Dienstvereinbarung
über die Einführung eines elektronischen Schließsystems
an der Universität Trier

Zwischen der Universität Trier,

vertreten durch den Präsidenten, Herrn Univ.-Prof. Dr. Peter Schwenkmezger,

und

dem Personalrat der Universität Trier

vertreten durch den Vorsitzenden, Herrn Werner Rüffer,

wird gemäß § 76 Abs. 1 in Verbindung mit § 80 Abs. 2, Nr. 5 Landespersonal-vertretungsgesetz (LPersVG) folgende Dienstvereinbarung geschlossen:

§ 1 – Zweckbestimmung und Geltungsbereich

(1) In den Gebäuden der Universität am Campus I ist eine Schließanlage im Einsatz, die im Jahre 1977 beschafft wurde und auf Grund ihres Alters sicherheitstechnisch nicht mehr den heutigen Anforderungen entspricht. Schlüsselverluste haben darüber hinaus erheblich dazu beigetragen, dass sich das Gefahrenpotential durch Diebstähle wesentlich erhöht hat.

Um die Sicherheit von Mitarbeiterinnen und Mitarbeitern sowie der in den Räumen untergebrachten Geräte und Einrichtungsgegenstände zu erhöhen, wird die Universität in den kommenden Jahren in allen Gebäuden (Campus I und II) zwei elektronische Schließsysteme (ISGUS und Simons & Voss) installieren. Der Einsatz dieser elektronischen Schließsysteme trägt ebenfalls dazu bei, dass die Schlüsselverwaltung besser organisiert werden kann und Schlüsselverluste die Gesamtsicherheit des Schließsystems nicht beeinträchtigen. Darüber hinaus reduzieren sich bei einem Schlüsselverlust mögliche Schadenersatzansprüche gegenüber den Bediensteten nur auf den Ersatz des Zugangsmediums, weil ein Austausch der Schließzylinder nicht mehr notwendig wird.

(2) Alle Personen, die das Schließsystem über ein Medium nutzen, werden in geeigneter Weise über die Wirkungsweise des Systems informiert.

(3) Diese Dienstvereinbarung gilt für den Verantwortungsbereich der Universität Trier.

§ 2 – Arten der Schließsysteme

(1) Im Bereich der Universität gibt es den Nutzerkreis der Studierenden, den Nutzerkreis der Bediensteten und den Nutzerkreis von nicht universitätsangehörigen Personen (Gäste, Zulieferer, Handwerker), die über ein Zutrittsmedium für die Gebäude und/oder den Innenbereich verfügen sollen. Um diesem Personenkreis einen Zugang zu ermöglichen, ist vorgesehen, für die Öffnung und Schließung von 14 Außentüren und der Parkschranken das ISGUS-Schließsystem einzubauen, das mit der Universitätskarte Tunika bedient werden kann. Das System basiert auf der Nutzung des kontaktlosen Mifare-Chips in der Chipkarte, die in Kürze flächendeckend ausgegeben sein wird. Die Nutzung des kontaktbehafteten Chips für den Betrieb der Schließsysteme wird ausgeschlossen.

(2) Daneben ist für Außentüren und für Büro- und Technikräume der Einbau eines Schließsystems der Fa. Simons & Voss vorgesehen (siehe Anlage), dass mit Transpondern bedient wird.

§ 3 – Nutzung und Funktionalität des ISGUS-Schließsystems

(1) Das ISGUS-Schließsystem wird in die in Anlage 1 aufgelisteten Außentüren/Zu-gänge eingebaut und mit einer Datenbank vernetzt.

