

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

Zwischen
der Stiftung Tierärztliche Hochschule (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 einen 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 Serviceleistungen anfordert, 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, die durchgeführt werden, um ohne Benutzer-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.

¹ Aus Gründen der besseren Lesbarkeit wird für Amtsbezeichnungen und Personen nur die männliche Sprachform verwendet. Sie soll jeweils die weibliche Sprachform mit umfassen.

§ 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-Benutzers 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

(siehe 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.

§ 5 Datensicherheit

- (1) Zum Schutz vor unbefugten Fernwartungszugriffen sind die Rechte für den Fernwartungszugriff auf den notwendigen Kreis an IT-Service-Personal zu beschränken.
- (2) Das IT-Service-Personal besteht aus den Mitarbeitern der TiHo-IDS.
- (3) Auf Antrag des Leiters einer Einrichtung an die TiHo-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. (siehe Anlage 2: Liste der dezentralen Fernwartungsberechtigten)
- (4) Der Zugriff darf nur in dem Umfang getätigt werden, der zur Analyse und Behebung des Problems bzw. Fehlers nötig ist.
- (5) 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.
- (6) Alle an der Fernwartung teilnehmenden Beschäftigten haben sich vor dem Fernzugriff angemessen gegenüber dem PC-Benutzer zu identifizieren.

§ 6 Fernzugriffe durch Externe

Zugriffe auf Benutzer-PCs durch externe Firmen sind nicht gestattet.

§ 7 Unterrichtung der Benutzer

- (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 Benutzer 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 Benutzer muss darauf hingewiesen werden, wie die Fernwartungssitzung jederzeit beendet werden kann. Die Übernahme und Übergabe der Steuerung muss im Dialogfeld bestätigt werden.
- (5) Der Benutzer des ferngewarteten PCs kann auf dem Bildschirm die sichtbaren Aktivitäten des IT-Service-Personals nachvollziehen.
- (6) Automatische Softwareverteilung sowie Updates der System- und Anwendungssoftware sind auch ohne vorherige Information der Benutzer zulässig.

§ 8 Verantwortlichkeit

- (1) Das IT-Service-Personal und deren Vorgesetzte 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 Vorgesetzte, ist 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) Die Teilnahme an der Unterweisung und die Kenntnis der Bedingungen und Risiken der Nutzung sowie die Kenntnis dieser Vereinbarung sind schriftlich zu bestätigen (Anlage 3 - Unterweisung).

§ 9 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 Benutzer 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 und automatisiert gelöscht.

§ 10 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).

§ 11 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 Liste der dezentralen Fernwartungsberechtigten nach §5 der DV
- Anlage 3 Unterweisung
- Anlage 4 Liste der Protokolldaten mit Angaben über die Bezeichnung der Protokolldaten und den Speicherort


Dienststelle

05.08.2014 B. L. May
Personalrat

Anlage 1

zur Dienstvereinbarung über die Ziele und Grundsätze bei der Durchführung von Fernsteuerung und Fernwartung an der Stiftung TiHo Hannover

Produktbeschreibung Fastviewer

FastViewer ist eine Anwendung für Fernwartung, Schulung und Präsentation welche über folgende Funktionen verfügt:

1. An der Stiftung Tierärztliche Hochschule Hannover eingesetzt

Remote-Kontrolle:

Ermöglicht den Zugriff auf den Desktop des fernzusteuern den Rechners. Übernahme von Tastatur und Maus (Remote-Session).

Dateitransfer:

Über diese Funktion kann der IT-Admin auf das Dateisystem des Anwenders zugreifen und Dateien transferieren.

Der Dateitransfer ermöglicht ein einfaches Austauschen von Dateien. So können beispielsweise Anwendungsdaten, Installationen oder Verzeichnisse zwischen IT-Admin und Anwender übertragen werden.

Systeminformationen (SysInfo) / Remote-Taskmanager:

Die SysInfo enthält wichtige Informationen zu dem Systemzustand des PCs des Anwenders wie z.B. eine Übersicht über alle Systemkomponenten oder den zur Verfügung stehenden Speicherplatz. Zusätzlich ist ein Remote- Taskmanager integriert, welcher es ermöglicht die aktuellen Prozesse anzuzeigen oder gezielt zu beenden.

Verbindungsperformance-Test:

Mit dieser Funktion können über einen externen Server (Fastviewer-Server) der Datendurchsatz der Internetverbindung getestet und evtl. auftretende Verbindungsprobleme schnell lokalisiert werden.

Remotedesktop ausblenden:

Mit dieser Funktion kann der IT-Admin den Desktop des Anwenders ausschalten. Für den Anwender bleibt der Desktop weiterhin sichtbar.

