Stiftung Tierärztliche Hochschule Hannover

Verkündungsblatt

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

Hannover, 24. Februar 2015 Nr. 209/2015

Dienstvereinbarung über die Ziele und Grundsätze bei der Durchführung von Fernsteuerung und Fernwartung an der Stiftung Tierärztliche Hochschule Hannover

Zwischen der Stiftung Tierärztliche Hochschule Hannover (TiHo) und dem Personalrat der Stiftung Tierärztliche Hochschule Hannover (PR) wird gemäß § 78 NPersVG folgende Vereinbarung geschlossen:

Präambel

(1) Die Verhandlungspartner stimmen darin überein, dass an der Stiftung Tierärztliche Hochschule Hannover dem IT-Service-Personal durch die Methodik der Fernwartung ein Arbeitsmittel zur Verfügung gestellt werden soll, um eine effiziente PC-Betreuung leisten zu können.

(2) Die Verhandlungspartner stimmen ferner darin überein, dass an der Stiftung Tierärztliche Hochschule Hannover zum Schutz der Beschäftigten vor einem unbefugten ebenso wie vor einem unkontrollierten Zugriff auf Benutzer-PCs sowie einer Verhaltens- und Leistungskontrolle und eines Leistungsvergleichs Schutzmaßnahmen getroffen werden müssen. Dazu werden die folgenden Grundsätze zur Durchführung vereinbart.

§ 1 Geltungsbereich

(1) Diese Dienstvereinbarung gilt für die Durchführung von Fernwartung und Fernsteuerung auf allen dienstlich beschafften Benutzer-PCs an der Stiftung Tierärztliche Hochschule Hannover.

(2) Sie gilt für Beschäftigte der Stiftung Tierärztliche Hochschule Hannover im Sinne des § 4 NPersVG. Die Dienststelle verpflichtet sich, die Regelungen dieser Dienstvereinbarung auch auf die Beschäftigten anzuwenden, die nicht vom Personalrat vertreten werden.

§ 2 Allgemeines

(1) Es werden die Grundsätze für die Durchführung von Fernwartung von Benutzer-PCs und zur Fernsteuerung von ferngesteuerten PCs festgelegt.

(2) In dieser Vereinbarung versteht man unter Benutzer-PC einen Desktop-PC oder ein Laptop, im Eigentum der Stiftung TiHo Hannover, der in der Regel von einem bestimmten Beschäftigten verwendet wird.

(3) Unter Fernwartung versteht man Maßnahmen, die durchgeführt werden, wenn ein PC-Nutzer um Serviceleistungen nachfragt, um entweder die Ursache einer Störung oder eines Problems zu erkennen und/oder diese zu beseitigen und die einen Fernzugriff auf den Benutzer-PC beinhalten.

(4) Unter Fernsteuerung versteht man Maßnahmen, um ohne User-Interaktion durch Fernzugriff einen lesenden oder schreibenden Zugriff auf PCs die nicht einem konkreten Beschäftigten zugeordnet werden können, z. B. im Hörsaal und in Kursräumen zu erhalten. Diese PCs werden deutlich als „Ferngesteuerte PCs“ gekennzeichnet.

§ 3 Beschreibung

(1) Programme zur Fernwartung auf Benutzer-PCs sind ein Hilfsmittel für die Administration von Computernetzwerken. Sie ermöglichen die Wartung und Steuerung der TiHo-Rechner von einem anderen Arbeitsplatz aus.
(2) Entsprechend den Funktionen der Software ist sowohl ein steuernder Eingriff als auch nur ein Lesezugriff möglich. Die Programme werden zur Fehlersuche und Fehlerbeseitigung eingesetzt. So kann das IT Service-Personal

- den Bildschirm eines PC-Users sehen,
- Software auf dem Rechner installieren, deinstallieren oder konfigurieren,
- Konfigurationen von Dateien vornehmen,
- steuernd in den Anwendungsdialog eingreifen,
- den gesteuerten Rechner, bei Bedarf neu starten.

