

Dienstvereinbarung

zwischen dem Personalrat der Universität Trier, vertreten durch den Vorsitzenden

und

der Universität Trier, vertreten durch den Präsidenten

zur

Einführung und zum Betrieb von Informationssystemen mit Chipkartennutzung (CIS)

Die Universität beabsichtigt die Ausgabe einer Chipkarte an alle Beschäftigten, mit deren Hilfe betriebliche Prozesse vereinfacht durchgeführt werden können. Diese Vereinbarung enthält Rahmenregelungen für den Betrieb der dafür notwendigen Informationssysteme, die Rechte der Beschäftigten und des Personalrates. Informationssysteme sind alle optischen, akustischen, mechanischen und elektronischen Geräte einschließlich der Software, die zur Verarbeitung, Verwaltung und Neuorganisation dieser Betriebsprozesse bestimmt sind.

§ 1 Geltungsbereich

Diese Dienstvereinbarung gilt für die erstmalige Inbetriebnahme, den laufenden Betrieb eines CIS sowie späterer Erweiterungen an der Universität Trier. Insbesondere fallen unter den Geltungsbereich der Dienstvereinbarung folgende Anwendungen:

1. Nutzung der Chipkarte als Dienstausweis
2. Freiwillige Nutzung der Chipkarte als Zahlungsmittel
3. Bibliotheksbenutzung
4. Arbeitszeiterfassung für die Mitarbeiter in bestimmten Bereichen
5. Zutrittssysteme zu Gebäuden und Räumen, Parkplatznutzung
6. Zugangssysteme via Kommunikationsnetz zu Daten und Dienstleistungen
7. Dienstliche Kopierernutzung
8. Durchführung von Hochschulwahlen

Einzelheiten zu den Anwendungen der lfd. Nr. 3 – 8 sind im Rahmen der Umsetzung einvernehmlich durch Einzelvereinbarungen zu regeln.

§ 2 Zweckbestimmung der Informationssysteme

- (1) Ziel der Einführung eines CIS ist die Stärkung der Leistungsfähigkeit sowie die Erhöhung der Servicefreundlichkeit der Universität, nicht der Abbau von Beschäftigung.
- (2) Eine Leistungs- und Verhaltenskontrolle findet nicht statt. Personenbezogene oder personenbeziehbare Daten dürfen nur nach gesetzlichen Vorschriften, tarifrechtlichen Vereinbarungen und den Regelungen dieser Dienstvereinbarung gespeichert, verarbeitet und genutzt werden. Die Teilsysteme dürfen nur entsprechend ihrer Zweckbestimmung genutzt werden. Eine darüber hinausgehende Verhaltenskontrolle und Verknüpfung von Daten ist nicht statthaft.

- (3) Ausdrücklich nicht zur Zweckbestimmung gehört die Überwachung der Leistung und des Verhaltens der Beschäftigten sowie die Erstellung von Nutzungs- und Arbeitsprofilen. Außer den in § 1 genannten CIS sollen nach derzeitigem Sachstand keine anderen Informationssysteme auf Kartenbasis eingeführt werden.
- (4) Der Dienstausweis dient der Identifikation der Beschäftigten intern und extern gegenüber Dritten.
- (5) Die Bibliotheksnutzung wird durch ein Selbstverbuchungssystem erleichtert. Ziel ist es den Bargeldverkehr in den Bibliotheken zu reduzieren. Die Inanspruchnahme von Leistungen soll auch weiterhin gegen Barzahlung möglich sein.
- (6) Die Arbeitszeiterfassung dient dem Ermitteln von An- und Abwesenheitszeiten mit Hilfe von elektronischen Erfassungssystemen.
- (7) Die Zutritts- und Zugangsberechtigung mit Chipkarten dient dem Schutz der Mitarbeiter/innen und des Eigentums der Dienststelle und soll die mißbräuchliche Nutzung von Einrichtungsgegenständen ausschließen. (z.B. Gebäudeschließsysteme und Schrankenanlagen).
- (8) Die dienstliche Kopierernutzung dient zur Vereinfachung der Abrechnungskosten des Geschäftsbedarfs.
- (9) Bei der Durchführung von Hochschulwahlen sollen zeitaufwendige Arbeitsprozesse durch die Einführung eines Automatisierungssystems effizienter gestaltet werden.

§ 3 Begriffsbestimmungen und Systembeschreibung

(1) Es wird grundsätzlich zwischen 3 Datenarten unterschieden:

- Systemdaten: Netzwerksoftware, Betriebssystem, Programmdateien und Protokoll-dateien.
- Berechtigungsdaten: Hochschulnummer, Personalnummer, Gültigkeitsdatum, Bibliotheksnummer, Personen-ID, Personenkennziffer, Kopierkontingent priv. Kopien, Kopierkontingent dienstliche Kopien, Zugangskennziffern, Kartenfolgenummer
- Ereignisdaten: Identifikationsnummer der Chipkarte, orts- und zeitabhängige Daten der Chipkartenbenutzung, Anzahl der Benutzungsversuche.

