Stiftung Tierärztliche Hochschule Hannover
University of Veterinary Medicine Hannover

Verkündungsblatt

Herausgeber: Der Präsident der Tierärztlichen Hochschule Hannover, Bünteweg 2, 30559 Hannover

Hannover, 12. September 2017 Nr. 242/2017

Das Präsidium der Stiftung Tierärztliche Hochschule Hannover hat in seiner Sitzung am 23.08.2017 folgende Richtlinie beschlossen:

Richtlinie des Präsidiums der Stiftung Tierärztliche Hochschule Hannover zur Benutzung der IT-Ressourcen

Präambel

Diese Richtlinie soll die störungsfreie, ungehinderte und sichere Nutzung der IT-Ressourcen der Stiftung Tierärztliche Hochschule Hannover (TiHo) gewährleisten. Die Richtlinie orientiert sich an den gesetzlich festgelegten Aufgaben der Hochschule. Sie stellt Grundregeln für einen ordnungsgemäßen Betrieb der IT-Infrastruktur auf und regelt das Nutzungsverhältnis zwischen den Nutzungsberechtigten und Dezernat 5 „Informations- und Datenverarbeitungsservice“ (nachfolgend IDS), welches die Aufgaben eines Hochschulrechenzentrums im Sinne des NHG übernimmt oder anderen Betreibern von IT-Ressourcen an der Hochschule. Ergänzungen zu dieser Regelung können durch die IT-Betreiber definiert werden.

§ 1 Geltungsbereich

(1) Diese Richtlinie gilt für alle Benutzer der IT-Ressourcen der TiHo.

(2) Unter den Begriff der Informationstechnischen Ressourcen (IT-Ressourcen) fallen alle Datenverarbeitungsanlagen (Server und Arbeitsplatzrechner sowie alle zentralen Datenspeicher) nebst den darauf ausgeführten Rechnerprogrammen sowie das gesamte Datennetz, die im Netz angebotenen Dienste sowie die Infrastruktur für die Telekommunikation.

(3) Zur Nutzung der IT-Ressourcen nach § 1 Abs. 2 können für alle oder einzelne IT-Dienste zugelassen werden:

a. Hochschullehrer, Hochschulbeschäftigte und eingeschriebene Studierende der TiHo;
b. Personen, die nicht Beschäftigte der TiHo sind, sondern in einem anderen Arbeitsverhältnis stehen, deren Arbeitsmittelpunkt sich aber in den Diensträumen der TiHo befindet sowie Stipendiaten. Diese Personen sind Hochschulbeschäftigten hinsichtlich der IT-Nutzung gleichgestellt;
c. Eingeschriebene Studierende anderer staatlicher Bildungseinrichtungen, sofern diese regelmäßig an Lehrveranstaltungen an der TiHo teilnehmen, Schüler der Lehranstalt für VMTAs sowie Teilnehmer des Weiterbildungsprogramms BEST-VET der TiHo.
Diese sind immatrikulierten Studierenden der TiHo hinsichtlich der IT-Nutzung gleichgestellt;

Aus Gründen der besseren Lesbarkeit wird für Amtsbezeichnungen und Personen nur die männliche Sprachform verwendet. Sie soll jeweils die weibliche Sprachform mit umfassen.

d. Personen mit Lehrauftrag und Privatdozenten der TiHo, nur sofern diese mit Aufgaben betreut sind, die einen eigenen Account zwingend voraussetzen, weil die in Zusammenhang mit der Lehrtätigkeit stehenden IT-Zugriffe nicht durch Beschäftigte der Einrichtung, die die Lehrveranstaltung anbietet, übernommen werden können;
e. Praktikanten aufgrund eines bestehenden Praktikantenvertrages;
f. Externe Dienstleister in Zusammenhang mit der Erfüllung von vertraglich vereinbarten Dienstleistungen z.B. Wartungsaufgaben an der technischen oder medizinischen Infrastruktur der TiHo;
g. Gäste mit IT-Berechtigung. Dieser Status kann Kooperationspartnern der Hochschule (aufgrund eines formlosen Antrages an die IDS) durch das Präsidium gewährt werden.

