Dienstvereinbarung

zum Einsatz des System Center Configuration Managers

zwischen der Universität Trier

- vertreten durch den Präsidenten -

und
dem Personalrat der Universität Trier

- vertreten durch die Vorsitzende -

Präambel

Der Abschluss der Dienstvereinbarung dient dem Schutz der Beschäftigten vor unbefugtem oder unkontrolliertem Zugriff auf ihre IT-Systeme. Durch sie wird vorgeschrieben, dass nur benannte Personen als bevollmächtigte Administratoren/innen und nur die in der Dienstvereinbarung autorisierten Softwaresysteme eingesetzt werden.

§ 1 Geltungsbereich

Die Dienstvereinbarung gilt für alle Beschäftigten der Universität Trier. Die Dienstvereinbarung regelt den hochschulweiten Einsatz des SCCMs (System Center Configuration Manager) zur Betreuung und Wartung aller universitätseigenen IT-Systeme.

§ 2 Begriffsbestimmung

(1) Unter **Fernwartung** wird der Zugriff von Servicetechnikern (Administratoren/innen) auf IT-Systeme zu Wartungs- und Reparaturzwecken aus der Ferne verstanden. Fernwartung ermöglicht Aktionen über das Netzwerk von einem System auf ein anderes, ohne direkt vor Ort zu sein. Fernwartungsszenarien sind Fernzugriff, Softwareverteilung und Ferninventur.

(2) Bei einem **Fernzugriff** wird durch den/die bevollmächtigte(n) Administrator/in eine Verbindung mit dem entfernten IT-System des Nutzers hergestellt. Tastaturanschläge, Mausbewegungen und Bildschirmausgaben werden übertragen.

(3) **Softwareverteilung** umfasst die automatisierte Verteilung und Installation bzw. De-Installation von Softwarepaketen und -komponenten (Updates, Upgrades, Patches) für System- und Anwendungssoftware auf entfernten IT-Systemen.

(4) Durch eine **Ferninventur** erfolgt eine automatisierte Bestandsaufnahme der Hard- und Softwarekomponenten von IT-Systemen.

(5) **Administratoren/innen** im Sinne dieser Dienstvereinbarung sind Beschäftigte im ZIMK oder in den Struktureinheiten, zu deren Aufgaben die Betreuung und Wartung dienstlicher IT-Systeme der Universität gehört.

(6) Ein informationstechnisches System (**IT-System**) im Sinne dieser Dienstvereinbarung ist ein universitätseigenes elektronisches datenverarbeitendes System, welches dienstlich genutzt wird, z.B. ein Computer, Drucker, Notebook oder Smartphone.

§ 3 Zweckbestimmung

(1) Die Dienstvereinbarung regelt die Einführung und den Einsatz des SCCM als Dienst zum kontrollierten Zugriff auf ein entferntes IT-System. Der SCCM ist ein IT-Werkzeug zur Fernwartung von IT-Systemen, das hochschulweit zur Fehlererkennung und -behebung, Verwaltung und Inventarisierung vorhandener Hard- und Software sowie zur automatischen Softwareverteilung der ans Hochschulnetz angeschlossenen universitätseigenen Computer verwendet wird.

(2) Der SCCM wird unter Gewährleistung des Schutzes der Persönlichkeitsrechte der Beschäftigten eingesetzt. Eine Leistungs- und Verhaltenskontrolle der Mitarbeiter/innen ist verboten. Zuwiderhandlungen werden disziplinar- oder arbeitsrechtlich verfolgt.

(3) Zweck der Fernwartung, insbesondere des Fernzugriffs, ist es, dass Administratoren/innen Fehler in der Funktionalität der IT-Systeme beheben oder Unterstützung bei deren Einsatz geben können, ohne sich selbst vor Ort begeben zu müssen, wo die Störung aufgetreten ist bzw. die Hilfe benötigt wird.

(4) Eine automatische Softwareverteilung erfolgt, damit dauerhaft und ohne großen zeitlichen Aufwand die Funktionsfähigkeit der IT-Systeme gewährleistet bzw. auf den neuesten Stand gebracht werden kann.

(5) Die Ferninventur der Hard- und Software dient der Erfassung der vorhandenen Hardware-bestandteile und Softwarelizenzen. Die im Rahmen der Ferninventur erhobenen Daten dienen ausschließlich der Sicherung der Funktionalität des Hochschulnetzes sowie der Durchführung von IT-Strukturmaßnahmen und der Einhaltung rechtlicher Bestimmungen (Compliance).

