Dienstvereinbarung

über die Einführung und Betrieb von Informationssystemen mit Chipkartennutzung

zwischen der

Technischen Universität Ilmenau

und dem

Personalrat der Technischen Universität Ilmenau

Die Technische Universität Ilmenau, vertreten durch den Rektor, und der Personalrat der Technischen Universität Ilmenau, vertreten durch den Vorsitzenden, schließen gemäß § 72 Abs. 1 und § 74 Abs. 3 Nrn. 18, 19 Thüringer Personalvertretungsgesetz (ThürPersVG) vom 29. Juli 1993 die nachstehende Dienstvereinbarung:

Die Informationssysteme (alle optischen, akustischen, mechanischen und elektronischen Geräte einschließlich der Software, die zur Verarbeitung, Verwaltung und Überwachung bestimmt sind), bei denen Teilprozesse mittels Chipkarten ausgelöst werden können, werden im folgenden CIS genannt. Diese Vereinbarung enthält Regelungen für den Betrieb dieser Informationssysteme, die Rechte der Beschäftigten und des Personalrates.

§ 1 Geltungsbereich

Diese Dienstvereinbarung gilt für die Inbetriebnahme und den Betrieb eines CIS sowie späterer Erweiterungen an der TU Ilmenau. Insbesondere fallen unter den Geltungsbereich folgende Anwendungen:

1. Nutzung der Chipkarte als Dienstausweis,
2. Arbeitszeiterfassung für die Mitarbeiter,
3. Bibliotheksnutzung,
4. Zutrittssysteme zu Gebäuden und Räumen,
5. Zugangssysteme via Kommunikationsnetz zu Daten und Dienstleistungen,
6. Parkplatznutzung,
7. Kopierernutzung.

Einzelheiten regeln spezielle Dienstvereinbarungen.

§ 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 Leistungskontrolle 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 sind nicht statthaft.

(3) Außer den im § 1 genannten CIS sollen keine anderen Informationssysteme auf Kartenbasis eingeführt werden.

(4) Die Arbeitszeiterfassung dient dem Ermitteln von An- und Abwesenheitszeiten mit Hilfe von elektronischen Erfassungssystemen.

(5) Die Bibliotheksnutzung kann durch ein Selbstverbuchungssystem erleichtert und der Bargeldverkehr in den Bibliotheken reduziert werden.

(6) Die Zutritts- und Zugangsberechtigung mit Chipkarten dient dem Schutz der Mitarbeiter und des Eigentums der Dienststelle und soll die missbräuchliche Nutzung von Einrichtungsgegenständen ausschließen. (z.B. Gebäudeschließsysteme und Schrankenanlagen).

§ 3 Begriffsbestimmungen und Systembeschreibung

(1) Es wird grundsätzlich zwischen 3 Datenarten unterschieden:

- Systemdaten: Netzwerksoftware, Betriebssystem, Programmdateien und Protokolldateien gemäß der besonderen Zweckbestimmung des § 20 Abs. 4 ThürDSG;
- Berechtigungsdaten: Identifikationsnummer der Chipkarte, bestimmungsgemäße Zuordnung der Berechtigung gemäß § 2, Zuordnung der Identifikationsnummer der Chipkarte zum Benutzer, Angaben zum Chipinhaber;
- Ereignisdaten: Identifikationsnummer der Chipkarte, orts- und zeitabhängige Daten der Chipkartenbenutzung, Anzahl der Benutzungsversuche.

In der Anlage 1 befindet sich die Beschreibung aller erfassten Daten inklusive der eindeutigen Definition der einzelnen Datenfelder der verschiedenen Datensätze, getrennt nach den in § 1 genannten Systemen, soweit sie in der Einführung sind. Werden weitere Teilsysteme eingeführt, so ist Anlage 1 mit Zustimmung des Personalrates vor der Inbetriebnahme zu ergänzen.

(2) Der Speicherort, die Art und Weise der Speicherung und die Dauer der Speicherung der Ereignisdaten gemäß der Leistungsbeschreibung des jeweiligen Informationssystems (§ 2) sind in der Anlage 2 festgelegt, soweit sie in der Einführung sind. Werden weitere Teilsysteme eingeführt, so ist Anlage 2 mit Zustimmung des Personalrates vor der Inbetriebnahme zu ergänzen. Dabei gilt grundsätzlich:

- Mitarbeiterdaten sind in Dateien zu verwalten, die getrennt von Studentendaten sind.
- 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 nach maximal 3 Monaten physikalisch zu löschen, es sei denn, gesetzliche Regelungen oder Dienstvereinbarungen der TU Ilmenau schreiben andere Fristen vor.