(4) Das Personal des Dezernats 5 - IDS ist berechtigt, bei Störungen der IT-Systeme oder einem Verdacht auf missbräuchliche Nutzung, unter Beachtung der gültigen Datenschutzbestimmungen Maßnahmen einzuleiten, welche die Einhaltung dieser Richtlinie sicherstellen. In diesem Fall sind der Datenschutzbeauftragte und/ oder die Personalvertretung der TiHo zu beteiligen, sofern Rechte von Personen bzw. Beschäftigten der TiHo betroffen sind.

§ 2 Regelungen für Benutzer

(1) Alle Benutzer des Datennetzes und der Rechenanlagen der TiHo erhalten eine „digitale Identität“ in Form einer Benutzerkennung in einem Verzeichnisdienst. Mit dieser Benutzerkennung („Account“) erhalten die Benutzer ein initiales, alsbald zu änderndes Passwort als Zugangsberechtigung, mit denen diese sich abgesicherten Diensten (z.B. zur Anmeldung an PCs oder Serverdiensten) gegenüber authentifizieren können. In diesen Verzeichnisdiensten werden Daten, Passwörter und Berechtigungen der Accounts verwaltet, hierdurch werden ausgewählte Daten und Dienste innerhalb der TiHo provisioniert. Zur Erzeugung und Verwaltung der Accounts und der E-Mailadresse werden für Benutzer im Sinne von § 1 Abs. 3 a) automatisierte Verfahren unter Verwendung elektronischer Daten verwendet. Näheres regeln die Dienstvereinbarungen zum Identitätsmanagement und SAP-HR. Für alle anderen Benutzer werden durch die IDS Verfahren bereitgestellt, die die Anlage und die Pflege der notwendigen Daten für die Anlage der Accounts entsprechend ermöglichen.

(2) Die Benutzerkennung und das dazugehörige Passwort dürfen keinesfalls an Dritte weitergegeben oder von Dritten benutzt werden. Sollte der Verdacht auf Drittnutzung bestehen, so kann die Zugangsberechtigung gesperrt werden. Jeder Benutzer verpflichtet sich zur Geheimhaltung des Passwortes. Sollte er den Verdacht haben, dass das Passwort bekannt geworden ist, ist er verpflichtet, das Passwort umgehend (ggf. mit Hilfe der IDS) zu ändern. Der Benutzer darf fremde Benutzerkennungen weder ermitteln noch nutzen. Den Benutzern ist es des Weiteren untersagt, unberechtigten Zugriff auf Informationen Anderer zu nehmen und bekannt gewordene Informationen Anderer ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu ändern. Entsprechendes gilt für weitere Authentifizierungsmethoden, wie z.B. elektronische Zertifikate oder Chipkarten (TiHo-Karte und Signaturkarte für SAP Zugriffe).

(3) Für Hochschullehrer und -bedienstete der TiHo gilt die Nutzungsberechtigung als erteilt, wenn ein Arbeitsverhältnis besteht und die IT-Nutzung wissenschaftlicher Natur ist oder im Rahmen der Aufgabenerfüllung von Lehre, Forschung, Studium, Dienstleistung, Patientenversorgung und Verwaltungsaufgaben steht. Für dienstliche Zwecke ist die Nutzung von zentral angebotenen IT-Ressourcen verbindlich, wenn eine für die Erfüllung der Aufgaben geeignete zentrale Ressource zur Verfügung steht.

(4) Für Studierende der TiHo gilt die Nutzungsberechtigung als erteilt, wenn eine gültige Immatrikulation besteht und die Nutzung in Zusammenhang mit dem Studium steht.

(5) Eine private Nutzung der IT-Ressourcen ist untersagt. Abweichend hiervon gelten bei der privaten Nutzung der Telefonsysteme durch Beschäftigte gesonderte Regelungen.

(6) Unbeschadet weiterer Regelungen ist generell jede Nutzung der IT-Ressourcen unzulässig, die geeignet ist, den Interessen der TiHo oder deren Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Netzwerks zu beeinträchtigen oder die gegen geltende Rechtsvorschriften verstößt.

