LEUPHANA
UNIVERSITÄT LÜNEBURG

DV-SAP- FI, CO und PSM Anlage 2 - Dienstanweisung

Dienstanweisung zur Nutzung von SAP-PCs

1. Einleitung

Die Nutzung von PCs als Klientensysteme für SAP (SAP-PC) bedingt die Verarbeitung sensitiver Daten, die Unbefugten weder zur Kenntnis gelangen noch von ihnen in irgendeiner Weise manipuliert werden dürfen. Deshalb sind besondere Sicherheitsmaßnahmen erforderlich, um die Sicherheitsrisiken auf ein vertretbares Maß zu reduzieren.

Die Sicherheit liegt im Interesse des Landes Niedersachsen und der Leuphana Universität Lüneburg.

Während die Sicherheit für Server und Übertragungswege vom jeweiligen Serverzentrum zu verantworten ist, liegt die Sicherheit der SAP-PCs ausschließlich bei den jeweiligen Betreibern dieser Systeme. SAP-PCs sollen auch multifunktionell genutzt werden können; aufgrund dieser Anforderung ergeben sich zusätzliche Risiken. Sicherer Betrieb und sichere Nutzung von SAP-PCs können jedoch nicht allein mit technischen Mitteln erreicht werden, sondern benötigen die aktive Mitwirkung der Anwender/innen. Daraus resultieren die in dieser Dienstanweisung enthaltenen Verhaltensvorschriften.

Es sei ausdrücklich darauf hingewiesen, dass die Sicherheit des SAP-Betriebs Vorrang vor der Multifunktionalität hat. Es liegt damit durchaus auch im sachlichen Interesse der Anwender/innen, die in dieser Dienstanweisung enthaltenen Regelungen einzuhalten. Denn wenn eine hinreichende Sicherheit nicht gewährleistet werden kann, müsste die Multifunktionalität der SAP-PCs eingeschränkt bzw. aufgehoben werden.

Die Sicherheit ist ein sehr komplexes Gebiet, und die hier aufgenommenen Regelungen können keineswegs vollständig sein. Es ist daher wichtig, dass sich jede/r Nutzer/in eines SAP-PCs bewusst ist, dass er/sie in einer sicherheitsrelevanten Umgebung arbeitet und sich entsprechend umsichtig verhält. (Hinweis: es ist in diesem Zusammenhang unerheblich, ob der/die Nutzer/in SAP-GUI oder beispielsweise Bürosoftware nutzt. Entscheidend ist ausschließlich, dass er/sie an einem als SAP-PC gekennzeichneten Gerät arbeitet.)

2. Festlegungen

2.1. SAP-PCs

SAP-PCs im Sinne dieser Dienstanweisung sind PCs, die durch ihre Softwareausstattung als Klientensystem für SAP konfiguriert sind.

Auf SAP-PCs können weitere Softwareprodukte (z. B. Textverarbeitung) installiert sein, um diese auch anderweitig verwenden zu können (multifunktionaler PC); sie haben jedoch in jedem Fall den Status SAP-PC.

3. Geltungsbereich etc.

Die Dienstanweisung gilt für alle Nutzer/innen von SAP-PCs der Leuphana Universität Lüneburg. Sie gilt für alle auf diesen Rechnern arbeitenden Benutzer/innen unabhängig davon auf welche Weise sie einen SAP-PC nutzen.

Die vorliegende Dienstanweisung ergänzt, aber ersetzt nicht möglicherweise bereits bestehende anderweitige Anweisungen und/oder Vereinbarungen.

Sobald sich Überschneidungen mit anderen Anweisungen/Vereinbarungen ergeben, ist jeweils die Regelung anzuwenden, die ein höheres Maß an Sicherheit gewährleistet.

4. Anmeldung an SAP-PCs

Nutzer/innen melden sich mit ihrer persönlichen Benutzerkennung/Passwortkombination am SAP-PC an.

SAP Anwender benötigen zusätzlich eine persönliche Chipkarte (siehe unter 5.5).

5. Für Sicherheitsmaßnahmen

5.1. Hardware

Veränderungen der Hardware (Austausch, Einbau und Entfernen von Komponenten) sowie an den Grundeinstellungen (wie BIOS, Systemeinstellungen) dürfen ausschließlich vom verantwortlichen Administrator vorgenommen werden.

Der Einsatz privater PCs als SAP-PC ist wegen der damit verbundenen Sicherheitsrisiken (Viren etc.) grundsätzlich untersagt. Eine Koppelung privater Geräte mit SAP-PCs ist verboten.