Sichtbar abgedruckt auf der Karte werden Bild, Titel, Vorname, Name, das Wort Dienstausweis, die Bibliotheksnummer und eine von der OFD-Personalnummer unabhängige laufende Personalnummer aus dem Personalverwaltungssystem.

(2) Der Speicherort, die Art und Weise der Speicherung und die Dauer der Speicherung der Ereignisdaten gemäß der Leistungsbeschreibung des jeweiligen Informationssystems (§ 2) werden in jeder Einzeldienstvereinbarung gesondert geregelt.

Grundsätzlich gilt dabei:

- Die Systeme sind so zu gestalten, dass ein unberechtigter Zugriff auf die Daten durch Dritte ausgeschlossen ist. Ist dies nicht möglich, sind Ereignisdaten verschlüsselt zu speichern.
- Es sind so wenig Daten wie möglich zu speichern.

Ungeachtet dessen sind Ereignisdaten spätestens nach 3 Monaten physikalisch zu löschen, es sei denn, gesetzliche Regelungen oder Dienstvereinbarungen zwischen der Universität und dem Personalrat schreiben andere Fristen vor.

- (3) Die auf der Chipkarte elektronisch gespeicherten Daten sind vor Manipulation zu schützen.

Die Kartenlesegeräte müssen so beschaffen sein, dass Lesevorgänge ausschließlich durch den/die Benutzer/in in Gang gesetzt werden können. Der Lesevorgang muß für den/die Benutzer/in nachvollziehbar sein. Automatische Lese- oder sonstige Erkennungsvorgänge, die eine nicht beabsichtigte Überwachung ermöglichen, sind auszuschließen.

Die Übertragung der erfaßten Daten vom Kartenlesegerät sowie von Eingabedaten des Kartenbenutzers zur jeweiligen Verarbeitungseinheit erfolgt gemäß § 3 Abs. 2 und den abgeschlossenen Einzeldienstvereinbarungen.

- (4) Zwischen den Kartenlesegeräten und einer entfernten Verarbeitungseinheit werden die besonders schützenswerten Daten verschlüsselt übertragen. Die Datensicherheit ist von dem/der Datenschutzbeauftragten oder einer unabhängigen Stelle zu zertifizieren.
- (5) Eine Übergabe von Datenbanken bzw. einzelnen Daten zwischen hochschulinternen und fremden Systemen ist unzulässig. Verknüpfung und Übergabe von Daten unterschiedlicher Zweckbestimmung innerhalb der Universität ist nur mit Zustimmung des Personalrates zulässig.
- (6) Auf die besonderen Bedürfnisse von Schwerbehinderten ist beim Umgang mit der Chipkarte und den vorgesehenen Anwendungen Rücksicht zu nehmen. Sollte durch die Art der Behinderung eine Kartennutzung nicht möglich sein, wird die Universität nach Wegen suchen, um auf andere Weise die Teilnahme an den einzelnen Anwendungen zu gewährleisten. In die notwendigen Überlegungen ist der Personalrat mit einzubeziehen.

§ 4 Autorisierung der Chipkarte gegenüber den CIS

Die Autorisierung gegenüber dem CIS erfolgt ausschließlich über eine im Chip intern gespeicherte, von der Dienststelle vergebene Identifikationsnummer (= OFD-Nummer fremde Personalnummer) der Chipkarte. Die Zuordnung der Chipkarte zum/zur jeweiligen Benutzer/in erfolgt über eine Nummer, die auf die Chipkarte aufgedruckt ist. Die aufgedruckte Personalnummer ist ungleich der Chipkartenummer und steht mit dieser in keinerlei Zusammenhang. Die Autorisierung kann für einzelne Teilsysteme zusätzlich durch eine persönliche Geheimnummer (PIN) ermöglicht werden.

§ 5 Betreiben der Systeme

- (1) Von der Dienststellenleitung werden Systemadministratoren und Stellvertreter/innen benannt. Die Systemadministratoren/innen sind für den laufenden Betrieb der einzelnen Teilsysteme des CIS zuständig.

