

**Dienstvereinbarung  
über die Einführung und Nutzung elektronischer Schließsysteme  
an der Universität Koblenz-Landau**

**§ 1 – Zweckbestimmung und Geltungsbereich**

- (1) In den Gebäuden der Universität an den Campi in Koblenz und Landau ist eine Schließanlage im Einsatz, die 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.
- (2) Um die Sicherheit von Mitarbeiterinnen und Mitarbeitern sowie der in den Räumen untergebrachten Geräte und Einrichtungsgegenstände zu erhöhen, wird die Universität in Gebäuden und Einrichtungen an den Campi in Koblenz und Landau elektronische Schließsysteme installieren. Der Einsatz dieser elektronischen Schließsysteme trägt 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.
- (3) Elektronische Schließsysteme dienen ausschließlich folgenden Zwecken: Prüfung der Zugangsberechtigung, Evakuierung der Gebäude im Notfall, Überprüfungs-möglichkeiten im Mißbrauchsfall.
- (4) Alle Personen, die das Schließsystem über ein Medium nutzen, werden in geeigneter Weise über die Systeme und deren Nutzungsbedingungen informiert.
- (5) Diese Dienstvereinbarung gilt für den Verantwortungsbereich der Universität Koblenz-Landau an den Campi in Koblenz und Landau. Es wird durch geeignete Maßnahmen der Dienststelle sichergestellt, daß die Einhaltung der Regelungen dieser Dienstvereinbarung auch für Externe gewährleistet ist.
- (6) An den Campi Koblenz und Landau kommen unterschiedliche Schließsysteme zum Einsatz, deren Schließzylinder je nach Zugangsbereich für den Online- bzw. Offline-Betrieb ausgestattet sind. Die Unterlagen über die eingesetzten Systeme sowie die Ausstattung der einzelnen Zugänge an den Standorten liegen den örtlichen Personalräten sowie dem Gesamtpersonalrat vor.
- (7) Durch diese Dienstvereinbarung bestimmt der Gesamtpersonalrat bei der Einführung und Nutzung elektronischer Schließsysteme gemäß § 80 Abs. 2 Nr. 1-4 LPersVG mit.

**§ 2 – Speicherung, Auswertung und Löschung der Daten**

- (1) Die elektronischen Schließsysteme werden in Türen und Einrichtungen der Universität eingebaut und können im Online-Betrieb mit einer Datenbank vernetzt werden. Die Klassifikation der Räume ist in Anlage 1 wiedergegeben.
- (2) Die elektronischen Schließsysteme und die für ihren Betrieb verwendeten Datenbanken werden durch arbeitsorganisatorische, technische und räumliche Maßnahmen gegen eine unbefugte Benutzung gesichert. Die jeweiligen Maßnahmen werden in einem Datenschutzkonzept gemäß § 9 LDSG Rheinland-Pfalz beschrieben.
- (3) Zur Nutzung der elektronischen Schließanlagen werden maximal folgende Daten auf dem Medium (Transponder) gespeichert: Berechtigung, Berechtigungsgruppen, Identifikationsnummer, Zeitzone, Ablaufdatum.

- (4) In den Datenbanken werden maximal folgende Stammdaten gespeichert: Name, Vorname, Berechtigung, Berechtigungsgruppen, Identifikationsnummer, Zeitzone, Ablaufdatum, Organisationseinheit. Zusätzlich zu den Stammdaten werden als Ereignisdaten maximal folgende Daten gespeichert: Name, Vorname, Identifikationsnummer, Datum, Uhrzeit, Ereigniscode. Ein Datenexport zu anderen Datenbanken ist unzulässig.
- (5) In den Schließzylindern werden maximal folgende Ereignisdaten gespeichert: Identifikationsnummer, Datum, Uhrzeit, Ereigniscode. Zusätzlich können maximal die für den jeweiligen Schließzylinder gültigen Berechtigungen gespeichert werden:
- (6) Die Speicherung weiterer Daten ist unzulässig. Änderungen bedürfen der vorherigen Zustimmung des Gesamtpersonalrats.
- (7) Ereignisdaten aus den Schließzylindern werden nicht an die Datenbanken übertragen, sondern ausschließlich in Mißbrauchsfällen.
- (8) Auswertungen der Ereignisdaten und/oder deren Verknüpfung mit anderen Daten der betreffenden Personen sind unzulässig. Insbesondere werden die fehlgeschlagenen Zugangsversuche nicht ausgewertet und keine Bewegungsprofile erstellt. Eine Verwendung der Daten zum Zweck einer Leistungs- und Verhaltenskontrolle ist ausgeschlossen.
- (9) Auswertungen sind nur bei einem im Einzelfall zu plausibilisierenden Missbrauchsverdacht zulässig. In diesen begründeten Ausnahmefällen dürfen Lesezugriffe auf die Ereignisdaten nur im Einvernehmen zwischen Kanzler/in und Gesamtpersonalrat erfolgen. Auswertungen sind nur in Gegenwart je eines/r Beauftragten des Kanzlers/der Kanzlerin und des Gesamtpersonalrats sowie des Datenschutzbeauftragten zulässig. Hierzu wird ein aus zwei Berechtigungen bestehender Schutz aktiviert. Eine Berechtigung verbleibt bei der Hausverwaltung, die zweite Berechtigung erhält der Gesamtpersonalrat. Der Zugriff und die Auswertung sind schriftlich zu dokumentieren. Bei Gefahr im Verzug handelt die Universitätsverwaltung unmittelbar. In diesen Fällen sind der Gesamtpersonalrat sowie der Datenschutzbeauftragte unverzüglich, spätestens jedoch nach einer Woche, über die durchgeführten Maßnahmen und deren Ergebnisse zu unterrichten. Die betroffenen Personen, deren Daten aufgrund eines Missbrauchsverdachts ausgewertet wurden, sind, sobald dies einer Beweissicherung nicht mehr entgegensteht, unverzüglich über diesen Sachverhalt sowie Ergebnisse zu unterrichten.

