Dienstvereinbarung

zwischen der Technischen Universität Bergakademie Freiberg

vertreten durch den Kanzler

und

dem Personalrat der Technischen Universität Bergakademie Freiberg

vertreten durch den Vorsitzenden

über die Nutzung des Elektronischen Schließ- und Zugangskontrollsystems (SIPORT)

§ 1
Gegenstand

(1) Diese Dienstvereinbarung regelt die Verwendung des Elektronischen Schließ- und Zugangskontrollsystems SIPORT (nachfolgend als SIPORT bezeichnet) in den Einrichtungen der TU Bergakademie Freiberg. Ziel dieser Vereinbarung ist es, beim Einsatz von SIPORT den Schutz personenbezogener Daten vor unzulässigem Gebrauch zu gewährleisten und den berechtigten Zugriff zu regeln. Der Einsatz von SIPORT dient der Sicherheit von Personen, Daten und Sachwerten in den Einrichtungen der TU Bergakademie Freiberg und der Umsetzung des in der Schließordnung der TU Bergakademie Freiberg geregelten Schlüsselberechtigungssystems.

(2) Zur Steuerung des elektronischen Schließ- und Zutrittskontrollsystems wird der kontaktlose Chip der Universitätschipkarte entsprechend der Dienstvereinbarung vom 23./26.05.2003 genutzt. Die Pflichten der Nutzer und die Verwaltung der Schlüsselfunktion ergibt sich aus der Schließordnung der TU Bergakademie Freiberg.

§ 2
Geltungsbereich

(1) Die Dienstvereinbarung gilt für alle Beschäftigten und sonstigen Nutzer, die die Universitätschipkarte als Schließ- und Zutrittsfunktion in SIPORT verwenden.

(2) Der räumliche Geltungsbereich erstreckt sich auf alle Einrichtungen der TU Bergakademie Freiberg.

§ 3
Datenverarbeitung

(1) Nachfolgende Daten werden in SIPORT erfasst:

- Ausweisnummer
- Chipkartenseriennummer
- Personalnummer
- Nachname
- Vorname
- Gültigkeitsdauer des Ausweises
- Betreuercode

(2) Die in Abs. 1 genannten Daten werden in einer Stammdatei in SIPORT (elektronischer Schlüsselplan) hinterlegt.

(3) Im SIPORT werden automatisiert Logbücher erstellt. In diesen werden bestimmte Ereignisse durch das System registriert, protokolliert und gespeichert. Solche Ereignisse sind z. B. Ausweisbuchungen, Alarme, systemsteuernde Aktivitäten. Es werden folgende Logbücher, die personenbezogene Daten enthalten, genutzt:

- Alarmlogbuch: Registrierung der Alarmmeldungen, welche durch Störungen bei der Nutzung ausgelöst werden.
- Zutrittslogbuch: Registrierung der berechtigten Zutritte zu Räumen durch die Nutzer. Das Zutrittslogbuch dient der Fehlerbehebung bei Zutrittsproblemen, die nicht im Alarmlogbuch angezeigt werden.
- Siportlogbuch: Protokollierung der Handlungen der berechtigten Nutzer im Siportsystem.

(4) Zur Datensicherung werden in Verantwortung der berechtigten Administratoren tägliche Abbilder der SIPORT-Datenbank gemacht und diese auf einem Server im Universitätsrechenzentrum der TU Bergakademie Freiberg gespeichert.

§ 4
Schutz der Persönlichkeitsrechte

(1) Es besteht Einvernehmen darüber, dass das Elektronische Schließ- und Zutrittskontrollsystem nicht zum Zweck der Leistungs- und Verhaltenskontrolle der Mitarbeiter eingesetzt wird.