5.2. Software

Die Installation von Software erfolgt ausschließlich durch den verantwortlichen Administrator.

Jegliche eigenmächtige Installation von Software ist verboten. Falls versehentlich eine Installation gestartet wurde, ist dieser Vorgang sofort abzubrechen.

Zur Nutzung des SAP-PCs sind ausschließlich die Softwareprodukte zu verwenden, die vom Administrator zugelassen sind. Die explizite Verwendung von anderer Software, die ggfs. auf den SAP-PCs vorhanden ist, ist verboten.

Installation/Einsatz/Start privat beschaffter Software ist ebenso verboten.

5.3. Passwörter

Für den Umgang mit Passwörtern gelten die einschlägigen Maßnahmen. Insbesondere ist zu beachten:
- Das Passwort ist geheim zuhalten.
- Die schriftliche Fixierung muss an einem sicheren Ort verwahrt werden.
- Eine Weitergabe des Passworts ist untersagt.
- Die Benutzung fremder Benutzerkennungen/Passwortkombinationen ist verboten.

Das Passwort muss eine Mindestlänge von acht Zeichen haben. Die Einbeziehung von Ziffern sowie Groß- und Kleinschreibung wird dringend empfohlen.

Folgende Regelung sollten berücksichtigt werden:
- Bei der Wahl des Passworts dürfen keine Trivialnamen verwendet werden!
- Kein Wort/Begriff/Name aus dem persönlichen Umfeld (weder privat noch dienstlich).
- Kein Wort, das in einem deutsch- oder fremdsprachigen Lexikon enthalten ist.
- Gut: Buchstaben (groß und klein) mit Ziffern mixen.

5.4. Chipkarten

Die Benutzerauthentisierung für SAP erfolgt über persönliche Chipkarten. Der zur Nutzung der Chipkarten erforderliche Pin-Code unterliegt der gleichen Sorgfaltspflicht des Anwenders wie ein Passwort. (Er darf nur Ziffern enthalten und besteht aus mindestens 6 Ziffern (8 Ziffern bei den neuen Karten).

Chipkarten sind sicher zu verwahren. Sie dürfen anderen Personen nicht überlassen werden. Es ist verboten, fremde Chipkarten zu benutzen (siehe auch 5.7)

Der Verlust der Chipkarte ist sofort dem/r zuständigen Key-User/in zu melden.

5.5. Nutzung des Internet

5.5.1. Installation von Programmen:

Die Nutzung des Internet ist mit besonderen Risiken verbunden, da unbemerkt schädliche Programme eingeschleust werden können, die SAP-PCs auf unvorhersehbare und äußerst gefährliche Weise manipulieren können.

Das Herunterladen, Starten oder die direkte Installation von Programmen aus dem Internet ist grundsätzlich verboten! Versehentlich initialisiertes Herunterladen oder Installieren ist sofort abzubrechen.

5.5.2. E-Mail:

Anhänge von E-Mails können Viren und andere gefährliche Programme enthalten. Das automatische Öffnen dieser Anhänge muss daher im Mailprogramm grundsätzlich deaktiviert sein. Anhänge von E-

Mails aus unbekannter Quelle oder mit unverlangtem Inhalt sollten nicht geöffnet, sondern gelöscht werden. In Zweifelsfällen ist der verantwortliche Administrator hinzuzuziehen.

5.6. Weitere Sicherheitsmaßnahmen

Wird der SAP-PC (auch nur vorübergehend) verlassen und soll die Sitzung anschließend fortgesetzt werden, so hat der Nutzer den SAP-PC in jedem Fall zu sperren (Tastenkombination Strg+Alt+Entf.). Soweit mit Chipkarte gearbeitet wurde, ist sie aus dem Chipkartenleser zu entfernen und sicher zu verwahren, damit sie nicht in unbefugte Hände gelangen. (Hinweis: das Ziehen der Chipkarte allein bewirkt keinerlei Zugangssperre)

Datenbestände auf der Festplatte sowie ggf. auf externen Datenträgern sind regelmäßig auf Virenfreiheit zu prüfen.

6. Störungen/Fehler/sicherheitsrelevante Ereignisse

Störungen und Fehler sowie jedes außergewöhnliche Erscheinungsbild oder Verhalten eines SAP-PCs sind sofort dem Administrator zu melden.

7. Weitere Informationen

Aktuelle Informationen und Warnhinweise zur IT-Sicherheit sowie der Fortschreibung dieser Dienstanweisung werden per E-Mail mitgeteilt und sind zu beachten.