(7) Auf die folgenden Straftatbestände wird besonders hingewiesen:

a. Ausspähen von Daten, § 202 a Strafgesetzbuch (StGB);
b. Datenveränderung, § 303 a StGB und Computersabotage, § 303 b StGB;
c. Computerbetrug, § 263 a StGB;
d. Verbreitung pornographischer Darstellungen, § 184 StGB;
e. Verbreitung gewalt- oder tierpornographischer Schriften, § 184 a StGB, Verbreitung, Erwerb und Besitz kinderpornographischer Schriften, § 184 b StGB, Verbreitung, Erwerb und Besitz jugendpornographischer Schriften, § 184 c StGB;
f. Verbreitung von Propagandamitteln verfassungswidriger Organisationen, § 86 StGB und Volksverhetzung, § 130 StGB;
g. Ehrdelikte, §§ 185 ff StGB;
h. strafbare Urheberrechtsverletzungen, z.B. durch urheberrechtswidrige Vervielfältigung von Software, §§ 106 ff UrhG;
i. Verletzung des Datenschutzrechts;
j. Verletzung des Post- oder Fernmeldegeheimnisses, § 206 StGB.

(8) Beendigung der Nutzungsberechtigung

a. Für Hochschulbeschäftigte endet die Nutzungsberechtigung mit dem Ende des Dienstverhältnisses, für Studierende mit der Exmatrikulation.
b. Studierenden wird eine Karenz von 4 Wochen eingeräumt, um den Übergang zwischen verschiedenen Studiengängen zu organisieren.
c. Der Account wird nach Ende der Nutzungsberechtigung deaktiviert. Hiermit verbunden ist der Verlust des Zugriffs auf Daten und Dienste.
d. In Abstimmung mit dem jeweiligen Einrichtungsleiter kann für deaktivierte Accounts eine automatisierte Mitteilung an den Sender einer E-Mail übermittelt werden, z. B. um für eine Übergangszeit eine Nachfolgeregelung mitzuteilen oder um die weitere Bearbeitung projektbezogener Mails zu erleichtern.
e. Es liegt in der Verantwortung der Organisationsverantwortlichen, vor dem Ausscheiden einer oder eines Beschäftigten, die Übergabe der dienstlichen Daten in geeigneter Form sicher zu stellen und irrelevante Anteile zur Einsparung unnötigen Speicherplatzes zu löschen.
f. Abweichend hiervon haben Universitätsprofessoren das Recht, ihren Account und die E-Mailadresse auch nach Ende ihrer Dienstzeit an der TiHo im Ruhestand zu nutzen. Diese Accounts werden deaktiviert, wenn über eine Zeit von 6 Monaten keine Logins erfolgen.

(9) Beschäftigte können (in Absprache mit dem Vorgesetzten) private Geräte benutzen, um an ihren persönlichen Account gerichtete E-Mails im TiHo-Mailsystem zu empfangen oder zu versenden, wenn dies im dienstlichen Interesse liegt. Die IDS stellt hierfür relevante Zugangsinformationen bereit, leistet aber keinen Support zur Konfiguration privater Geräte. Es liegt in der Verantwortung des Besitzers des jeweiligen Gerätes durch geeignete organisatorische und/oder technische Maßnahmen den Zugriffsschutz auf dienstliche Daten zu gewährleisten.

§ 3 Besondere Regelungen für Benutzer im Sinne von § 1 Abs. 3 b. bis g.

(1) Im Zusammenhang mit gegebenen Aufgaben in Forschung, Dienstleistung und Lehre der TiHo können auch Benutzer im Sinne von § 1 Abs. 3 b. bis 3 g. auf Antrag an die IDS mit Zustimmung der jeweiligen Einrichtungsleitung eine Benutzungsberechtigung gemäß § 2 Absatz 1 erhalten, sofern hierdurch die Belange der unter § 1 Abs. 3 a genannten Nutzer nicht beeinträchtigt werden.

(2) Dieser Antrag enthält neben den persönlichen Angaben zum Antragsteller mindestens Angaben zu Beginn und Ende, zu Zweck und Umfang der geplanten Nutzung und benennt einen Beschäftigten der TiHo als Ansprechpartner hierfür.