Neustart:

Führt einen Neustart des Rechners durch, wenn dies für eine Re-Konfiguration nötig ist und verbindet nach erfolgreichem Neustart die Remote-Session wieder.

Bildübertragungsqualität:

Zur Verfügung stehen folgende Einstellungen: „Niedrig, Normal, Hoch, Verlustfrei“.

2. Zusätzliche Funktionen, technisch möglich, aber an der TiHo nicht für Fernwartung genutzt

Sitzungsaufzeichnung:

Ermöglicht die komplette oder teilweise Aufzeichnung der Remote-Session. Die Aufnahme wird in ein nicht veränderbares Format umgewandelt und als exe-Datei abgespeichert. Durch den „FastViewer-Player“ ist die Aufzeichnung vor Fälschung und Manipulation gesichert.

Remotebildschirm sperren:

Mit dieser Funktion wird der Desktop des Anwenders gesperrt und folgender Text angezeigt: „Dieser Computer wird gerade ferngewartet und ist gesperrt“.

Portmapper:

Durch das Portmapping (Zugangsverbindung) ist es möglich über Betriebssystemgrenzen hinweg TCP-Ports direkt mit dem lokalen Zugriff zu verbinden. Für diese Funktion gibt es ein breites Anwendungsspektrum, so ist es beispielsweise möglich auf Netzwerkgeräte generell, Maschinensteuerungen oder auch Linux- Geräte zuzugreifen.

Anlage 3

zur Dienstvereinbarung über Ziele und Grundsätze bei der Durchführung von Fernsteuerung und Fernwartung

Bestätigung durch Frau/Herrn

.....

(Name, Vorname)

Ich bestätige meine Teilnahme an der Unterweisung zu dem Programm

.....

amdurchgeführt von Frau / Herrn.....

Ich wurde dabei über die Funktionalitäten des Programms, die technischen Möglichkeiten und die Einsatzbereiche aufgeklärt. Außerdem wurde mir die „Vereinbarung über die Ziele und Grundsätze bei der Einführung und Nutzung von Fernsteuerungs-, Fernwartungs-, Auswertungssoftware“ in der aktuellen Fassung erläutert und ausgehändigt. Insbesondere wurde ich über die Bedingungen und Risiken der Nutzung der Software aufgeklärt und über das Verbot einer Verhaltens- und Leistungskontrolle und eines Leistungsvergleichs der betroffenen Benutzerinnen und Benutzer sowie über meine Sorgfaltspflicht im Umgang mit dem Programm zum Schutz der Datenintegrität unterrichtet.

.....

(Ort, Datum)

.....

(Unterschrift der oder des Beschäftigten)

Anlage 4

zur Dienstvereinbarung über die Ziele und Grundsätze bei der Durchführung von Fernsteuerung und Fernwartung an der Stiftung TiHo Hannover

Logdateien:

Die Loginformationen über die Fernwartung werden gespeichert in:

Verzeichnis: \Programme\Matrix42\Remote Control Host\sessionlog

Dateiname: sessionlog_JJJJ-T-MM H-MM-SS Zufallszahl.log

.....
(Ort, Datum)

.....
(Unterschrift IDS)



Stiftung Tierärztliche Hochschule Hannover, Physiologisches Institut,
Bischofsholer Damm 15, 30173 Hannover

Physiologisches Institut

Apl. Prof. Dr. Bernd Schröder
Behördlicher Datenschutzbeauftragter
Bischofsholer Damm 15
30173 Hannover

Tel. +49 511 856-7281
Fax +49 511 856-7687
bernd.schroeder@tiho-hannover.de

Personalrat der TiHo

Dr. B. Franz, Leiter IDS

Ihre Nachricht vom | Ihr Zeichen

Meine Nachricht vom | Mein Zeichen

Datum
Hannover, 18.10.2013

Dienstvereinbarung „Fernwartung“ Stellungnahme des Datenschutzbeauftragten

Sachstand

Bei dem datenschutzrechtlich relevanten Verfahren „Fernwartung“ wird zum Zwecke der Abwicklung Vor- und Nachname des den Service der IDS in Anspruch nehmenden Teilnehmers bzw. Teilnehmerin gespeichert (Aussage Dr. Franz, 08.10.13 Email). Gemäß §9 NDSG dürfen personenbezogene Daten erhoben werden, „wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist“. Im Fall der Fernwartung ist die Erforderlichkeit gegeben. Gemäß §4 NDSG ist die Zulässigkeit der Verarbeitung personenbezogener Daten dadurch gegeben, dass die Teilnehmer zu Beginn der Fernwartung auf dem Monitor im Klickverfahren ihre Zustimmung geben und diese während der Sitzung jederzeit zurückziehen können. Rechtsfolgen, die sich an die geplante bzw. tatsächliche Speicherung personenbezogener Daten knüpfen, ist ggf. eine Vorabkontrolle (§7 Abs. 3 NDSG) und ggf. die Erstellung einer Verfahrensbeschreibung (§8 NDSG).

