

**Dienstvereinbarung
über die Einführung und Nutzung
der Fernwartungssoftware TeamViewer
zwischen der Universität Oldenburg
(Dienststelle) und dem
Personalrat der Universität Oldenburg**

vom 16.12.2011

**§ 1
Grundsätze**

(1) Diese Dienstvereinbarung regelt die Einführung und den Einsatz der Fernwartungssoftware TeamViewer, die den kontrollierten Zugriff auf Benutzer-PC ermöglicht.

(2) Diese Vereinbarung dient dem Schutz der Beschäftigten insbesondere vor

- einem unbefugten wie vor einem unkontrollierten Zugriff auf den Arbeitsplatz-PC,
- einer Verhaltens- und Leistungskontrolle und
- einer Nutzung von Daten für personalrechtliche Vorgänge (ausgenommen im Zusammenhang mit nachgewiesenen Dienstpflichtverletzungen).

Sie dient außerdem der Gewährleistung der Informationssicherheit (Datensicherheit).

**§ 2
Beschreibung des eingesetzten Programms**

(1) Zur Fernbetreuung von PC-Problemen (z. B. in den Bereichen Betriebssystem, Anwendung, Konfiguration) wird TeamViewer eingeführt.

(2) Durch die Einführung der neuen Software sollen den MitarbeiterInnen in den IT-Diensten, die PC-Nutzerinnen und Nutzern betreuen, ein Arbeitsmittel zur Verfügung gestellt werden, um bei Bedarf PC-Betreuung mittels Fernwartung leisten zu können. So kann die Anwenderin oder der Anwender dieser Software z. B.

- eine Übersicht über die Hardwarekomponenten und der aktiven Software erhalten,
- den Bildschirm angezeigt bekommen,
- Software auf dem Rechner installieren oder deinstallieren,
- Eingriffe in Dateien vornehmen,
- steuernd in den Dialog eingreifen,

- den gesteuerten Rechner neu starten,
- die Bedienung übernehmen.

(3) Bei wesentlichen funktionalen Änderungen der eingesetzten Software sowie beim Einsatz neuer Software sind die oder der Datenschutzbeauftragte, die oder der IT-Sicherheitsbeauftragte und der Personalrat zu beteiligen.

**§ 3
Datensicherheit**

(1) Zum Schutz vor unbefugten Fernzugriffen sind die Rechte für den Fernzugriff auf den notwendigen Kreis an Beschäftigten im First- und Second-Level-Support beschränkt. Der First-Level-Support wird von der Funktion Service Desk, der Second-Level-Support von der Funktion IT-Support (DS, CS und DCI) ausgeführt. Der Zugriff darf nur in dem Umfang getätigt werden, der zur Analyse und Behebung des Problems bzw. Fehlers nötig ist. Die im First- und Second-Level-Support eingesetzten Beschäftigten haben sich vor dem Fernzugriff angemessen zu authentisieren.

(2) Der Schutz der Integrität (Garantie der Unverfälschtheit) der Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, so dass das Risiko eines Fehler verursachenden Eingriffs minimiert wird.

**§ 4
Datenschutz**

Für Zwecke der Fehleranalyse und -behebung dürfen personenbezogene Daten oder Dateien mit personenbezogenen Daten nur mit vorheriger Zustimmung der Benutzerin oder des Benutzers kopiert oder übertragen werden. Im Übrigen ist der Zugriff auf und das Herunterladen von Dateien untersagt.

**§ 5
Unterrichtung der Benutzerinnen und Benutzer**

(1) Der Fernzugriff ist nur mit der vorherigen Zustimmung der Benutzerin oder des Benutzers zulässig. Die Benutzerin oder der Benutzer erteilt seine Zustimmung, indem sie oder er den Betreuenden telefonisch das für die Session generierte 4-stellige Kennwort mitteilt. Der Fernwartungszugriff wird auf dem Bildschirm der Benutzerin bzw. des Benutzers angezeigt. Daten, die nach vorheriger Genehmigung der Nutzerin oder des Nutzer zu Analysezwecken und Fehlerbehebung durch die Betreuenden übertragen wurden, sind nach Beendigung des Remote-Zugriffs sofort zu löschen.

(2) Automatische Updates der System- und Anwendungssoftware sind ohne Zustimmung zulässig.

Eine Information der Benutzerin oder des Benutzers hat zu erfolgen.