(3) Wenn zu diesen Punkten Einvernehmen zwischen der IDS und der antragstellenden

Einrichtung besteht, vergibt die IDS eine passende Benutzeridentifikation, welche nach Bestätigung der Kenntnisnahme und Anerkennung der IT-Benutzungsrichtlinie durch den Benutzer mit einem nur ihm bekannten Passwort versehen wird. Diese Nutzer werden im Sinne dieser Richtlinie der Einrichtung zugeordnet, die den Antrag auf Benutzung gestellt hat.

(4) Die Nutzungsberechtigung endet mit dem Ende der begründenden Umstände des Antrages.

(5) Benutzer nach § 1 Abs. 3 d. bis 3 f. erhalten nur Zugriffe auf IT-Dienste, wenn diese unabdingbar für die sich aus der Kooperation mit TiHo ergebenden Aufgaben sind. Diese Benutzer erhalten keine personalisierte Mailadresse und keinen personenbezogenen Speicher-platz (Home - Laufwerk).

§ 4 Regelungen für die kurzfristige Nutzung der IT - Ressourcen ohne personalisierte Kennung durch Tagungsteilnehmer und Gäste

(1) Externe Teilnehmer an Tagungen (und ähnlichen Veranstaltungen) sowie Gäste der Einrichtungen können zeitlich befristete Zugangsmöglichkeiten („Tickets“) zum TiHo-Netz erhalten. Diese Nutzungsberechtigungen sind rechtzeitig vom Tagungsverantwortlichen oder Gastgeber bei der IDS zu beantragen. Es ist die Aufgabe der Tagungsveranstalter oder Gastgeber diese Nutzungsberechtigungen auszuhändigen und die Zuordnung der Kennungen zur Identität der Tagungsteilnehmer und Gäste festzustellen und zu dokumentieren. Für diese Benutzer gelten die Bestimmungen dieser IT-Benutzungsrichtlinie entsprechend, insbesondere § 3 Abs. 1-5.

(2) Die TiHo ist Mitglied in der Föderation „eduroam“ und stellt externen Gästen aus anderen Hochschulen und wissenschaftlichen Einrichtungen, die ebenfalls Mitglieder dieser Föderation sind, ohne weitere Vorbereitungen entsprechende Netzzugänge zur Verfügung. Diese Benutzung ist mit Auflagen verbunden.

§ 5 Regelungen für PCs

(1) Die mit dem TiHo-LAN zu verbindenden PCs (= alle Formen programmierbarer Geräte mit direkter Benutzerbedienung, wie z.B. Desktop-PCs, Workstations, tragbare PCs, Tablets) werden in folgende Gruppen eingeteilt:

a. TiHo-PCs: PCs im Besitz der TiHo zu Erfüllung dienstlicher Aufgaben
   a) TiHo-Standard-PCs:
      PCs für Standardaufgaben
   b) TiHo-Nicht-Standard-PCs: PCs für Spezialaufgaben

b. Fremd-PCs: PCs, die sich nicht im Besitz der TiHo befinden (z.B. PCs im Privatbesitz von Studierenden oder Gästen der TiHo)

(2) Für dienstliche Aufgaben ist der Einsatz von TiHo-PCs zwingend. Die Beschaffung dieser Geräte erfolgt durch die IDS. Die Beschaffung kann auch durch die Einrichtungen der TiHo erfolgen, wenn die zentrale Beschaffung nach Einschätzung der IDS nicht möglich oder nicht sinnvoll ist und wenn die Ausstattung der zu beschaffenden Geräte hinsichtlich Hardware und Software, der Konfiguration und der Beschaffungsverfahren schriftlich zwischen IDS und beschaffender Einrichtung detailliert abgestimmt wurde.

(3) TiHo-Standard-PCs sind PCs mit einer zwischen der Einrichtung (hinsichtlich der Anforderungen der Anwender) und der IDS (hinsichtlich der Administration der PCs vorgesehenen administrativen Prozesse und Sicherheitsaspekte) abgestimmten Hardwareausstattung, Softwareinstallation und -konfiguration für Standardaufgaben. Hierdurch werden zentrales Management und Einhaltung von Sicherheitsstandards gewährleistet. Diese PCs besitzen eine durch Lieferung oder durch Zusatzverträge abgedeckte Lizenz für das Betriebssystem sowie für die in der Standardkonfiguration enthaltenen Softwareanwendungen inklusive eines Virenschutzes, der sich automatisch über einen zentralen Serverdienst aktualisiert. Eine einheitliche IT-Struktur ist für einen sicheren Betrieb innerhalb der TiHo eine unerlässliche Voraussetzung.

