BEUTH HOCHSCHULE
FÜR TECHNIK
BERLIN
University of Applied Sciences

Dienstvereinbarung über den Betrieb von Zutrittskontrollanlagen an der Beuth Hochschule für Technik Berlin

Gemäß § 85 Abs. 1 Nr. 13 des Personalvertretungsgesetzes wird folgende Dienstvereinbarung geschlossen:

§ 1 Geltungsbereich

Diese Dienstvereinbarung regelt die Nutzung und den Betrieb der nachgenannten Zutrittskontrollanlagen für alle Dienstkräfte der Beuth Hochschule für Technik Berlin, die unter das Personalvertretungsgesetz des Landes Berlin fallen.

§ 2 Elektronische Zutrittskontrollsysteme entsprechend § 1

(1) Um ein kontrolliertes Betreten und Verlassen der Gebäude für berechtigte Personen zu gewährleisten, ist jeweils an den im Anhang gelisteten Zugängen der Gebäude ein Zutrittskontrollsystem installiert. Damit ist der Zugang für berechtigte Personen innerhalb und außerhalb der Öffnungszeiten gewährleistet.

(2) Im Außengelände der Beuth Hochschule befinden sich Zutrittskontrollsysteme an Zufahrten, um das berechtigte Befahren von Abschnitten des Hochschulaußengeländes zu ermöglichen.

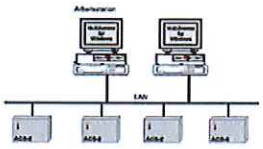
(3) Innerhalb der Häuser befindet sich das Zutrittskontrollsystem an den Türen von besonders schützenswerten Räumen mit hochwertiger Technik und bei Bedarf an weiteren Räumen.

(4) Das Zutrittskontrollsystem besteht aus einem Server-/Clientsystem (Arbeitsstation). Das gesamte System ist mandantenfähig und in diverse Mandanten unterteilt. Die Server-Software zur Zutrittskontrolle wird auf einer virtuellen Maschine (Server) auf einem Zentralserver betrieben und befindet sich physikalisch in einem Serverraum des Hochschulrechenzentrums. Der Server und die Zutrittskontrollsoftware sind durch getrennte Passwörter (Zugriff Host-Server, ZK-Server, ZK-Software) geschützt. Der Umfang des Zugriffs innerhalb der Zutrittskontrolle wird über Passwörter geregelt. Die Client-Software läuft auf einer Arbeitsstation (PC-System). Hier erfolgt die Verwaltung des eigentlichen Systems.

Die Serverräume sind ebenfalls mit einer Zutrittskontrolle gegen unberechtigtes Betreten gesichert. Hier ist sowohl ein persönlicher Zugangscode, als auch eine Zutrittskarte zum Betreten der Räume erforderlich.

Das Zutrittskontrollsystem unterteilt sich in ein Online- und ein Offline-System.

Die Türen im Online-System können zentral von einem Bearbeitungsplatz aus verwaltet werden.





Die Türen im Offline-System werden von einem Bearbeitungsplatz aus verwaltet, die Programmierung erfolgt aber grundsätzlich vor Ort. Eine Auswertung der Ereignisse kann dabei auch nur vor Ort erfolgen, eine Fernabfrage ist nicht möglich.

§ 3 Datenaufzeichnung/Datenspeicherung/Datenverwendung und -auswertung

(1) Auf dem Zutrittskontrollserver werden die Nutzer des Zutrittskontrollsystems mit Namen, Datum und Uhrzeit erfasst. Diese Daten werden nicht zur Überwachung von Leistung und Verhalten von Beschäftigten oder zur Erzeugung von Bewegungsprofilen verwendet. Auf den Arbeitsstationen werden keine Daten erfasst.

(2) Vom DSB und PR als geeignet identifizierte und genehmigte Server werden für die Datenaufzeichnung eingesetzt. Die Genehmigung kann nach schriftlicher qualifizierter Begründung durch die Dienststelle beim DSB + PR durch DSB + PR erteilt werden. Server mit Datenaufzeichnung werden in der *Anlage 1* aufgeführt.