Vorabkontrolle

Zur Prüfung der Zulässigkeit einer automatisierten Verarbeitung sind Verfahren, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien besondere Risiken in sich tragen, vor ihrer Einführung einer Vorabkontrolle (früher: Technikfolgenabschätzung) zu unterziehen, um festzustellen, ob die mit der automatisierten Verarbeitung verbundenen Risiken für die Rechte der Betroffenen durch technische und organisatorische Maßnahmen wirksam beherrscht werden können. Personenbezogene Daten, deren automatisierte Verarbeitung **besondere Risiken** für die Rechte der Betroffenen mit sich bringen, sind solche, deren Missbrauch Existenz, Leben oder Freiheit der Betroffenen gefährden oder sie in ihrer gesellschaftlichen Stellung erheblich beeinträchtigen würden (S. 61 NDSG, Gesetzestext und Kommentar, Stand 12/2012).

Besondere Risiken liegen im Verfahren „Fernwartung“ nicht vor, so dass die Erforderlichkeit zur Durchführung einer Vorabkontrolle nicht gegeben ist.

Seiten insgesamt
1 / 2

Stiftung Tierärztliche Hochschule Hannover
Physiologisches Institut
Bischofsholer Damm 15
30173 Hannover
Steuer-Nr. 25/202/26506
Ust-ID-Nr. DE 233060166

Bankverbindung
Norddeutsche Landesbank Hannover
BLZ 250 500 00
Konto 106 031 347
IBAN DE07 2505 0000 0106 0313 47
SWIFT-BIC: NOLA DE 2H

www.tiho-hannover.de

Verfahrensbeschreibung

§8 NDSG sieht die obligatorische Erstellung einer Verfahrensbeschreibung durch die Daten verarbeitende Stelle vor, die dem behördlichen Datenschutzbeauftragten zwecks Aufnahme in das Verzeichnissverzeichnis zuzuleiten ist. Allerdings bedarf es nicht der Erstellung einer Verfahrensbeschreibung bei personenbezogenen Daten, die ausschließlich zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage (hier TiHo-Netz und Benutzer-PC) gespeichert und genutzt werden (S. 64 NDSG, Gesetzestext und Kommentar, Stand 12/2012).

Im Verfahren „Fernwartung“ ist die Notwendigkeit zur Erstellung einer Verfahrensbeschreibung nicht gegeben.

Hinweis

Bei potenziellen Veränderungen im Verfahren „Fernwartung“ gegenüber dem aktuellen Stand muss vorab von der Daten verarbeitenden Stelle in Zusammenarbeit dem Datenschutzbeauftragten geprüft werden, ob unter den neuen Bedingungen die Erstellung einer Vorabkontrolle und/oder einer Verfahrensbeschreibung gemäß NDSG notwendig wird.

Bernd Schröder

Bernd Schröder
Behördlicher Datenschutzbeauftragter



Stiftung Tierärztliche Hochschule Hannover, Physiologisches Institut,
Bischofsholer Damm 15, 30173 Hannover

Physiologisches Institut

Apl. Prof. Dr. Bernd Schröder
Behördlicher Datenschutzbeauftragter
Bischofsholer Damm 15
30173 Hannover

Personalrat der TIHo

Dr. B. Franz, Leiter IDS

Tel. +49 511 856-7281
Fax +49 511 856-7687
bernd.schroeder@tiho-hannover.de

Ihre Nachricht vom | Ihr Zeichen

Meine Nachricht vom | Mein Zeichen

Datum
Hannover, 18.10.2013

Dienstvereinbarung „Fernwartung“ Stellungnahme des Datenschutzbeauftragten

Sachstand

Bei dem datenschutzrechtlich relevanten Verfahren „Fernwartung“ wird zum Zwecke der Abwicklung Vor- und Nachname des den Service der IDS in Anspruch nehmenden Teilnehmers bzw. Teilnehmerin gespeichert (Aussage Dr. Franz, 08.10.13 Email). Gemäß §9 NDSG dürfen personenbezogene Daten erhoben werden, „wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist“. Im Fall der Fernwartung ist die Erforderlichkeit gegeben. Gemäß §4 NDSG ist die Zulässigkeit der Verarbeitung personenbezogener Daten dadurch gegeben, dass die Teilnehmer zu Beginn der Fernwartung auf dem Monitor im Klickverfahren ihre Zustimmung geben und diese während der Sitzung jederzeit zurückziehen können. Rechtsfolgen, die sich an die geplante bzw. tatsächliche Speicherung personenbezogener Daten knüpfen, ist ggf. eine Vorabkontrolle (§7 Abs. 3 NDSG) und ggf. die Erstellung einer Verfahrensbeschreibung (§8 NDSG).