(4) Im Kaufpreis der TiHo-Standard-PCs ist eine Garantie für fünf Jahre ab Lieferung enthalten. Während der gesamten Garantiedauer der PCs erfolgt - im Falle eines festgestellten Hardwarefehlers - der Service durch einen Techniker des Herstellers in der nutzenden Einrichtung vor Ort oder in den Räumen der IDS – in der Regel innerhalb des nächsten Arbeitstages nach Meldung des Defektes beim Hersteller. Evtl. sind vor Ort organisatorische Regelungen zu treffen, um dem beauftragten Techniker Zugang zu dem Gerät in einer hierfür geeigneten Umgebung zu verschaffen. Softwarefehler (z.B. Konfigurationsfehler, Bugs,
Bedienungsprobleme, Netzfehler etc.) fallen nicht unter diese Regelung. Ansprechpartner bei Störungen ist daher jeweils zunächst der zuständige dezentrale DV-Beauftragte oder die IDS, um festzustellen, ob es sich um einen Softwarefehler oder einen Hardwarefehler handelt.

(5) TiHo-Nicht-Standard-PCs werden nur beschafft, wenn der Einsatz von TiHo-Standard-PCs technisch nach Einschätzung der IDS nicht möglich oder nicht sinnvoll ist, um die dienstlich geforderten Funktionalitäten zu erfüllen. Auch die TiHo-Nicht-Standard-PCs werden mit einer zwischen der Einrichtung (hinsichtlich der Anforderungen der Anwender) und der IDS (hinsichtlich der Administration der PCs vorgesehenen administrativen Prozesse und
Sicherheitsaspekte) abgestimmten „individuellen“ Hardwareausstattung, Softwareinstallation und -konfiguration beschafft und betrieben, um die Funktionsfähigkeit, Betriebssicherheit, die Netz-Compliance und die Lizenz-Compliance sicherzustellen. Relevante Beispiele für TiHo-Nicht-Standard-PCs sind Workstations zur Bearbeitung von Bild- und Videodaten oder PC-ähnliche Geräte zur Steuerung von Laborgeräten oder medizinischen Geräten der Bildgebung oder Steuerungsgeräte in der Gebäudeleittechnik.

(6) Die Integration in das Netzwerk der TiHo sowie die Nutzung der zentral angebotenen Netzdienste (z.B. Datei-Server, Druck- und Mailserver, Softwareverteilung, Updateservice etc.) durch TiHo-Nicht-Standard-PCs kann nur erfolgen, wenn dieser mit vertretbarem Aufwand, mit den an der TiHo vorhandenen zentralen Methoden, realisiert werden kann.

(7) Für Fremd-PCs werden keine Zugriffe auf zentrale IT-Ressourcen der TiHo (z.B. Speicherdienste, Zugriffe auf Easyvet oder Labcontrol) zur Verfügung gestellt. Es erfolgt auch kein Support.

§ 6 Regelungen für Drucker, Scanner, Kopierer und Fax-Geräte

Drucker, Scanner, Kopierer, Fax-Geräte sowie Multifunktionsgeräte zum Anschluss an PCs oder zum Anschluss über das TiHo–Netzwerk werden von der IDS in der Regel aus Rahmenverträgen beschafft und in Betrieb genommen. Für andere Geräte stellt die IDS keine Serviceleistungen zur Verfügung.