§ 4 Rahmenbedingungen für den Einsatz

(1) Die Funktionen des SCCMs werden durch festgelegte Mitarbeiter/innen (Administratoren/innen) verwendet. Das ZIMK führt eine Liste (siehe Anlage) mit den vorhandenen Zugangsberechtigungen und teilt dem Personalrat Änderungen der Zugangsberechtigungen unverzüglich mit.

(2) Der Fernzugriff zur Behebung von Fehlern (Supportleistung) muss vom Benutzer selbst angefordert werden und erfolgt ausschließlich im Dialog. Dem Zugriff muss ausdrücklich zugestimmt werden. Die Benutzerin/der Benutzer kann den Fernzugriff jederzeit beenden.

(3) Im Rahmen der Softwareverteilung wird der Benutzer in der Standardeinstellung zum Start der Installation aufgefordert. Auf Anfrage des/der Benutzers/Benutzerin können die Programme vollautomatisiert installiert werden.

(4) Die Ferninventur der Rechner erfolgt automatisch und ausschließlich durch das ZIMK. Das Inventarisierungsprogramm durchsucht die Rechner nur nach der installierten Software. Die Ergebnisse dienen dem Abgleich mit den von der Universität Trier erworbenen Softwarelizenzen und als Daten für die Software- und Lizenzverwaltung.

Identifiziert wird die Liste installierter Programme. Es ist nur der Zugriff auf System- und Programmdateien gestattet. Jegliche Art von Zugriffen auf nutzereigene Dateien ist verboten!

§ 5 Datenschutz

(1) Die Nutzung des SCCMs steht nur den zugriffsberechtigten Mitarbeitern/Mitarbeiterinnen (Administratoren/innen) zu, die auf einer entsprechenden Liste (siehe Anlage) festgehalten werden. Der Systemzugang ist durch ein Passwort geschützt.

(2) Bei der Ferninventur werden Daten über die Hardwareausstattung sowie die vorhandene Software (Programme, Versionen, Patch-Stand) erhoben und gespeichert. Dateiinhalte sind nicht betroffen. Die Inventarisierung läuft automatisch ab.

(3) Die Auswertung erhobener Daten erfolgt ausschließlich durch zugriffsberechtigte Mitarbeiter/innen (Administratoren/innen).

(4) Die Daten der Ferninventur werden mit Hilfe des SCCMs aufbereitet und verdichtet, um einen Vergleich mit den Daten der Lizenzverwaltung zu ermöglichen. Bei Abweichungen werden Listen erzeugt, um eine Überprüfung des Lizenzbedarfs zu ermöglichen.

(5) Es werden keine Daten über das Verhalten der Beschäftigten bzw. Nutzungsprofile erhoben. Dazu zählen insbesondere Daten zum Aufruf und zur Beendigung von Programmen aus denen sich die Verwendung bzw. Nutzungsdauer einzelner Anwendungen ergeben oder die Erfassung von An- und Abmeldezeiten.

(6) Allen Zugriffsberechtigten ist es untersagt, personenbezogene Daten, die ihnen im Rahmen ihrer Aufgabenerfüllung bekanntwerden, zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren; dies gilt auch nach Beendigung ihrer Tätigkeit.

(7) Die Standardeinstellungen des SCCM-Klienten sowie die Einstellungen des Virenscanners sind jederzeit auf den IT-Systemen (Systemsteuerung) einsehbar und in der Anlage zur Dienstvereinbarung spezifiziert.

(8) Listen-Rollenkonzept: Pro Geltungsbereich ist ein/e Hauptadministrator/in und ein/e stellvertretende/r Hauptadministrator/in zu benennen. Der/die verantwortliche Hauptadministrator/in befindet sich in einem festen Arbeitsverhältnis zum Arbeitgeber. In Ausnahmefällen können stellvertretende Hauptadministratoren/innen zeitlich befristet beschäftigt sein.

§ 6 Beteiligung des Personalrats und der/des Datenschutzbeauftragten

(1) Der Personalrat kann die Einhaltung der Regelungen der Dienstvereinbarung jederzeit unangekündigt kontrollieren und überwachen. Zur Kontrolle darf der Personalrat interne, ggf. externe, Sachverständige hinzuziehen.