(2) Um das Schließsystem mit der Universitätskarte Tunika betreiben zu können, werden – ebenso wie bei dem bisherigen Schließsystem auch – in einer Datenbank die folgenden personenbezogenen Daten gespeichert:

a) Kartennummer (bei den Bediensteten handelt es sich um eine interne, vom SVA vergebene Personalnummer zuzüglich einer Kartenfolgennummer) – Feldlänge: 8-stellig
b) Nummer des Ausweises – Feldlänge: 8-stellig
c) Name – Feldlänge: maximal 25-stellig
d) Vorname – Feldlänge: maximal 15-stellig
e) Personen-Gruppe (Mitarbeiter/in Universität, Azubis, Mitarbeiter/in Studentenwerk, Theologische Fakultät oder kooperierende Einrichtung, Fremdfirmen) – Feldlänge: maximal 4-stellig
f) Zutrittsgruppe – Feldlänge: maximal 4-stellig
g) gültig ab – Feldlänge: 10-stellig (tt.mm.jjjj)
h) gültig bis – Feldlänge: 10-stellig (tt.mm.jjjj)

(3) Die Personalisierung der Universitätskarte Tunika erfolgt derzeit durch eine EDV-Anlage in der Universität. Dabei wird in dem Mifare-Chip ein besonderer Sektor für den Zugang zu Gebäuden angelegt. In diesem Sektor werden lediglich die frei lesbare Kartennummer und die für die Türöffnung notwendige fünfstellige PIN in verschlüsselter Form abgelegt. Zum Öffnen der Tür muss die Chipkarte in den Empfangsbereich des Lesegerätes gehalten werden. Nach einem Bestätigungston muss der Kartenbesitzer die PIN eingeben. Dabei wird die eingegebene PIN mit der auf der Karte abgelegten PIN verglichen und bei gleicher Zahlenkombination die Tür zum Öffnen frei geschaltet.

§ 4 – Nutzung und Funktionalität des Simons & Voss-Schließsystems

(1) Das Simons & Voss-Schließsystems wird vernetzt in alle Außentüren eingebaut und unvernetzt in Büro- und Technikräume. Die elektronischen Schließzylinder für Innentüren haben grundsätzlich keine Speichermöglichkeit und werden auch nicht mit Datenbanken verbunden. In begründeten Ausnahmefällen können mit Zustimmung des Personalrats jedoch speicherfähige Schließzylinder zum Einsatz kommen. Derzeit ist dies nur für die in Anlage 2 genannten Räume vorgesehen.

(2) Haupteingangstüren sind mit motorbetriebenen Türschlössern ausgestattet, die zeitlich zentral gesteuert werden. Öffnungs- und Schließzeiten dieser Haupteingangstüren können wechselnden Erfordernissen angepasst und müssen nicht mehr manuell durch die Hausverwaltung verschlossen oder geöffnet werden. Auch können alle Außentüren auf ihren Verschlusszustand hin geprüft werden. Außer den Haupteingangstüren sind alle anderen Außentüren der Universität dauerhaft für den Zutritt von außen verschlossen. Ein Öffnen der Tür von innen ist jedoch in allen Fällen möglich.

§ 5 – Zugriff, Speicherung und Löschung von Eintragungen in den Datenbanken

(1) Beide Datenbanksysteme (ISGUS und Simons & Voss) werden auf einem Server der Technischen Abteilung installiert und von dort betrieben. Die für den Betrieb der Datenbanken notwendigen Datensätze werden über eine Schnittstelle von der noch anzulegenden Benutzerdatenbank importiert. Ein Datenexport von den Schließsystemdatenbanken zur Benutzerdatenbank oder zu anderen Datenbanken ist unzulässig.

(2) Um unberechtigte Zugriffe auf die Schließsystemdatenbanken auszuschließen, ist eine dreifache Absicherung nach außen vorzunehmen. Die erste und zweite Absicherung hat über ein VLAN und eine Firewall mit der Eintragung der Zugriffsberechtigten IP-Adressen zu erfolgen. Die dritte Sicherheitsstufe ist mit einer User-Passwort-Zugangsberechtigung zu den Datenbanken zu regeln.