(3) Die Chipkarten sind so fälschungssicher wie möglich gestaltet, die auf der Chipkarte elektronisch gespeicherten Daten sind vor Manipulation zu schützen. Wird eine Standardchipkarte verwendet, sind die von der TU Ilmenau aufgebrachten Nutzerdaten ebenfalls in das Sicherungsverfahren einzubeziehen. Der Lesevorgang muss für den Benutzer nachvollziehbar sein. Automatische Lese- oder sonstige Erkennungsvorgänge, die eine nicht beabsichtigte Überwachung ermöglichen, sind ausgeschlossen.
Die Übertragung der erfassten Daten vom Kartenlesegerät sowie von Eingabedaten des Kartenbenutzers zur jeweiligen Verarbeitungseinheit erfolgt gemäß § 3 Abs. 2 zu den in Anlage 2 festgelegten Speicherorten.

(4) Zwischen den Kartenlesegeräten und einer entfernten Verarbeitungseinheit werden die Daten ausschließlich verschlüsselt übertragen. Die Datensicherheit ist vom Datenschutzbeauftragten oder einer unabhängigen Stelle zu zertifizieren. Die für die Übertragung der Daten verwendeten Übertragungswege sind in Anlage 3 aufgeführt.

(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 sind nur mit Zustimmung des Personalrates zulässig. Alle Daten, die übergeben und verknüpft werden dürfen sowie Herkunft und Ziel der Übergabe und die Art ihrer Verknüpfung sind in einer Anlage zu dieser Dienstvereinbarung aufzunehmen.

(6) Hard- und Softwareschnittstellen sind zu benennen und in der Anlage 4 aufzuführen.

§ 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 der Chipkarte. Die Zuordnung der Chipkarte zum jeweiligen Benutzer erfolgt über eine Nummer, die auf die Chipkarte aufgeprägt ist. Die aufgeprägte Nummer ist ungleich der Chipkartennummer und steht mit dieser in keinerlei Zusammenhang. Die Autorisierung kann zusätzlich durch eine persönliche Identifikationsnummer (PIN) ermöglicht werden.

§ 5 Betreiben des Systems

(1) Von der Dienststellenleitung werden Systemadministratoren und Stellvertreter benannt. Die Systemadministratoren sind für den laufenden Betrieb des CIS zuständig. Die Namen der Administratoren sind in der Anlage 5 aufgelistet. Sämtliche 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 und Anlage 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. Andere Auswertungen sind unzulässig.

(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 Beauftragten nur die Ereignisdaten zugänglich gemacht, die die Ausnahmesituation erfordert. 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 und vor der Erneuerung von Chipkartenterminals 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. Der Personalrat kann dies auch verlangen.

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

(1) Alle Mitarbeiter, die am CIS teilnehmen, werden in umfassender und geeigneter Weise über die Wirkungsweise des gesamten Systems informiert.
Nach § 4 ThürDSG kann der Einsatz von CIS nur über die Einwilligung der Betroffenen gerechtfertigt werden. Eine wirksame Einwilligung setzt nach § 4 Abs. 2 ThürDSG die Schriftform voraus.
Mitarbeiter, die am CIS teilnehmen, erhalten eine schriftliche Mitteilung über alle Datenfelder, die ihre Person betreffen, zu Beginn des Systembetriebes und bei jeder Änderung der in Anlage 1 genannten Berechtigungsdaten.
Die Teilnahme an jedem der Systeme innerhalb von CIS ist kostenlos. Die Kostentragungspflicht für Ersatzbeschaffungen im Falle des Verlustes bleibt unberührt.
Jeder Beschäftigte hat das Recht, sich die auf seiner Chipkarte gespeicherten Daten und die auf seine Person bezogenen im CIS gespeicherten Daten bei einer Person, die mit der Administration der Berechtigungsdaten betraut ist, darstellen zu lassen (§ 13 ThürDSG). Die Darstellung erfolgt in einer für den Mitarbeiter nachvollziehbaren und verständlichen Form.