(2) Er hat das Recht, vorhandene Projekt- und Protokolldaten des gesamten Systems unangekündigt einzusehen und sich erläutern zu lassen. Die Mitarbeiter/innen des ZIMKs haben den Personalrat bei seiner Kontrollpflicht zu unterstützen und sind diesem gegenüber auskunftspflichtig.

(3) Die/der Datenschutzbeauftragte hat die gleichen Rechte wie der Personalrat.

(4) Um die Einhaltung der Fernwartungsszenarien zu überprüfen, ist dem Personalrat oder einem /einer von diesem beauftragten Sachverständigen und dem/der Datenschutzbeauftragten auf Verlangen unverzüglich der erforderliche Zugang zu allen Fernwartungssystemen zu gewähren.

§ 7 Beweisverwertungsverbot

Informationen, die unter Verstoß gegen die vorgenannten Bestimmungen erhoben oder verarbeitet wurden, sind als Beweismittel zur Begründung personeller Maßnahmen (z.B. Abmahnung, Versetzung, Kündigung) nicht zulässig. Hierauf gestützte Einzelmaßnahmen sind unwirksam.

§ 8 Schlussbestimmungen

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

(2) Die Beschäftigten, die vom Einsatz dieser Software betroffen sind, werden über deren Anwendung und die Folgen für ihren Arbeitsplatz bzw. ihre Arbeitsabläufe rechtzeitig und umfassend informiert. Hierzu werden für die betroffenen Bereiche Informationsveranstaltungen durchgeführt und schriftliche Informationen zu Verfügung gestellt. Die Dienstvereinbarung wird ihnen bekanntgemacht. Sie werden insbesondere darauf hingewiesen, dass ausschließlich lizenzierte Software auf den Arbeitsplatzrechnern installiert sein darf und über die besonderen Probleme im Umgang mit unlizenzierter Software informiert.

(3) Alle Mitarbeiter/innen der Universität, die mit dem System arbeiten, müssen in geeigneter Weise geschult und über die Inhalte der Dienstvereinbarung in Kenntnis gesetzt sein.

(4) Änderungen und Erweiterungen der Dienstvereinbarung und deren Anlagen sind jederzeit schriftlich mit Zustimmung des Personalrates ohne Kündigung der Dienstvereinbarung möglich.

(5) Die Dienstvereinbarung tritt mit der Unterzeichnung beider Parteien in Kraft. Sie ist von beiden Seiten mit einer Frist von sechs Monaten kündbar.

(6) Die Kündigung bedarf der Schriftform. Nach Eingang der Kündigung sind unverzüglich Verhandlungen über eine neue Vereinbarung aufzunehmen. Bis zum Inkrafttreten einer neuen Dienstvereinbarung gilt die gekündigte fort.

Trier, den	Trier, den
Der Präsident	Die Vorsitzende des Personalrates
_____	_____
Univ.-Prof. Dr. Michael Jäckel	Maria Kiefer-Koltes

Anlagen zur
Dienstvereinbarung zum Einsatz des
System Center Configuration Managers (SCCM)

1 Standardeinstellungen der Klienten

Die Einstellungen (d.h. aktiven Komponenten) des lokal installierten Klienten können unter folgendem Pfad eingesehen werden:

 Systemsteuerung -  > Configuration Manager

Auflistung **aller** Komponenten einschließlich deren **Standardwerte**:

Komponente	Status	Bemerkung
CCM-Benachrichtigungs-Agent	Aktiviert	Ermöglicht es dem Klienten eine Nachricht an den Benutzer zu senden. Z.B.: „Es liegt neue Software bereit zur Installation – möchten Sie diese installieren?“
Quelllistenupdate-Agent	Aktiviert	Quelllisten sind Orte von denen Windows Betriebssystemupdates und generelle Neuerungen beziehen. Z.B.: Windows Update ist eine Quelle. Der SCCM leitet diese Anfragen auf einen zentralen WSUS Server um. Damit wird der externe Netzwerkverkehr stark entlastet.
Softwareinventur-Agent	Aktiviert	Diese Komponente erzeugt eine Liste der installierten Software und übermittelt diese an den SCCM. Die Liste ist die gleiche Liste wie sie unter „Systemsteuerung -> Programme & Funktionen“ zu finden ist.
Softwareverteilungs-Agent	Aktiviert	In regelmäßigen Abständen wird auf dem SCCM nach neuer Software gesucht und dem Benutzer angeboten.
Energieverwaltungs-Agent	Deaktiviert	standardmäßig ohne Funktion
Hardwareinventur-Agent	Deaktiviert	standardmäßig ohne Funktion
Kompatibilitäts- und Einstellungsverwaltung	Deaktiviert	standardmäßig ohne Funktion
Softwaremessungs-Agent	Deaktiviert	standardmäßig ohne Funktion
Softwareupdate-Agent	Deaktiviert	standardmäßig ohne Funktion
Out-of-Band-Verwaltungs-Agent	Aktiviert	standardmäßig ohne Funktion (aber aktiviert) --- Die Komponente wird nur im Zusammenhang mit Pool-Computern verwendet, die die neue Technologie „Intel V-Pro“ unterstützen. Diese ermöglicht, grundlegende BIOS Einstellungen, wie z.B.: „Boot von Festplatte 1“ ---
Remotetools-Agent	Deaktiviert	Die Komponente ist universitätsweit deaktiviert!
CCM-Framework	Installiert	Grundlage des Klienten
CCM-Richtlinien-Agent	Installiert	Grundlage des Klienten
CCM-Status- und Ereignis-Agent	Installiert	Grundlage des Klienten
Gemeinsame SMS-Komponenten	Installiert	Grundlage des Klienten
Kernkomponenten	Installiert	Grundlage des Klienten

Komponenten für die Betriebssystembereitstellung	Installiert	Ermöglich Betriebssysteminstallationen, wie z.B. in der Computerwerkstatt des ZIMKs.
Tasksequenzkomponenten	Installiert	Eine Erweiterung der Betriebssystembereitstellung. Nach der grundlegenden Installation von Windows ermöglicht diese die zusätzliche Installation von Treibern oder Veränderung von Einstellungen, wie z.B. das Hinzufügen zur Domäne.
Wartungstaskkoordinator	Installiert	Die Komponente ist der „Terminplaner“ des SCCM. Sie sorgt dafür, dass z.B. während einer Benutzeranmeldung keine Neustarts gemacht werden oder rechenintensive Softwareinstallationen erst nach den Arbeitszeiten passieren.

Hinweis: In der Standardeinstellung des Klienten, werden Softwareupdates nicht automatisiert ohne Zustimmung des Benutzers installiert. Wünscht der/die Benutzer/in eine automatische Installation der Softwareupdates, muss dieses mit dem/der Administrator/in des jeweiligen Klientsystems abgestimmt werden.

2 Einstellung Virenscanner (SCEP)

Der vom SCCM unterstütze Virenscanner System Center Endpoint Protection (SCEP) kann als „unmanaged“ oder als „managed“ installiert werden. In der „unmanaged“-Variante, ist der Benutzer für alle Einstellungen, Pflege und Updates selber verantwortlich. In der „managed“-Version werden alle Updates vom SCCM verteilt, so dass der Benutzer immer einen aktuellen Virenscanner einsetzt. Zusätzlich wird auf verschiedene Einstellungen geachtet (Pflege), die ein Gleichgewicht zwischen Sicherheit und Geschwindigkeit sicherstellen.

Auflistung der Standard SCEP-Einstellungen:

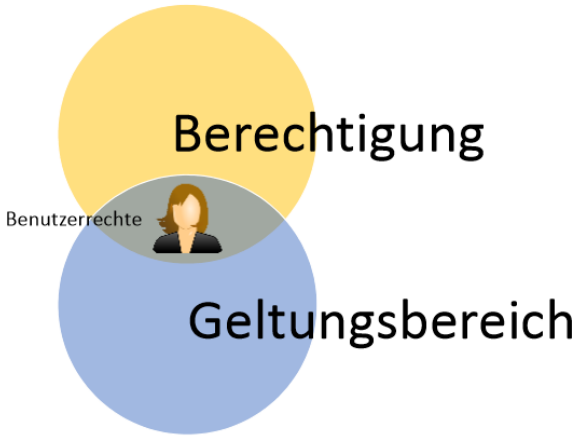
Gruppe	Name	Wert
Geplante Überprüfungen	Aktiviert	Ja
	Überprüfungstyp	Schnellüberprüfung
	Tag der Überprüfung	jeden Montag
	Zeit	08:00
	tägliche Überprüfung	Nein
	vor Überprüfung Updaten	Ja
	Nur starten, wenn Computer im Leerlauf ist	Ja
	Überprüfungen erzwingen, wenn diese 2x ausgefallen ist	Ja
	CPU Auslastung begrenzen auf	50%
Überprüfungseinstellungen	E-Mails und Anhänge überprüfen	Nein
	Wechselmedien überprüfen	Nein
	Netzlaufwerke überprüfen	Nein
	Archivdaten überprüfen	Nein
	Benutzer darf CPU-Begrenzung konfigurieren.	Ja
	Benutzersteuerung bei Überprüfung	Vollzugriff
Standardaktionen	Schwerwiegende Bedrohung	Quarantäne
	Hohe Bedrohung	Quarantäne
	Mittlere Bedrohung	Quarantäne
	Niedrige Bedrohung	Quarantäne
Echtzeitschutz	Aktiviert	Ja
	Datei und Programmaktivität überwachen	Ja
	Systemdateien überprüfen	Ja
	alle heruntergeladenen Dateien und Anhänge überprüfen	Ja
	Verhaltensüberwachung aktivieren	Ja
	Schutz gegen netzwerkbasierte Exploits aktivieren	Ja
	Benutzer das Konfigurieren gestatten	Ja

Ausschlusseinstellungen	ausgeschlossene Ordner	Liste mit verschiedenen Windows-Verzeichnissen, die nicht gescannt werden sollten/dürfen
	ausgeschlossene Dateitypen	(keine)
	ausgeschlossene Prozesse	(Keine)
Erweitert	Vor dem Bereinigen von Computern einen Systemwiederherstellungspunkt erstellen.	Nein
	Benutzeroberfläche deaktivieren	Nein
	Benachrichtigungen anzeigen	Ja
	Dateien in Quarantäne löschen	Ja, nach 30 Tagen
	Benutzern das Konfigurieren der Quarantäne gestatten	Ja
	Benutzern das Konfigurieren der Ausschlusseinstellungen gestatten	Ja
	Allen Benutzern die Anzeige der vollständigen Verlaufsergebnisse gestatten	Nein /
	Überprüfung von Analysepunkten aktivieren	Ja
	Startzeiten zufällig erzeugen	Nein
Außerkraftsetzungen von Bedrohungen	Außerkraftsetzungsaktion	(keine)
Microsoft Active Protection Service	MAPS-Mitgliedschaftstyp	Nicht an MAPS teilnehmen
	Benutzern das Ändern gestatten	Nein
Definitionsupdates	Suche nach Updates	alle 2 Stunden
	Update erzwingen, wenn dieses 2x ausgefallen ist	Nein
	Quellen für Updates	SCCM-Quelleliste*
	Alternative Quelle der Liste verwenden, wenn Definition älter als	72 Stunden ist

*Global geltende Liste mit 4-Quellen:

1. SCCM – Server (zimksccm.uni-trier.de)
2. WSUS – Server (zimksccm.uni-trier.de) // Könnte auch ein anderer WSUS Server sein.
3. Microsoft Update
4. Microsoft Malware Protection Center Updates

3 Rollensystem (Benutzerrechte)



Die Benutzerrechte ergeben sich aus der Überschneidung eines zugewiesenen Geltungsbereichs (Anlage 4) und der Berechtigung (Sicherheitsrolle) (Anlage 5). Der Benutzer kann weder in anderen Geltungsbereichen seine gesetzten Sicherheitsrechte verwenden, noch im gesetzten Geltungsbereich außerhalb seiner Rolle fungieren.

4 Geltungsbereiche

ALL: Vom System vorgegeben, umfasst alle Geltungsbereiche

POOLS: Geltungsbereich für alle Computer in den CIP – Pools.

SCEP: Geltungsbereich für den Virenscanner.

VDV: Geltungsbereich für die Computer in der Verwaltungsdatenverarbeitung.

ZIMK: Geltungsbereich für Computer der Mitarbeiter, außer VDV-Bereich.