(3) Jeder Öffnungsvorgang wird bei vernetzten und verschlossenen Türen in den zentralen Datenbanken gespeichert. Ist das Universitätsnetz aus technischen Gründen kurzzeitig nicht verfügbar, erfolgt bis zur Netzverfügbarkeit eine Speicherung der Daten in einem Puffer des Schließsystems. Bei erneuter Verfügbarkeit der Datenbank werden die Ereignisdaten ergänzt. Bei unvernetzten Türen erfolgt eine Speicherung nur in den in Anlage 2 aufgelisteten speicherfähigen Zylindern. Bauartbedingt können in den Zylindern derzeit 127 Schließvorgänge aufgezeichnet werden.

(4) Datensätze von z. B. exmatrikulierten Studierenden und ausgeschiedenen Bediensteten sind in den Datenbanksystemen nach spätestens 6 Monaten zu löschen. Alle in den Datenbanken hinterlegten Ereignisdaten werden spätestens nach 2 Monaten gelöscht.

§ 6 – Datenadministration, Auswertung von Daten

(1) Die für die Administration der Daten zuständigen Universitätsbediensteten sind dem Personalrat bekannt zu geben. Diesen Personen sind aktenkundig zu belehren, dass personenbezogene Daten vertraulich zu behandeln sind, jede missbräuchliche Verwendung des Systems zu unterlassen ist und sie diese Dienstvereinbarung zur Kenntnis genommen haben.

Die Schließsysteme werden für alle Büroräume von der Abteilung I, Sachgebiet Liegenschaften, und für die Technischen Räume von der Technischen Abteilung verwaltet. Zu der Verwaltung des Schließsystems in den Büroräumen durch die Abteilung I gehört insbesondere die Erstellung, Pflege und Aktualisierung der Schließpläne bzw. der Schließplandatenbank, die Programmierung, Ausgabe und die Rücknahme der Transponder, die Programmierung der elektronischen Schließzylinder nach der Erstinstallation sowie der Austausch der Batterien in den elektronischen Schließzylindern. Die gleichen Aufgaben werden von der Abteilung IV alleinverantwortlich für die noch festzulegenden technischen Räume der Technischen Abteilung wahrgenommen.

Darüber hinaus gehört zu den Aufgaben der Technischen Abteilung die Erstinstallation und die Sicherstellung der Funktionsfähigkeit aller elektronischen Schließsysteme einschließlich der Schließzylinderprogrammierung sowie die Einrichtung und Betreuung des gesamten Netzwerkbetriebes für die Steuerung der Haupteingangstüren und für die Außentürüberwachung.

Für Planung, Erstinstallation und den technischen Betrieb des elektronischen Schließsystems sowie für die Programmierung der Berechtigungen zu Technikräumen und den Austausch der Batterien in den Schließzylindern ist die Abteilung IV zuständig.

(2) In begründeten Ausnahmefällen dürfen Lesezugriffe auf die durch die Schließung und Öffnung aufgezeichneten Daten sowie deren Auswertung nur mit Zustimmung des Personalrates und in Anwesenheit eines Beauftragten des Personalrats sowie des Datenschutzbeauftragten erfolgen. Der Zugriff und die Auswertung sind schriftlich zu dokumentieren.

§ 7 – Technische Veränderung der Schließanlagen

Technische Veränderungen der Anlagen und Systeme in einen anderen Zustand als in dieser Vereinbarung beschrieben, bedürfen der vorherigen Zustimmung des Personalrats. Wenn notwendig, ist diese Dienstvereinbarung entsprechend zu ändern.

§ 8 – Geltungsdauer, Änderungen

Die Dienstvereinbarung gilt ab dem Tag der Unterzeichnung. Alle Änderungen bedürfen der Schriftform.

Trier, den 22.12.2004	Trier, den 17.12.2004
Univ.-Prof. Dr. Peter Schwenkmezger	Werner Rüffer