Datenverändernde Zugriffe der Administratoren auf das CIS sind automatisch zu protokollieren. Sollte dies nicht möglich sein, ist ein handschriftliches Protokoll anzulegen. Die Protokolle sind vor Veränderung zu schützen und mindestens 1 Jahr länger als die im § 3 Abs. 2 genannten Fristen aufzubewahren. Aus den Protokolldaten muß eindeutig hervorgehen, welche Zugriffe auf die Systemdaten, die Zugriffsberechtigungsdaten und die Ereignisdaten von welchen Personen vorgenommen wurden, und welche Aktionen während des Zugriffs in Gang gesetzt wurden.

Die Protokolldateien sind auf Verlangen für den Personalrat einsehbar. Die Darstellung erfolgt in lesbarer, allgemeinverständlicher Form. Dieser Zugriff erfolgt ausschließlich im

4-Augen-Prinzip zusammen mit dem/der Systemadministrator/in. Andere Auswertungen sind unzulässig.

Für die Herstellung des Ausweises wird ein/e Ansprechpartner/in und Stellvertreter/in benannt, die auch im Falle eines Verlustes alle notwendigen internen Schritte durchführen und für die Ausstellung einer neuen Chipkarte verantwortlich sind.

- (2) Personen, die mit Administrationsaufgaben betraut werden, sind aktenkundig zu belehren, dass personenbezogene Daten vertraulich zu behandeln sind, dass jede mißbräuchliche Verwendung der Systeme zu unterlassen ist und daß diese Dienstvereinbarung ihnen zur Kenntnis gebracht wurde.
- (3) In begründeten Ausnahmefällen (Gefahrenabwehr, schwerwiegende Beeinträchtigung der Rechte eines anderen) sind Lesezugriffe auf die Ereignisdaten den ausdrücklich dazu vom Kanzler berechtigten Personen gestattet. Hierbei werden dem/der Beauftragten nur die Ereignisdaten zugänglich gemacht, die die Ausnahmesituation erfordern. Über einen solchen Zugriff ist ein schriftliches Protokoll anzufertigen und dem Personalrat vorzulegen.
- (4) Die Dienststellenleitung hat vor der Inbetriebnahme eines neuen Teilsystems des CIS, einer Erweiterung oder Ergänzung eines Systembestandteils oder Verfahren der Datenübertragung oder Verfahren der Datenverarbeitung eine Analyse der Sicherheit zu erstellen und diese dem Personalrat vorzutragen.

Die Dienststelle ist verpflichtet, ein CIS ganz oder teilweise außer Betrieb zu nehmen, wenn sich herausstellt, dass Datensicherheit und Datenschutz im Sinne dieser Dienstvereinbarung nicht gewährleistet sind.

§ 6 Rechte und Pflichten der Beschäftigten, die am CIS teilnehmen

- (1) Alle Mitarbeiter/innen, die am CIS teilnehmen, werden in umfassender und geeigneter Weise über die Wirkungsweise des gesamten Systems informiert.

Mitarbeiter/innen, die am CIS teilnehmen, erhalten eine schriftliche Mitteilung über alle Datenfelder, die ihre Person betreffen, zu Beginn des Systembetriebes und bei jeder Änderung, die sich durch den Abschluss und Umsetzung einer Einzeldienstvereinbarung ergeben.

Die Teilnahme an jedem der Systeme innerhalb von CIS ist kostenlos.

Die erstmalige Ausgabe der Chipkarte geht zu Lasten der Universität. Neuausstellungen bedingt durch Verlust o. ä. müssen von dem/der Mitarbeiter/in getragen werden.

Jeder/jede Beschäftigte hat das Recht, sich die auf seiner/ihrer Chipkarte gespeicherten Daten und die auf seine Person bezogenen im CIS gespeicherten Daten anzusehen. Die Darstellung erfolgt in einer für den/die Mitarbeiter/in nachvollziehbaren und verständlichen Form.

- (2) Jeder/jede Beschäftigte hat das Recht, andere außerdienstliche Funktionen der Chipkarte zu nutzen oder nicht zu nutzen, ohne dass ihm/ihr dadurch dienstliche Nachteile entstehen. Für die Benutzung dieser Funktionen gelten die Bedingungen der jeweiligen anderen Anbieter.
- (3) Der Verlust der Chipkarte ist unverzüglich dem/der zuständigen Administrator/in der Berechtigungsdaten zu melden. Der/die Administrator/in ist den Beschäftigten in geeig-

* Personalnummer (OFD unabhängig), Bibliotheksnummer, Personen-ID, Personenkennziffer, Zugangskennziffern und Kartenfolgennummer

netter Weise bekannt zu machen. Werden mehrere CIS betrieben, schafft der Arbeitgeber ein zentrales Register über alle Chipkartenanwendungen an der Universität. Dieses ist dem/der Mitarbeiter/in schriftlich gemäß § 6 Abs. 1 mitzuteilen. Die Verlustmeldung des/der Beschäftigten wird von dem/der zentralen Administrator/in automatisch an alle im Register aufgeführten Stellen zum Zwecke der Sperrung der Karte weitergeleitet. Nach Meldung des Kartenverlustes bei dem/der Administrator/in ist der/die Universitätsbedienstete für Schäden, die durch den Missbrauch der Chipkarte entstehen nicht haftbar. Dieser Haftungsausschluss gilt nicht für ein vorsätzliches Handeln.