5 Sicherheitsrollen (Berechtigungen)

Sicherheitsrolle	Beschreibung
Analyst mit Leseberechtigung	Erteilt Berechtigungen zur Anzeige aller Configuration Manager-Objekte.
Anwendungsadministrator	Hiermit werden Berechtigungen zum Ausführen der Rollen "Anwendungsbereitstellungs-Manager" und "Anwendungsautor" gewährt. Administratoren, denen diese Rolle zugeordnet ist, können zudem Abfragen verwalten, Standorteinstellungen anzeigen, Sammlungen verwalten, die Einstellungen der Affinität zwischen Benutzer und Gerät bearbeiten und virtuelle App-V-Umgebungen verwalten.
Anwendungsautor	Hiermit werden Berechtigungen zum Erstellen, Ändern und Außerkraftsetzen von Anwendungen gewährt. Administratoren, denen diese Rolle zugeordnet ist, können außerdem Anwendungen, Pakete und virtuelle App-V-Umgebungen verwalten.
Anwendungsbereitstellungs-Manager	Hiermit werden Berechtigungen zum Bereitstellen von Anwendungen gewährt. Administratoren, denen diese Rolle zugeordnet ist, können eine Liste der Anwendungen anzeigen und Bereitstellungen für Anwendungen, Warnungen, Vorlagen und Pakete sowie Programme verwalten. Ferner können Administratoren, denen diese Rolle zugeordnet ist, Sammlungen und deren Mitglieder, Statusmeldungen, Abfragen, Regeln für eine bedingte Bereitstellung und virtuelle App-V-Umgebungen anzeigen.
Asset-Manager	Erteilt Berechtigungen zum Verwalten des Asset Intelligence-Synchronisierungspunkts, der Asset Intelligence-Berichtsklassen, der Software- und Hardwareinventur und der Messungsregeln.
Betriebsadministrator	Erteilt Berechtigungen für alle Aktionen in Configuration Manager mit Ausnahme derer, die zur Verwaltung der Sicherheit erforderlich sind. Zu letzterer gehört die Verwaltung der Administratoren, der Sicherheitsrollen und der Sicherheitsbereiche.
Betriebssystembereitstellungs-Manager	Hierdurch werden Berechtigungen zum Erstellen von Betriebssystemabbildern und für deren Bereitstellung auf Computern gewährt. Administratoren, denen diese Rolle zugeordnet ist, können Installationspakete und Abbilder von Betriebssystemen, Tasksequenzen, Treiber, Startabbilder und Zustandsmigrationseinstellungen verwalten.
Endpoint Protection-Manager	Hierdurch werden Berechtigungen zum Definieren und Überwachen von Sicherheitsrichtlinien gewährt. Administratoren, denen diese Rolle zugeordnet ist, können

	Endpoint Protection-Richtlinien erstellen, ändern und löschen. Außerdem können sie Sammlungen Endpoint Protection-Richtlinien bereitstellen, Warnungen erstellen und ändern und den Endpoint Protection-Status überwachen.
Hauptadministrator	Erteilt sämtliche Berechtigungen in Configuration Manager. Der Administrator, der eine neue Configuration Manager-Installation erstellt, wird dieser Sicherheitsrolle, allen Bereichen und allen Sammlungen zugewiesen.
Infrastrukturadministrator	Hierdurch werden Berechtigungen zum Erstellen, Löschen und Ändern der Configuration Manager-Serverinfrastruktur und zum Durchführen von Migrationstasks gewährt.
Kompatibilitätseinstellungs-Manager	Erteilt Berechtigungen zum Definieren und Überwachen von Kompatibilitätseinstellungen. Administratoren, die dieser Rolle zugewiesen sind, können zudem Konfigurationselemente und Basislinien bearbeiten und löschen. Sie können außerdem Konfigurationsbasislinien für Sammlungen bereitstellen, eine Kompatibilitätsauswertung aktivieren und die Wiederherstellung für nicht kompatible Computer aktivieren.
Remotetoolsverantwortlicher	Hierdurch werden Berechtigungen zum Ausführen und Überwachen der Remoteverwaltungstools gewährt, mit deren Hilfe Benutzer Computerprobleme lösen können. Administratoren, denen diese Rolle zugeordnet ist, können über die Configuration Manager-Konsole die Remotesteuerung, die Remoteunterstützung und den Remotedesktop ausführen. Außerdem können sie die Out-of-Band-Verwaltungskonsole und die AMT-Energiesteuerungsoptionen ausführen.
Sicherheitsadministrator	Erteilt Berechtigungen zum Hinzufügen und Entfernen von Administratoren und zum Zuweisen von Administratoren zu Sicherheitsrollen, Sammlungen und Sicherheitsbereichen. Administratoren, die dieser Rolle zugewiesen sind, können zudem Sicherheitsrollen und diesen zugewiesene Sicherheitsbereiche und Sammlungen erstellen, bearbeiten und löschen.
Softwareupdate-Manager	Erteilt Berechtigungen zum Definieren und Bereitstellen von Softwareupdates. Administratoren, die dieser Rolle zugewiesen sind, können zudem Softwareupdategruppen, Bereitstellungen und Bereitstellungsvorlagen verwalten und Softwareupdates für den Netzwerkzugriffsschutz (Network Access Protection, NAP) aktivieren.