(2) Der Anwendung von SIPORT liegt ein dezidiertes Berechtigungskonzept zugrunde, welches sicherstellt, dass die in SIPORT hinterlegten Daten und Vorgänge nur von wenigen besonders autorisierten Mitarbeitern eingesehen und ggf. bearbeitet werden können. Das Berechtigungskonzept wird durch den Dezernenten des Dezernates Bau- und Gebäudemanagement außerhalb von SIPORT dokumentiert und dem Personalrat schriftlich angezeigt. Das Berechtigungskonzept beruht auf folgenden Grundlagen:

- Der Zugang zur Software und den Daten ist passwortgeschützt.
- Administratoren haben passwortgeschützten Zugang zu SIPORT. Diese haben vollumfänglich Zugang zu Daten und Vorgängen und Bearbeitungsrechte.
- Nutzerrechte können in eng begrenzten Fällen an Mitarbeiter oder Dritte vergeben werden. Derartige eng begrenzte Fälle sind insbesondere die Verwaltung der Stammdaten, die Einarbeitung in SIPORT zur Vorbereitung auf die Einräumung von Administratorrechten sowie die Fehlerbehebung, Wartung und Entwicklung von SIPORT. Nutzerrechte verleihen lediglich passwortgeschützte eingeschränkte Zugriffsrechte. Die Zugriffsrechte werden entsprechend des Zwecks der Nutzungsrechteeinräumung für ein oder mehrere Module vergeben. Jeder Nutzer kann nur die Daten und Vorgänge innerhalb seines Nutzbereiches einsehen und bearbeiten.
- Die Administratoren und Nutzer werden über den Datenschutz belehrt. Die Belehrung wird dokumentiert.

(3) Die Einsichtnahme in die in SIPORT gespeicherten Daten und Vorgänge sowie die entsprechende Protokollierung zu anderen als dem in § 1 benannten Zweck ist nur bei hinreichendem Verdacht auf Missbrauch der Zugangsberechtigung, sonstige schwerwiegende dienstrechtliche Verstöße oder strafbare Handlungen zulässig. Die Einsichtnahme darf nur durch den Rektor, den Kanzler oder eine von diesen namentlich benannte Person in Anwesenheit eines Mitgliedes des Personalrates durchgeführt werden, welche sich zur Einsichtnahme eines Administrators bedienen. Der Personalrat ist vor Einsichtnahme in die Daten und Vorgänge von Mitarbeitern anzuhören. Hiervon kann abgesehen werden, wenn unverzüglicher Handlungsbedarf besteht. In einem solchen Fall ist der Personalrat anschließend unverzüglich und umfassend über die Maßnahme zu informieren. Ihm sind der betroffene Mitarbeiter und der Anlass für die Einsichtnahme mitzuteilen. Der Personalrat wird die beabsichtigte Einsichtnahme, Protokollierung und anschließende Auswertung der erlangten Daten durch die Dienststelle vertraulich behandeln.

(4) Der elektronische Schlüsselplan und die Logbücher sind grundsätzlich durch geeignete technische Maßnahmen vor dem Zugriff durch andere Programme oder Systeme zu schützen.

(5) Die in den Logbüchern gespeicherten Daten werden automatisiert nach einer Dauer von 60 Tagen in SIPORT gelöscht. Die Aktualisierung der Stammdatendatei erfolgt in regelmäßigen Abständen - mindestens alle zwei Monate - durch das Dezernat Bau- und Gebäudemanagement. Nicht mehr erforderliche Stammdaten werden dabei gelöscht.

§ 5
Inkrafttreten

(1) Diese Dienstvereinbarung ergänzt die Dienstvereinbarung zur Nutzung einer multifunktionalen Universitätschipkarte als Mitarbeiterausweis vom 23./26.05.2003. Sie tritt mit der Unterzeichnung durch beide Seiten in Kraft.

(2) Die Dienstvereinbarung kann mit einer Frist von drei Monaten durch beide Seiten gekündigt werden.

(3) Im Falle der Kündigung gelten die Regelungen dieser Dienstvereinbarung bis zum Abschluss einer neuen Dienstvereinbarung fort.

Freiberg, 30.06.2014

gez. Dr. Handschuh
Kanzler

Freiberg, 25.06.2014

gez. Dr. Wagner
Personalratsvorsitzender