausgewählten Personen. Unzulässig sind Auswertungen insbesondere von Protokolldaten (Nutzungs-, Verkehrs- und Inhaltsdaten), um Informationen über die Nutzung des Dienstes Internet und die E-Mail-Kommunikation in Zusammenhang mit besonders zu schützenden Funktionen (zum Beispiel Personalvertretungen, Gleichstellungsbeauftragte, Schwerbehindertenvertretung, behördliche Datenschutz-beauftragte, Personalreferat) zu erlangen.

4. Einigung über einen Überprüfungstermin.

5. Am Überprüfungstermin werden die ausgewählten Personen gebeten, die zuständige Personalvertretung, die oder den behördlichen Datenschutzbeauftragten, eine ITSC-Vertretung (ggf. die Gleichstellungsbeauftragte und ggf. die Schwerbehindertenvertretung) gemeinsam über die Fernwartungssoftware zur Einsichtnahme auf dem dienstlich genutzten Endgerät am Arbeitsplatz zuzulassen.

6. Die ausgewählte Person wird sodann gebeten, das E-Mail-Programm zu öffnen und eine Listenansicht zu maximieren, um die Inhalte der E-Mails auszublenden bzw. zu minimieren.

7. Die Betreffzeilen werden gemeinsam grob überflogen und auf private Merkmale durchgesehen. Der Zeitraum der Kontrolle der E-Mail sollte 3 Monate nicht überschreiten.

8. Der Überprüfungsbesuch sollte nicht länger als 10 Minuten dauern. 5 Minuten zur Vorstellung und Zweck der Überprüfung und 5 Minuten zur Überprüfung selbst.

9. Die Ergebnisse werden den Betroffenen bekanntgegeben. Entsprechend der Ergebnisse ist das weitere Vorgehen abzuwägen:

    a) Einstellen der Kontrollen/keine weitere Überwachung,
    b) erneutes Ermahnen des betroffenen Personenkreises und Fortführen der gezielten Kontrolle oder
    c) Verschärfen der Kontrolle, in dem die Protokollierung auf dem Arbeitsplatzrechner stattfindet (Stufe 4). Für die Protokollierung auf dem Arbeitsplatz gelten dieselben Anforderungen wie in Stufe 3 mit Ausnahme der Ankündigung. Die Beschäftigten müssen über diese Maßnahme aufgeklärt werden. Ggf. kann auch eine Strafanzeige gestellt und es kann eine Strafverfolgungsbehörde hinzugezogen werden.

10. Am Ende wird eine schriftliche Dokumentation mit Unterschriften der Prüfenden über die Überprüfung erstellt.

11. Bei fortgesetzten Verstößen sind dienst- oder arbeitsrechtliche Maßnahmen gegen die betreffenden Beschäftigten nicht ausgeschlossen. Bei Verdacht von Straftaten ist die Auswertung von Protokolldaten den zuständigen Strafverfolgungsbehörden zu überlassen.