§ 7 Regelungen für weitere netzwerkfähige Geräte

Weitere netzwerkfähige Geräte z.B.

a. medizinische Geräte für Forschung, Lehre und Patientenbehandlung, wie Röntgengeräte, CT, MRT, Ultraschall, Labordiagnostik;
b. Geräte der Gebäudeleittechnik, wie Geräte für Zugangskontrolle, Klimatechnik, Gebäudeüberwachung;
c. sowie weitere von den TiHo-Einrichtungen beschaffte und/oder betriebene Geräte zur Erfüllung ihrer Dienstaufgaben können auf Antrag des Leiters der betreibenden Einrichtung in das TiHo-Netz integriert werden, wenn die hinsichtlich der Netzwerk- und Sicherheitstechnik relevanten technischen und organisatorischen Fragen zur Betriebsführung einvernehmlich zwischen der betreibenden oder verursachenden Einrichtung und der IDS als Betreiber des TiHo-Netz geregelt wurden. Diese Regelungen sollten mit einem angemessenen Vorlauf während des Beschaffungsprozesses getroffen werden, um eine Verzögerung der Inbetriebnahme zu vermeiden.

§ 8 Regelungen für den Betrieb des TiHo-Netzwerks

Für den Anschluss von Geräten an das EDV- und Telekommunikationsnetz der TiHo

(TiHo-Netzwerk) gelten folgende Bestimmungen:

(1) Die zentrale IT-Infrastruktur der TiHo (Server- und Speichersysteme mit allen darauf bereitgestellten Diensten, aktiven und passiven Netzkomponenten (LAN und WLAN)) werden ausschließlich von den Mitarbeitern der IDS, gegebenenfalls nach Absprache der Anforderungen mit den betroffenen Einrichtungen, beschafft und betrieben, um die Gesamtfunktionalität des TiHo-Netzes sicherzustellen.

(2) Die Installation bzw. Erweiterung des TiHo-Netzwerks und aller damit verbundenen aktiven und passiven Komponenten und Netzdiensten erfolgt nur von der IDS oder dazu autorisierten Fachfirmen unter Aufsicht der IDS und/oder des Dezernats für Liegenschaften und Technik.

(3) Der Anschluss von Geräten an das TiHo-Netzwerk, der Rechnerbetrieb sowie die Aufstellung/Installation neuer Rechner erfolgen nach den technischen und organisatorischen Regelungen der IDS. Diese Regelungen werden den Nutzern in geeigneter Form mitgeteilt. Die Bedienungsvorschriften für die einzelnen Geräte sind einzuhalten. Bei Betriebsstörungen, Beschädigungen und Fehlern an DV-Einrichtungen und Datenträgern ist die IDS zu verständigen.

(4) Netzwerkfähige Geräte, deren Funktionalität entweder von einer Verbindung zum TiHo-Netz oder zu analogen Telefonverbindungen abhängt sowie dienstliche Mobilfunkgeräte, werden ausschließlich von der IDS beschafft (oder geleast) und administriert.

(5) Die Qualität des Zugangs zum TiHo-LAN wird in Internet und Intranet unterschieden:

a) Internet Zugang ermöglicht das Aufrufen von Webseiten innerhalb der TiHo und deren Zugang zum Internet (im Normalfall über Proxyserver der IDS über die Standard Ports für die Protokolle http für https);
b) Intranet Zugang ermöglicht darüber hinaus Zugang zu weiteren Ressourcen der TiHo, insbesondere zu Netzlaufwerken (z.B. G, H und T), anderen gemeinsam in der Einrichtung oder TiHo-weit genutzte Laufwerken, Dienste der medizinischen Krankenversorgung (Labcontrol, EasyVet), E-Mailclient, Netzwerkdrucker sowie weitere zentral bereit gestellte IT-Dienste.

(6) Intranet Zugang haben nur die TiHo-PCs nach § 5, die Drucker und ähnlichen Geräte nach § 6 sowie die sonstigen Geräte nach § 7, wenn dieses für die erforderliche Funktionalität notwendig erscheint. Für diese letzte Gruppe muss die betreibende Einrichtung die inhaltlichen Anforderungen an die Netzanbindung so detailliert formulieren, dass die entsprechenden technischen und organisatorischen Details von der IDS so geplant, durchgeführt und überwacht werden können, dass die Funktionssicherheit des TiHo-LANs einerseits und die Funktionalität des netzwerknutzenden Gerätes anderseits gesichert werden kann. Wenn es zwischen diesen beiden Zielen einen auch mit großem Aufwand oder mit externer Unterstützung unauflösbaren Zielkonflikt gibt, ist die Betriebssicherheit des TiHo-LANs höher zu bewerten.