(2) Jeder Beschäftigte hat das Recht, andere außerdienstliche Funktionen der Chipkarte zu nutzen oder nicht zu nutzen, ohne dass ihm dadurch dienstliche Nachteile entstehen. Für die Benutzung dieser Funktionen gelten die Bedingungen der jeweiligen anderen Anbieter.

(3) Personenbezogene Operationen, die im Dialogbetrieb mittels der Chipkarte ausgelöst werden können, bedürfen einer ausdrücklichen Freigabe am Eingabegerät durch den Chipkartenbenutzer. Der Vorgang wird auf dem Display bestätigt. Die Gestaltung der Bildschirmmaske bzw. des Eingabegerätes muss eindeutig erkennen lassen, was und zu welchem Zweck gespeichert wird.

(4) Der Verlust der Chipkarte ist unverzüglich dem zuständigen Administrator der Berechtigungsdaten zu melden. Nur dann ist der Beschäftigte von einer Haftung für Schäden gegenüber Dritten, die mit seiner abhanden gekommenen Chipkarte entstanden sind, befreit. Der Administrator ist den Beschäftigten in geeigneter Weise bekannt zu machen, Werden mehrere CIS betrieben, schafft der Arbeitgeber ein zentrales Register über alle Chipkartenanwendungen an der Universität. Dieses ist dem Mitarbeiter schriftlich gemäß § 6 Abs. 1 mitzuteilen. Die Verlustmeldung des Beschäftigten wird vom zentralen Administrator automatisch an alle im Register aufgeführten Stellen zum Zwecke der Sperrung der Karte weitergeleitet.

(5) Fügt die Dienststelle dem Betroffenen einen Schaden zu, der durch eine nach dieser Dienstvereinbarung, nach dem ThürDSG oder nach einer anderen Vorschrift über den Datenschutz unzulässigen oder unrichtigen Verarbeitung seiner personenbezogenen Daten entsteht, ist sie unabhängig von einem Verschulden zum Ersatz des Schadens verpflichtet. Bei schweren Verletzungen des Persönlichkeitsrechtes ist gemäß § 18 Abs. 2 ThürDSG dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(6) Personelle Maßnahmen, die einen Nachteil für den Mitarbeiter zu Folge haben, weil sie auf Informationen beruhen, die unter Verletzung dieser Dienstvereinbarung gewonnen wurden, sind unwirksam und werden zurückgenommen. Soweit dies rechtlich nicht möglich ist, müssen bestehende negative Folgen beseitigt werden oder falls dies nicht möglich ist, der entstandene Schaden nach § 6 Abs. 5 ersetzt werden.

§ 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 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 zu benennen, heranzuziehen, und mit Verhandlungsvollmachten auszustatten. Dabei soll zunächst auf Mitarbeiter bzw. Angestellte der Universität zurückgegriffen werden. Erst wenn sich beide Seiten in einem Streitfall nicht einigen können, ist die Benennung unabhängiger Experten zulässig. Die entstandenen Kosten werden von der Dienststelle getragen. Die hinzugezogenen Sachverständigen unterliegen der Geheimhaltungs- bzw. Schweigepflicht nach § 10 ThürPersVG i.V.m. § 6 ThürDSG 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 Gleichstellungsklausel

Status- und Funktionsbezeichnungen in dieser Dienstvereinbarung gelten gleichermaßen in der weiblichen und männlichen Form.

§ 9 Schlussbestimmungen

Diese Dienstvereinbarung tritt mit beidseitiger Unterzeichnung in Kraft.
Diese Dienstvereinbarung 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 einzubringen. Der 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.
Die Anlagen dieser Dienstvereinbarung sind Bestandteil der Dienstvereinbarung. Sie werden fortlaufend aktualisiert und können ohne Kündigung dieser Dienstvereinbarung einvernehmlich geändert werden.
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.

Ilmenau, den 19.07.2000	Ilmenau, den 19.07.2000
Gez. Prof. Kern	gez. Dr. Hanella
Rektor	Personalrat

Anlagen, gesondert für jede Anwendung

Anwendung: **Arbeitszeiterfassung für die Mitarbeiter / Dienstvereinbarung über die gleitende Arbeitszeit**