- (4) Tritt durch technische Manipulationen an dem Chip, die der Universitätsbedienstete nicht zu vertreten hat, ein Schaden ein, muss die Universität diesen tragen.

§ 7 Einhaltung der Dienstvereinbarung

- (1) Über Maßnahmen, die das CIS betreffen und die über den Austausch funktionsgleicher Hard- und Softwarekomponenten hinausgehen, ist der Personalrat nach seinen Beteiligungsrechten rechtzeitig und umfassend durch die Dienststelle zu unterrichten. Rechtzeitig ist die Unterrichtung dann, wenn sie erfolgte, solange noch unterschiedliche Lösungsalternativen im Interesse der betroffenen Mitarbeiter/innen berücksichtigt werden können und noch keine betrieblichen oder technischen Sachzwänge geschaffen wurden.
- (2) Der Personalrat ist berechtigt, jeweils mit bis zu 2 Mitgliedern /Vertretern an den Veranstaltungen teilzunehmen, die anlässlich der Einführung, Veränderungen oder Erweiterungen von CIS durchgeführt werden.
- (3) Die Dienststellenleitung und der Personalrat sind berechtigt zur fachlich-technischen Prüfung der Durchführung dieser Dienstvereinbarung geeignete Experten/innen zu benennen, heranzuziehen und mit Verhandlungsvollmachten auszustatten. Dabei soll zunächst auf Mitarbeiter/innen bzw. Angestellte der Universität zurückgegriffen werden. Erst wenn sich beide Seiten in einem Streitfall nicht einigen können, ist die Benennung unabhängiger Experten/innen zulässig. Die entstandenen Kosten werden von der Dienststelle getragen. Die hinzugezogenen Sachverständigen unterliegen der Geheimhaltungs- bzw. Schweigepflicht oder sie sind zur Verschwiegenheit zu verpflichten.
- (4) Im Rahmen des ihm eingeräumten Rechtes zur Überprüfung erhalten der Personalrat oder die von ihm beauftragten Sachverständigen auf Verlangen Einsicht in alle Unterlagen, Protokolle und sonstigen Aufzeichnungen, die im Zusammenhang mit dem Betrieb des CIS anfallen.

§ 8 Schlußbestimmungen

Diese Dienstvereinbarung tritt am 01.09.2003 in Kraft.

Sie kann von jedem Vertragspartner mit einer Frist von sechs Monaten schriftlich gekündigt werden. Die Dienstvereinbarung behält im Falle der Kündigung weiter Gültigkeit bis zum Abschluß einer neuen Dienstvereinbarung zum CIS, es sei denn, die Vereinbarungen sind inhaltlich gegenstandslos geworden.

In der Erprobungsphase von mindestens 6 Monaten je Teilsystem haben beide Partner das Recht, Änderungsvorschläge für diese Dienstvereinbarung und die Teilvereinbarungen einzubringen. Der/die Datenschutzbeauftragte der Dienststelle wird während der Erprobungsphase in die Beurteilung der Systeme einbezogen.

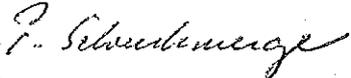
Werden Vorschriften dieser Dienstvereinbarung durch gesetzliche Regelungen ersetzt oder hinfällig, gelten die gesetzlichen Regelungen. Nicht von diesen Regelungen erfaßte Teile dieser Dienstvereinbarung bleiben weiterhin gültig. Diese Dienstvereinbarung ist in angemessener Frist den gesetzlichen Regelungen anzupassen.

Werden Systeme nach §1 dieser Dienstvereinbarung von Fremdfirmen in der Einrichtung betrieben, so sorgt die Dienststelle dafür, dass diese Dienstvereinbarung sinngemäß Anwendung findet, insbesondere die §§ 3, 4 und 6.

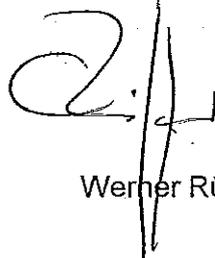
Trier, den 30.7.03

Trier, den 25. Juli 2003

Für die Universität Trier
Der Präsident


Prof. Dr. Peter Schwenkmezger

Für den Personalrat
Der Vorsitzende


Werner Ruffer