§ 4 Eingesetzte Programme

(Anlage 1: Produktbeschreibung)

(1) Dem Personalrat und dem Datenschutzbeauftragten werden alle Informationen über die eingesetzten bzw. einzusetzenden Programme zur Verfügung gestellt. Den Leitungen der Hochschuleinrichtungen werden diese Unterlagen auf Wunsch auch zur Verfügung gestellt. § 22 Abs. 4 NDSG bleibt unberührt.
(2) Für Änderungen der an der TiHo genutzten Softwarefunktionalitäten für die Fernwartung bzw. Fernsteuerung ist die Zustimmung des Datenschutzbeauftragten und des Personalrats einzuholen.
(3) Die Vertragspartner gehen aufgrund einer Prüfung des Datenschutzbeauftragten davon aus, dass die aufgrund der vorliegenden Dienstvereinbarung zur Fernwartung eingesetzten Programme weder eine datenschutzrechtliche Vorabkontrolle noch eine Verfahrensbeschreibung nach § 8 NDSG erforderlich machen. (Anlage 5)

§ 5 Datensicherheit

(1) Zum Schutz vor unbefugten Fernwartungszugriffen sind die Rechte für den Fernwartungszugriff auf den notwendigen Kreis an IT-Service-Personal zu beschränken. (Anlage 2: Berechtigungskonzept)
(2) Das IT-Service-Personal besteht aus den Mitarbeitern der TiHo-IDS. Auf Antrag des Leiters einer Einrichtung an die IDS kann auch dezentralen Beschäftigten in einer Einrichtung, die in erheblichem Umfang IT-Service-Aufgaben übernehmen, Zugriff auf Fernwartungssoftware gewährt werden, wenn die Einrichtung die dafür notwendigen Softwarelizenzen beschafft.
(3) Der Zugriff darf nur in dem Umfang getätigt werden, der zur Analyse und Behebung des Problems bzw. Fehlers nötig ist.
(4) Zum Schutz der Integrität (Garantie der Unverfälschtheit) der Daten ist durch die Umsetzung geeigneter technischer und/oder organisatorischer Maßnahmen (z. B. Wahrung der IT-Berechtigungen der Anwender) sicherzustellen, dass das Risiko eines Fehler verursachenden Eingriffs minimiert wird.
(5) Alle an der Fernwartung teilnehmenden Beschäftigten haben sich vor dem Fernzugriff angemessen gegenüber dem PC-User zu identifizieren.

§ 6 Fernzugriffe durch Externe

(1) Zugriffe auf Benutzer PCs durch externe Firmen sind nicht gestattet.

§ 7 Datenschutz

(1) Die Dienststelle gewährleistet die organisatorischen und technischen Maßnahmen, die die im Landesdatenschutzgesetz geforderten Ziele sicherstellen.

§ 8 Unterrichtung der User

(1) Die Beschäftigten sind vor der Einführung und während der weiteren Nutzung von Fernsteuerungs- und Fernwartungssystemen von der Dienststelle rechtzeitig und umfassend zu informieren.
(2) Der Fernwartungszugriff ist nur mit der vorherigen Zustimmung der User zulässig; diese erfolgt in der Regel durch eine telefonische Kontaktaufnahme.
(3) Die Fernwartung wird durch eine Meldung oder ein Symbol während der Dauer der Sitzung auf dem Bildschirm des ferngesteuerten Rechners angezeigt.
(4) Der User muss darauf hingewiesen werden, wie die Fernwartungssitzung jederzeit beendet werden kann. Die Übernahme und Übergabe der Steuerung muss im Dialogfeld bestätigt werden.
(5) Der User des ferngewarteten PCs kann auf dem Bildschirm die sichtbaren Aktivitäten des IT-Service-Personals nachvollziehen. Er kann auf dieses Recht z. B. aus zeitlichen Gründen verzichten.
(6) Automatische Softwareverteilung sowie Updates der System- und Anwendungssoftware sind auch ohne vorherige Information der User zulässig.

