Dienstvereinbarung
über die Nutzung
von Fernwartungssoftware zwischen der
Hochschule Anhalt (Dienststelle) und dem
Personalrat der Hochschule Anhalt

vom 22.02.2016

§ 1
Grundsätze

(1) Diese Dienstvereinbarung regelt die Benutzung von Fernwartungssoftware (FWS), 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) Die FWS wird verwendet zur Fernsteuerung von PC-Problemen (z. B. in den Bereichen Betriebssystem, Anwendung, Konfiguration).

(2) Durch die FWS wird den Mitarbeitern der IT-Dienste, die PC-Nutzer betreuen, ein Arbeitsmittel zur Verfügung gestellt, 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 die aktive 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 FWS 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 Fernwartungszugriffen sind die Rechte für den Fernwartungszugriff auf den notwendigen Kreis an Beschäftigten im First- und Second-Level-Support beschränkt. Der Zugriff darf nur in dem Umfang erfolgen, der zur Analyse und Behebung des Problems bzw. Fehlers nötig ist. Die im First- und Second-Level-Support eingesetzten Beschäftigten haben sich vor dem Fernwartungszugriff dem Nutzer gegenüber 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 schriftlicher oder mündlicher 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 Fernwartungszugriff ist nur mit der vorherigen Zustimmung der Benutzerin oder des Benutzers zulässig. Die Benutzerin oder der Benutzer erteilt ihre oder 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 Fernwartungszugriff sofort zu löschen.

(2) Automatische Updates der System- und Anwendungssoftware sind ohne Zustimmung zulässig.
Eine Information der Benutzerin oder des Benutzers hat zu erfolgen.