§ 9 Folgen bei Verstößen

Bei strafrechtlich relevanten Tatbeständen oder einem Verstoß gegen diese Richtlinie kann der Benutzer von der Leitung der IDS vorübergehend oder dauerhaft in der Benutzung beschränkt oder auf Vorschlag der Leitung der IDS durch das Präsidium hiervon dauerhaft ausgeschlossen werden. Diese Maßnahmen sollen erst nach vorheriger erfolgloser Abmahnung erfolgen. Dem Betroffenen ist Gelegenheit zur Stellungnahme zu geben. Die vorübergehende Nutzungsbeschränkung wird aufgehoben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet erscheint. Eine dauerhafte Nutzungsbeschränkung oder der dauerhafte Ausschluss eines Benutzers kommt nur bei schwerwiegenden oder wiederholten Verstößen gegen die IT-Benutzungsrichtlinie in Betracht, wenn auch künftig kein ordnungsgemäßes Verhalten zu erwarten ist. Die Entscheidung über den dauerhaften Ausschluss ergeht durch schriftlichen Bescheid des Präsidiums.

§ 10 Sicherheitsrichtlinien

(1) Die Absicherung des Zuganges zum Internet wird durch eine zentral betriebene Firewall sowie weitere technische und organisatorische Maßnahmen sichergestellt.

(2) Arbeitsplätze müssen wirksam durch Virenschutzprogramme vor Schadsoftware gesichert werden. Das Betriebssystem sowie die Anwendungen erhalten automatisiert sicherheitskritische Updates. Diese Programme dürfen durch Nutzer nicht eigenständig manipuliert oder deaktiviert werden. Gleiches gilt für alle Sicherheitsprogramme und -einstellungen.

(3) Zur Gefahrenabwehr werden E-Mails auf unerwünschte Inhalte (Spam, Malware) gescannt und E-Mails mit unerwünschtem Inhalt oder solche von denen Gefahren für das TiHo-Netz ausgehen, werden nicht zugestellt. Das grundsätzlich gegebene Risiko einer „falsch positiven“ Spam oder Malware-Klassifikation einer Mail ist allen Beteiligten bewusst.

(4) Aus Wirtschaftlichkeits- und IT-Sicherheitsgründen wird die Internetnutzung beschränkt: Bestimmte Typen von Webseiten (potentiell schädliche Seiten mit hohem Malware-Risiko oder Seiten mit unerwünschtem Inhalt (Spam, Malware, Pornographie, Hacker-Tools, gewaltverherrlichender Inhalt) werden gesperrt. Im Falle eines Zugriffsversuchs erfolgt ein Blockadehinweis sowie die Option, die Seite als „dienstlich benötigt und fehlklassifiziert“ der IDS mit der Bitte um Freischaltung zu melden. Auf die Inhalte der hierzu abgeschlossenen Vereinbarung zur Filterung unerwünschter Inhalte beim Browsen im Internet an der Stiftung Tierärztliche Hochschule Hannover mit dem Personalrat wird verwiesen.

(5) Bei der Benutzung von Software, Dokumentationen und anderen Daten sind die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten von der IDS zur Verfügung gestellt werden, zu beachten. Von der IDS bereitgestellte Software, Dokumentationen und Daten dürfen weder kopiert noch an Dritte weitergegeben werden. Eine Ausnahme hiervon bildet das Kopieren von selbsterstellten Dateien.

(6) Die Installation und Konfiguration von Anwendungsprogrammen sowie die Sicherstellung der Lizenzbestimmungen erfolgt durch die IDS. DV-Beauftragte der Einrichtungen können an diesen Aufgaben beteiligt werden, wenn sichergestellt ist, dass dieses nicht den konzeptionellen Vorgaben der IDS widerspricht und die Lizenz-Vorgaben sicher gewahrt bleibt. Die IDS regelt die Details des Verfahrens.

(7) Urheberrechtlich geschützte Softwareprogramme, für die keine Lizenz vorhanden ist, dürfen nicht auf den Rechenanlagen der TiHo gespeichert und ausgeführt werden.