Vorabkontrolle

Zur Prüfung der Zulässigkeit einer automatisierten Verarbeitung sind Verfahren, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien besondere Risiken in sich tragen, vor ihrer Einführung einer Vorabkontrolle (früher: Technikfolgenabschätzung) zu unterziehen, um festzustellen, ob die mit der automatisierten Verarbeitung verbundenen Risiken für die Rechte der Betroffenen durch technische und organisatorische Maßnahmen wirksam beherrscht werden können. Personenbezogene Daten, deren automatisierte Verarbeitung **besondere Risiken** für die Rechte der Betroffenen mit sich bringen, sind solche, deren Missbrauch Existenz, Leben oder Freiheit der Betroffenen gefährden oder sie in ihrer gesellschaftlichen Stellung erheblich beeinträchtigen würden (S. 61 NDSG, Gesetzestext und Kommentar, Stand 12/2012).

Besondere Risiken liegen im Verfahren „Fernwartung“ nicht vor, so dass die Erforderlichkeit zur Durchführung einer Vorabkontrolle nicht gegeben ist.

Seiten insgesamt
1 / 2

Stiftung Tierärztliche Hochschule Hannover
Physiologisches Institut
Bischofsholer Damm 15
30173 Hannover
Steuer-Nr. 25/202/26506
Ust-ID-Nr. DE 233060166

Bankverbindung
Norddeutsche Landesbank Hannover
BLZ 250 500 00
Konto 106 031 347
IBAN DE07 2505 0000 0106 0313 47
SWIFT-BIC: NOLA DE 2H

www.tiho-hannover.de



Produktbeschreibung Fastviewer

FastViewer ist eine Anwendung für Fernwartung, Schulung und Präsentation welche über folgende Funktionen verfügt:

1. An der Stiftung Tierärztliche Hochschule Hannover eingesetzt

Remote-Kontrolle:

Ermöglicht den Zugriff auf den Desktop des fernzusteuernenden Rechners. Übernahme von Tastatur und Maus (Remote-Session).

Dateitransfer:

Über diese Funktion kann der IT-Admin auf das Dateisystem des Anwenders zugreifen und Dateien transferieren.

Der Dateitransfer ermöglicht ein einfaches Austauschen von Dateien. So können beispielsweise Anwendungsdaten, Installationen oder Verzeichnisse zwischen IT-Admin und Anwender übertragen werden.

Systeminformationen (SysInfo) / Remote-Taskmanager:

Die SysInfo enthält wichtige Informationen zu dem Systemzustand des PCs des Anwenders wie z.B. eine Übersicht über alle Systemkomponenten oder den zur Verfügung stehenden Speicherplatz. Zusätzlich ist ein Remote-Taskmanager integriert, welcher es ermöglicht die aktuellen Prozesse anzuzeigen oder gezielt zu beenden.

Verbindungsperformance-Test:

Mit dieser Funktion können über einen externen Server (Fastviewer-Server) der Datendurchsatz der Internetverbindung getestet und evtl. auftretende Verbindungsprobleme schnell lokalisiert werden.

Remotedesktop ausblenden:

Mit dieser Funktion kann der IT-Admin den Desktop des Anwenders ausschalten.

Für den Anwender bleibt der Desktop weiterhin sichtbar.

Neustart:

Führt einen Neustart des Rechners durch, wenn dies für eine Re-Konfiguration nötig ist und verbindet nach erfolgreichem Neustart die Remote-Session wieder.

Bildübertragungsqualität:

Zur Verfügung stehen folgende Einstellungen: „Niedrig, Normal, Hoch, Verlustfrei“.

2. Zusätzliche Funktionen, technisch möglich, aber an der TiHo nicht genutzt

Sitzungsaufzeichnung:

Ermöglicht die komplette oder teilweise Aufzeichnung der Remote-Session.

Die Aufnahme wird in ein nicht veränderbares Format umgewandelt und als exe-Datei abgespeichert.

Durch den „FastViewer-Player“ ist die Aufzeichnung vor Fälschung und Manipulation gesichert.

Remotebildschirm sperren:

Mit dieser Funktion wird der Desktop des Anwenders gesperrt und folgender Text angezeigt: „Dieser Computer wird gerade ferngewartet und ist gesperrt“.

Portmapper:

Durch das Portmapping (Zugangsverbindung) ist es möglich über Betriebssystemgrenzen hinweg TCP-Ports direkt mit dem lokalen Zugriff zu verbinden. Für diese Funktion gibt es ein breites Anwendungsspektrum, so ist es beispielsweise möglich auf Netzwerkgeräte generell, Maschinensteuerungen oder auch Linux- Geräte zuzugreifen.