§ 9 Verantwortlichkeit

(1) Das IT-Service-Personal und deren Führungskräfte sind für den gewissenhaften Umgang mit den eingesetzten Programmen verantwortlich. Insbesondere dürfen sie programmtechnisch eventuell vorhandene Möglichkeiten einer Verhaltens- und Leistungskontrolle und eines Leistungsvergleichs nicht nutzen bzw. deren Nutzung nicht anordnen oder zulassen.
(2) Das IT-Service-Personal und, soweit erforderlich, deren Führungskräfte, sind im Umgang mit der Software zu unterweisen und über die Bedingungen und Risiken der Nutzung sowie über den Inhalt dieser Vereinbarung aufzuklären. Sie sind auf die strafrechtlichen Konsequenzen bei Verstößen gegen die Verschwiegenheitspflicht hinzuweisen.
(3) Sie haben die Teilnahme an der Unterweisung und die Kenntnis der Bedingungen und Risiken der Nutzung sowie die Kenntnis dieser Vereinbarung schriftlich zu bestätigen
(Anlage 3: Unterweisung).

§ 10 Erstellung und Aufbewahrung von Protokollen und Protokolldateien

(Anlage 4: Liste der Protokolldaten)

(1) Beim Einsatz der Fernwartungssoftware werden zentrale, automatisierte Protokolldateien erstellt, die festhalten, wann welcher User auf welchem Rechner mit dem IT-Service-Personal zuletzt eine Fernwartungssitzung durchgeführt hat.
(2) Zugriffe externer Firmen auf Protokolldaten sind nicht zulässig, mit Ausnahme des Softwarelieferanten der Software in § 4, wenn dieser zu Wartungszwecken oder zur Störungsbeseitigung auf diese zugreifen muss.
(3) Daneben werden dezentrale Protokolldateien auf den ferngewarteten PCs erzeugt. Diese werden mit angemessenen Verfahren, wenn sie zur rechtmäßigen Erfüllung, der Aufgaben nicht mehr erforderlich sind, spätestens nach 7 Tagen automatisiert gelöscht.

§ 11 Schutz der Beschäftigten

(1) Diese Vereinbarung dient dem Schutz der Beschäftigten insbesondere vor
   a. einem unbefugten ebenso wie vor einem unkontrollierten Zugriff auf Benutzer- PCs einschließlich der Daten und Programme,
   b. einer Verhaltens- und Leistungskontrolle und eines Leistungsvergleichs,
   c. einer Nutzung von Daten für personalrechtliche Vorgänge.

(2) Sie dient außerdem der Gewährleistung der Informationssicherheit (Datensicherheit).

§ 12 Schlussbestimmungen

(1) Diese Dienstvereinbarung tritt am Tag nach ihrer öffentlichen Bekanntmachung im Verkündungsblatt der Hochschule in Kraft und löst die bisherige Dienstvereinbarung vom Mai 2005 ab. Die Dienstvereinbarung kann von jeder Seite mit sechsmonatiger Frist gekündigt werden. In diesem Fall wirkt sie bis zum Abschluss einer neuen Dienstvereinbarung nach.

(2) Sollten einzelne Punkte der Dienstvereinbarung unwirksam sein oder ihre Gültigkeit aufgrund neuer Gesetzgebung oder Rechtsprechung verlieren, so bleiben die übrigen Teile hiervon unberührt und weiterhin in Kraft.

(3) Alle Anlagen sind Bestandteil dieser Dienstvereinbarung. Bei Änderung einer Anlage muss diese dem Personalrat zur Kenntnis vorgelegt werden.

Anlage 1	Produktbeschreibung
Anlage 2	Berechtigungskonzept nach § 5 der DV
Anlage 3	Unterweisung
Anlage 4	Liste der Protokolldaten mit Angaben über die Bezeichnung der Protokolldaten und den Speicherort
Anlage 5	Stellungnahme des Datenschutzbeauftragten

Hannover, 05. August 2014
Für den Personalrat
gez. Birgitt Mendig

Hannover, 05. August 2014
Für die Dienststelle
gez. Dr. Dr. h. c. mult. Gerhard Greif

Hannover, 24. Februar 2015

Dr. Dr. h. c. mult. Gerhard Greif
Präsident