Dienstvereinbarung

Einführung und Betrieb elektronischer Zugangskontrollsysteme für Räume der Fachhochschule Erfurt

Für den Zugang zu Räumen und Geräten werden elektronische Zugangskontrollsysteme eingeführt. Mit ihnen lassen sich Berechtigung kostengünstig und effektiv verwalten. Herkömmliche Schließsystem werden abgelöst. Risiken und Kosten durch Schlüsselverluste lassen sich dadurch minimieren.

§ 1 Gegenstand und Geltungsbereich

Diese Dienstvereinbarung regelt die Anwendung der elektronischen Zugangskontrollsysteme in den Gebäuden der Fachhochschule Erfurt. Sie gilt für alle vom Personalrat vertretenen Beschäftigten der FH Erfurt.

Die Dienstvereinbarung findet analoge Anwendung als Nutzerordnung für alle sonstigen Personen, die zugangskontrollierte Räume nutzen, auch wenn sie nicht Angehörige der FH Erfurt sind.

§ 2 Zweckbestimmung

Die elektronischen Zugangskontrollsysteme werden eingesetzt um

- Zugangsberechtigungen effizienter und wirtschaftlicher zu verwalten,
- den Zutritt zu Gebäuden, Bereichen und Räumen zeitlich begrenzt auf berechtigte Personen einzuschränken,
- Unbefugten den Zutritt zu Gebäuden, Bereichen und Räumen zu verwehren, um die darin befindlichen Werte vor Diebstahl, Zerstörung und Manipulation zu schützen.

§ 3 Systemdokumentation

Es werden verschiedene Arten von Zutritts-/ Zugangssystemen eingesetzt.
Die Dokumentation befindet sich in Anlage 1.

§ 4 Erhebung, Verarbeitung und Nutzung von Daten

Es werden ausschließlich die Zugangsdaten und die in der Anlage 1 aufgeführten Nutzerdaten erfasst.

Zugriff auf die Systeme und die darin gespeicherten Daten haben nur die in der Anlage 2 aufgeführten Personen als Verwalter der Zugangskontrollsysteme.

Die Systeme und die darin gespeicherten Daten sind vor unbefugtem Zugriff und Missbrauch zu schützen.

Eine Auswertung der Daten zur Erstellung von Bewegungs- und Anwesenheitsprofilen ist unzulässig. Eine Leistungs- und Verhaltenskontrolle der Beschäftigten findet nicht statt.

Eine Auswertung der gespeicherten Daten erfolgt nur bei

- einem ausdrücklich begründeten Missbrauchsverdacht
- sicherheitsrelevanten Ereignissen (z. B. Diebstahl).

Das Ereignis darf nicht länger als 3 Werktage zurück liegen. In solchen Fällen ist ein Antrag (entsprechend Anlage 5 des Leitfadens) zu stellen. und zeitweise zur Verwaltung der Zugangsberechtigten ist eine Vernetzung der Zugangskontrollsysteme zulässig. Eine Auswertung erfolgt nur nach vorheriger Genehmigung durch den Dienststellenleiter und den Personalrat.

im Beisein von Vertreterinnen oder Vertretern von D 4, der Systemverwaltung und des Personalrats.

Alle Zugangsdaten einschließlich etwaiger Kopien werden maximal sechs Monate gespeichert und dann gelöscht, soweit sie nicht zur Aufklärung/ Beweissicherung von konkreten Vorkommnissen weiterhin benötigt werden (z. B. bis zum Abschluss eines gerichtlichen Verfahrens). Sofern Daten länger als sechs Monate gespeichert werden müssen, sind die Personalvertretung und der Datenschutzbeauftragte zu informieren.

§ 5 Rechte der Beschäftigten

Jede/r zutrittsberechtigte Beschäftigte kann einen Transponder kostenfrei erhalten. Transponder können gleichzeitig für die Zeiterfassung und als elektronische Schlüssel genutzt werden.

Die Beschäftigten sind verpflichtet, mit den Transpondern sorgfältig umzugehen, sie vor Verlust und Beschädigung zu schützen und diese nicht weiterzugeben.

Der Verlust eines Transponders ist unverzüglich anzuzeigen, damit eine Sperrung veranlasst werden kann.

§ 6 Rechte des Personalrates

Der Personalrat hat das Recht, die Einhaltung dieser Dienstvereinbarung zu überprüfen. Hierzu erhält er auf Verlangen Einsicht in alle mit dem Betrieb der Systeme zusammenhängenden Unterlagen, Protokolle und sonstigen Aufzeichnungen.

Der Personalrat kann vor Ort nach vorheriger Information der Dienststelle Besichtigungen vornehmen.

Zur Überprüfung der Arbeitsweise der Systeme hat der Personalrat das Recht, Sachverständige hinzu zu ziehen.

§ 7 Bekanntmachung der Dienstvereinbarung

Alle Verwalter (Anlage 2) werden aktenkundig über die Einhaltung dieser Dienstvereinbarung belehrt.

Diese Dienstvereinbarung ist allen betroffenen Beschäftigten bekannt zu geben.

§ 8 Inkrafttreten und Geltungsdauer

Diese Dienstvereinbarung tritt am Tag nach ihrer Unterzeichnung in Kraft. Sollten eine oder mehrere Bestimmungen ganz oder teilweise rechtsunwirksam werden, wird von der Gültigkeit der übrigen Bestimmungen nicht berührt. Sie kann mit einer dreimonatigen Frist zum Ende eines Quartals gekündigt werden.

Bis zum Abschluss einer neuen Dienstvereinbarung gilt diese Dienstvereinbarung fort.

Einvernehmliche Änderungen und Erweiterungen sind jederzeit schriftlich möglich.

08. Mai 06	gez. Kill	gez. Sturm
Datum	Dienststelle	Personalrat

Anlagen:
1. Liste der genutzten Programme und der erfassten Nutzerdaten
2. Liste der zugriffsberechtigten Personen

Anlage1:

Verwendete elektronische Zugangskontrollsysteme und erfasste Nutzerdaten

Liste der genutzten Progamme:

Zeus Access
DOM ELS
EnterpriseAccess 2000 (MultiAccess)

Liste der erfassten Nutzerdaten

- Ausweis-Nr. (entspricht der Nummer des Transponders oder der Chipkarte)
- Personal-Nr. (nur für ZEUS Access, die Personal-Nr. entspricht hier der Ausweis-Nr.
- Name
- Vorname
- Titel (optional)
- Bereich
- Ausweisart (nur für DOM ELS)
- Sperr-Status
- Berechtigungen
- Gruppenzuordnung
- gültig von
- gültig bis
- Zeitzone (Zutrittszeitraum)

Anlage 2:

Liste der zugriffsberechtigten Personen

Das System lässt unterschiedliche Strukturierung in der Anwendung zu.
Für die separat gesicherten Bereiche haben Zugriff auf die Nutzerdaten in der Anwendung der Systeme:

1. Fachbereich Konservierung und Restaurierung: (Zeus Access)	Frau Lorenz
2. Hochschulrechenzentrum: (Zeus Access)	Dr. Schmidt
3. Hörsäle einschl. deren Medientechnik: (DOM ELS, EnterpriseAccess 2000)	Herr Sowada (ZW)
4. Rechnerpools, Zeichen- und Arbeitsräume: (DOM ELS)	Frau Würbach/ Frau Feith D 4

4.1 Die ständige Vertretung für Frau Würbach nimmt Frau Feith war. Die Vertretung in begründeten Ausnahmen übernimmt Herr Sowada. Auf alle gespeicherten Daten hat selbstverständlich der Systemadministrator des HRZ Zugriff.