6 Liste der Mitarbeiter/innen-Rollen

Mitarbeiter	Rolle	Geltungsbereich
Klein, Achim	Asset-Manager	All
Lengerke, Johana von	Asset-Managerin	All
Leoprechting, Alexander von	Hauptadministrator Stellvertreter	All
Schilz, Marc	Hauptadministrator	All
Hilfskraft/Aushilfskraft 1 **	Anwendungsautor	Pools
Hilfskraft/Aushilfskraft 2 **	Anwendungsautor	Pools
Zonker, Volkmar	Anwendungsadministrator	ZIMK, Pools
Auszubildende Endgeräte Service*	Anwendungsautor	ZIMK, Pools
Auszubildende System Center*	Anwendungsbereitstellungs-Manager	ZIMK, Pools
Baltes-Götz, Bernhard	Anwendungsadministrator	ZIMK, Pools
Bredtmann, Andreas	Hauptadministrator Stellvertreter	VDV
Christmann, Ralf	Hauptadministrator	VDV
Wick, Christoph	Anwendungsautor	VDV
Röpke, Jörg	Hauptadministrator	UB
Sauerwein, Harald	Hauptadministrator Stellvertreter	UB
Hansen, Wilhelm	Hauptadministrator Stellvertreter	UB
Kickertz, Johannes	Anwendungsautor	UB

* Die Auszubildenden im ZIMK wechseln im Rahmen des internen Rotationsmodells alle drei Monate. Innerhalb der Rotation ist jederzeit nachvollziehbar, welche/r Auszubildende zu welchem Zeitpunkt die jeweilige Rolle wahrgenommen hat.

** Wissenschaftliche Hilfskräfte/Studentische Aushilfskräfte melden sich mit Ihrer personenbezogenen Nutzerkennung am System an und haben nur während Ihrer Vertragslaufzeit Berechtigungen. Es ist jederzeit nachvollziehbar, wer die Benutzerrolle zum jeweiligen Zeitpunkt wahrgenommen hat.

§ 8 Schlussbestimmungen

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

(2) Die Beschäftigten, die vom Einsatz dieser Software betroffen sind, werden über deren Anwendung und die Folgen für ihren Arbeitsplatz bzw. ihre Arbeitsabläufe rechtzeitig und umfassend informiert. Hierzu werden für die betroffenen Bereiche Informationsveranstaltungen durchgeführt und schriftliche Informationen zu Verfügung gestellt. Die Dienstvereinbarung wird ihnen bekanntgemacht. Sie werden insbesondere darauf hingewiesen, dass ausschließlich lizenzierte Software auf den Arbeitsplatzrechnern installiert sein darf und über die besonderen Probleme im Umgang mit unlizenzierter Software informiert.

(3) Alle Mitarbeiter/innen der Universität, die mit dem System arbeiten, müssen in geeigneter Weise geschult und über die Inhalte der Dienstvereinbarung in Kenntnis gesetzt sein.

(4) Änderungen und Erweiterungen der Dienstvereinbarung und deren Anlagen sind jederzeit schriftlich mit Zustimmung des Personalrates ohne Kündigung der Dienstvereinbarung möglich.

(5) Die Dienstvereinbarung tritt mit der Unterzeichnung beider Parteien in Kraft. Sie ist von beiden Seiten mit einer Frist von sechs Monaten kündbar.

(6) Die Kündigung bedarf der Schriftform. Nach Eingang der Kündigung sind unverzüglich Verhandlungen über eine neue Vereinbarung aufzunehmen. Bis zum Inkrafttreten einer neuen Dienstvereinbarung gilt die gekündigte fort.

Trier, den 15.1.2019
Der Präsident

Univ.-Prof. Dr. Michael Jäckel

Trier, den 15. Jan. 2019
Die Vorsitzende des Personalrates

Maria Kiefer-Koltes