(8) Software, die zum Betrieb auf den Rechenanlagen der TiHo beschafft wurde, darf nicht auf Rechnern, die sich nicht im Besitz der TiHo befinden, genutzt werden, es sei denn, dass die Lizenzvereinbarungen mit dem Hersteller dieses explizit regeln.

(9) Software, die nicht von der IDS bereitgestellt oder beschafft oder in Absprache mit ihr beschafft wurde, darf nicht auf Rechnern im Besitz der TiHo installiert oder genutzt werden.

§ 11 Rechte der TiHo

(1) Die TiHo speichert Daten (insbesondere die Benutzerkennungen, Mailkennungen, die Namen des Benutzers, Matrikelnummern, Personalnummern, TiHo-Telefonnummern sowie organisatorische Daten) in geeigneter Weise, um den Zugang der Benutzer zum Netzwerk zu steuern. Die Regelungen bezüglich des Datenschutzes werden in ihrer jeweils gültigen Form hierbei beachtet.

(2) Die TiHo ist berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme durch die Gesamtheit der Nutzer zu dokumentieren und auszuwerten soweit dies erforderlich ist

a. zur Gewährleistung eines ordnungsgemäßen Systembetriebs;

b. zur Ressourcenplanung und Systemadministration;
c. zum Schutz der personenbezogenen Daten anderer Nutzer;
d. für das Erkennen und Beseitigen von Störungen sowie;
e. zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung. Eine Leistungskontrolle findet nicht statt.

(3) Die TiHo kann zum Erhalt der Funktionalität und der Ressourcen des TiHo-LANs automatisierte Programme zur Prüfung des Netzverkehrs einsetzen und die Integrität des Systems störende Ereignisse unterbinden.

(4) Die an das TiHo-Netz angeschlossenen Rechner werden ferngewartet und inventarisiert. Auf die Inhalte der hierzu abgeschlossenen Dienstvereinbarung wird verwiesen.

§ 12 Haftung des Nutzers

(1) Der Nutzer haftet für alle Schäden, die der TiHo durch missbräuchliche oder rechtswidrige Verwendung der Rechenanlagen sowie deren Nutzungsberechtigung entstehen. Er haftet auch für Schäden, die durch schuldhafte Nichteinhaltung seiner Pflichten aus dieser IT-Benutzungsrichtlinie verursacht werden.

Für Nutzer, die sich in einem Beamten- oder Beschäftigungsverhältnis zur TiHo befinden, gelten die von der arbeitsgerichtlichen Rechtsprechung entwickelten Grundsätze und die tariflichen Regelungen zur Haftung gegenüber dem Dienstherrn bzw. Arbeitgeber.

(2) Der Nutzer haftet auch für Schäden, die im Rahmen seiner ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe seiner Benutzerkennung und des dazugehörigen Passwortes an Dritte.

(3) Der Nutzer hat die TiHo von allen Ansprüchen freizustellen, wenn Dritte die TiHo wegen eines missbräuchlichen oder rechtswidrigen Verhaltens der Benutzer auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen.

§ 13 Haftung der TiHo

(1) Aus der Benutzung entstehen keinerlei Ansprüche gegenüber der TiHo. Die TiHo übernimmt keine Garantie dafür, dass alle Dienste fehlerfrei und jederzeit ohne Unterbrechung zur Verfügung stehen. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.

(2) Im Übrigen haftet die TiHo nur bei Vorsatz oder grober Fahrlässigkeit ihrer Mitarbeiter. Die Haftung ist auf Ersatzleistungen für unmittelbare Schäden beschränkt.

(3) Mögliche Amtshaftungsansprüche gegen die TiHo bleiben von den vorstehenden Regelungen unberührt.

§ 14 In-Kraft-Treten

Diese Richtlinie tritt am Tag nach der Bekanntmachung im Verkündungsblatt der Hochschule in Kraft. Sie ersetzt die IT-Richtlinie in der Fassung vom 31.05.2017.

Hannover, 12. September 2017
I.V.

Joachim Mertes
Hauptberuflicher Vizepräsident