### **§ 3 – Systemadministration, Systemanwender und Datenschutz**

- (1) Es wird sichergestellt, dass nur Personen mit entsprechender Aufgabenübertragung Administrations- bzw. Anwenderzugang erhalten. Sie sind entsprechend der Bestimmungen der Datenschutzgesetze auf den Umgang mit geschützten Daten zu verpflichten und vor der erstmaligen Nutzung umfassend zu qualifizieren.
- (2) Die Aufgaben der Systemadministration umfassen insbesondere die technische Systembetreuung oberhalb der Anwendungsebene, die auch extern sichergestellt werden kann.
- (3) Die Schließsysteme werden für alle Einrichtungen von den Systemanwendern betreut. Zur Betreuung der Schließsysteme 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 die Wartung der elektronischen Schließzylindern.
- (4) Darüber hinaus gehört zu den Aufgaben der mit der Verwaltung der Schließsysteme Beschäftigten die Sicherstellung der Funktionsfähigkeit des elektronischen Schließsystems einschließlich der Schließzylinderprogrammierung.

- (5) Werden personenbezogene oder personenbeziehbare Daten erhoben, gespeichert, übermittelt oder weiterverarbeitet, die aufgrund dieser Dienstvereinbarung unzulässig sind, so unterliegen sie einem Verwertungsverbot.

#### **§ 4 - Rechte des Gesamtpersonalrats**

- (1) Der Gesamtpersonalrat erhält Einsicht in alle der Dienststelle vorliegenden Unterlagen über den Einsatz und die Nutzung der Anlagen und Geräte zu den Schließsystemen. Er ist darüber hinaus berechtigt, ergänzende Auskünfte zu verlangen und die mit der Durchführung dieser Dienstvereinbarung zusammenhängenden Verfahrensschritte und -abläufe zu überprüfen.
- (2) Der Gesamtpersonalrat kann an allen Anwenderschulungen teilnehmen.
- (3) Der Gesamtpersonalrat erhält am Produktivsystem Einsicht in alle verfügbaren Systemprotokolle und Daten, sofern datenschutzrechtliche Belange dem nicht entgegenstehen.

#### **§ 5 – Schlußbestimmungen**

- (1) Die Dienstvereinbarung tritt mit dem Tag der Unterzeichnung in Kraft. Alle Änderungen bedürfen der Schriftform.
- (2) Die Kündigungsfrist beträgt 6 Monate zum Jahresende, erstmals zum 31.12.2012. Im Falle der Kündigung dieser Dienstvereinbarung findet die Nachgeltung gem. § 76 Abs. 3 LPersVG für die gesamte Dienstvereinbarung Anwendung.
- (3) Im Falle einer Kündigung der Dienstvereinbarung verpflichten sich die Vertragsparteien, unverzüglich über eine neue Dienstvereinbarung in Verhandlungen zu treten mit dem Ziel, innerhalb einer Frist von sechs Monaten eine neue Vereinbarung abzuschließen.
- (4) Gesamtpersonalrat und Dienststelle werten 6 Monate nach Implementierung und Inbetriebnahme der elektronischen Schließsysteme (aus KII-Programm finanziert) gemeinsam die Erfahrungen mit den Regelungen dieser Dienstvereinbarung aus, vor allem im Hinblick auf die mit der Umstellung auf elektronische Schließsysteme und deren Betrieb verbundene zeitliche Inanspruchnahme der dafür verantwortlichen Beschäftigten und deren Veränderung gegenüber dem vorherigen Schließsystem. Ziel dieser Auswertungen ist die Feststellung, ob und inwieweit ein Handlungsbedarf in bezug auf die erforderlichen personellen Kapazitäten bzw. deren Veränderung (Quantität und Qualität) vorliegt. Für diese Bewertung werden aktualisierte Stellenbeschreibungen sowie die Prozeßbeschreibungen des alten und des neuen Systems zugrunde gelegt.
- (5) Sollten einzelne Bestimmungen dieser Dienstvereinbarung unwirksam sein oder werden oder im Widerspruch zu tariflichen oder gesetzlichen Regelungen stehen, so bleiben die übrigen Bestimmungen bestehen.

Mainz, den 04.05.2011

gez. Simone Mertel-Scherer  
i. V. für Präsidenten

Landau, den 19.05.2011

gez. Bernd Wunder  
Gesamtpersonalratsvorsitzender

#### Anlagen

Anlage 1: Klassifikation der Räume für die Ausstattung mit der elektronischen Schließanlage

**Anlage 1: Klassifikation der Räume für die Ausstattung mit der elektronischen Schließanlage**

Die mit elektronischen Schließsystemen auszustattenden Räume und Einrichtungen sind in folgender Weise klassifiziert:

- Räume mit hohen Anforderungen (z.B. Forschungslabore, Lager von Gefahrstoffen, Außentüren, Lehrveranstaltungsräume, Besprechungsräume mit Medientechnik, Technikräume, Serverräume, sonstige schutzwürdige Räume)
- Räume mit normalen Anforderungen (z.B. Büros, Sammlungsräume)
- Räume ohne Anforderungen (z.B. Besprechungsräume ohne Medientechnik, Teeküchen, Toiletten oder sonstige Räume, die für jedermann zugänglich sein sollten).