§ 6 Verantwortlichkeit

(1) Die für den First- und Second-Level-Support eingesetzten Beschäftigten und deren Führungskräfte sind für den gewissenhaften Umgang mit der eingesetzten Fernwartungssoftware TeamViewer verantwortlich. Insbesondere dürfen sie programmtechnisch vorhandene Möglichkeiten einer Verhaltens- und Leistungskontrolle nicht nutzen bzw. deren Nutzung nicht anordnen oder zulassen.

(2) Die für den First- und Second-Level-Support eingesetzten Beschäftigten und, soweit erforderlich, deren Führungskräfte sind auf Kosten der Dienststelle 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. Sie haben die Teilnahme an der Unterweisung und die Kenntnis der Bedingungen und Risiken der Nutzung sowie die Kenntnis dieser Vereinbarung schriftlich zu bestätigen. Die Bestätigungen werden zu ihren Personalakten genommen (Anlage).

§ 7 Erstellung und Aufbewahrung von Protokollen

(1) Beim Einsatz der Fernwartungssoftware TeamViewer werden automatisiert Protokolle erstellt, die festhalten, wann wer welche Funktionen auf welchem Rechner ausgeführt hat.

(2) Protokolle werden für den Zeitraum von drei Monaten aufbewahrt, darüber hinaus nur bei Vorliegen von konkreten Anhaltspunkten für eine Straftat.

(3) Protokolle dürfen vom Personalrat unter Beteiligung der zuständigen Administratorin oder des zuständigen Administrators unter Beteiligung der oder des datenschutzbeauftragten eingesehen werden. § 22 Abs. 4 NDSG bleibt unberührt.

(4) Protokolle dürfen von der zuständigen Administratorin oder des zuständigen Administrators unter Beteiligung der oder des Datenschutzbeauftragten eingesehen werden, wenn dies zur Aufgabenerfüllung erforderlich ist.

§ 8 Weitergabe der Daten an Dritte

(1) Daten dürfen nicht an Dritte weitergegeben werden.

(2) Die Fernwartungssoftware darf nicht eingesetzt werden, um Externen den Zugriff auf PCs zu ermöglichen.

§ 9 Verhaltens- und Leistungskontrolle, personenbeziehbare Auswertungen von Protokollen

(1) Die Nutzung der sich aus dem Einsatz der Fernwartungssoftware TeamViewer ergebenden Möglichkeiten einer Verhaltens- und Leistungskontrolle ist nicht gestattet.

(2) Eine personenbeziehbare Auswertung von Protokollen ist nur bei hinreichendem Verdacht der Verletzung dienstrechtlicher bzw. arbeitsvertraglicher Pflichten oder auf Anordnung eines Gerichts bzw. einer Strafverfolgungsbehörde zulässig.

(3) Mit Ausnahme gerichtlich oder von einer Strafverfolgungsbehörde angeordneter Auswertungen ist vor einer beabsichtigten Auswertung die Zustimmung des Personalrates einzuholen. Er hat das Recht, an der seiner Zustimmung unterliegenden Auswertungen teilzunehmen. § 7 Abs. 3 gilt entsprechend.

§ 10 Schlussbestimmungen

(1) Die Dienstvereinbarung tritt mit der Unterzeichnung in Kraft. Sie ist unverzüglich in den Amtlichen Mitteilungen zu veröffentlichen.

(2) Sie kann von beiden Seiten mit einer Frist von sechs Monaten gekündigt werden. Die einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform.

(3) Mit Inkrafttreten dieser Dienstvereinbarung tritt die Dienstvereinbarung über die Einführung und Nutzung der Fernwartungssoftware NetOp Remote Control vom 08.09.2008 außer Kraft.

Oldenburg, den 16.12.2011

gez. Prof. Dr. Babette Simon
(Präsidentin)

gez. Bernd Wichmann
(Vorsitzender des Personalrats)

Bestätigung durch Frau/Herrn

(Name)

Hiermit bestätige ich meine Teilnahme an der Unterweisung zu der Fernwartungssoftware TeamViewer am
_____.

Ich wurde dabei über die Funktionalitäten des Programms, die technischen Möglichkeiten und die Einsatzbereiche aufgeklärt.

Außerdem wurde mir die Dienstvereinbarung über die Einführung und Nutzung der Fernwartungssoftware TeamViewer 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 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)