(3) Datenaufzeichnungen finden nur für Räume statt, die vom DSB und PR genehmigt wurden. Die Genehmigung kann nach schriftlicher qualifizierter Begründung durch die Dienststelle beim DSB + PR durch DSB + PR erteilt werden. Räume mit Datenaufzeichnung werden in der *Anlage 2* aufgeführt.

(4) Der Zugriff innerhalb der ZK-Software auf die Protokolldatenbank ist durch das Vier-Augen-Prinzip geschützt. Dazu sind zwei passwortgesicherte Benutzerkonten eingerichtet, nur die gemeinsame Eingabe des Passwortes ermöglicht den Zugriff. Mit Ausnahme der Systemadministratoren ist allen weiteren Nutzern der Zugriff auf die Protokolldatenbank verwehrt. Die Systemadministratoren sind verpflichtet, keine Daten an Dritte herauszugeben. Auf dem Server sind die entsprechenden Dateien durch Verschlüsselung gesichert.

(5) Das Zutrittskontrollsystem ist gegen unberechtigte Nutzung in mehreren Stufen gesichert und passwortgeschützt. Zugriff auf den ZK-Server haben nur die vom Dienststellenleiter ermächtigten Personen. Diese sind im Anhang gelistet. Der Zugriff auf die Daten ist passwortgeschützt (4-Augen-Prinzip). (Schema Zutrittskontrolle siehe *Anlage 1*)

(6) Die Administration des Host-Servers erfolgt durch den Personenkreis der Zutrittsberechtigten zum Serverraum. Die Administratorinnen und Administratoren haben keinen Zugriff auf die durch Nutzung der Zutrittssysteme erzeugten Daten. Ausnahmen werden in § 6 Abs. 2 geregelt.

(7) Die auf einem Zentralserver gespeicherten Informationen werden nach maximal zehn Kalendertagen automatisch gelöscht und neu überschrieben. Nur bei begründeten Auffälligkeiten und damit verbundener Meldung bei der Polizei (Anzeige) kann der DSB die Löschung fallgebundener Daten aussetzen. Daten aufgezeichneter Delikte werden

nach Wegfall ihres Zweckes gelöscht. Im Verdachtsfall, wie unberechtigter Zutritt von Gebäuden und Räumen oder zur Erkennung von Diebstählen/Vandalismus, kann die Löschung durch den DSB kurzfristig bis zur Klärung des Sachverhaltes ausgesetzt werden, längstens jedoch für zehn Werktage in Verbindung mit einer Anfrage des zuständigen Polizeiabschnittes. Bei Ermittlungen erfolgt eine Auswertung der Daten.

(8) Eine Weitergabe der Daten erfolgt nur, sofern die Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG erfüllt sind. Jede Auswertung und Weitergabe von Daten wird dokumentiert.

§ 4 Sonstige Regelungen

Erweiterungen der im Anhang gelisteten Zutrittskontrollanlagen oder Änderungen der Zutrittsberechtigung zum Serverraum bedürfen einer Erweiterung / Änderung der Anlage zur Dienstvereinbarung. Die Aktualität der Anlage wird mindestens einmal jährlich im Laufe des Monats Mai durch Abteilung III geprüft und dem Personalrat bis zum 15. Juni in aktualisierter Version vorgelegt. Die Anschaffung und der Betrieb weiterer Zutrittskontrollsysteme (in Ergänzung zu §1) bedürfen zwingend einer Änderung/Ergänzung dieser Dienstvereinbarung.

§ 5 Grundsätze der Einsichtnahme in die gespeicherten Daten

(1) Der Personalrat stimmt sich im Falle einer Missbrauchsvermutung mit dem DSB ab.

(2) Vor jeder Einsichtnahme in die gespeicherten Daten ist die Rechtsgrundlage durch den behördlichen Datenschutzbeauftragten zu prüfen.

(3) Die Einsicht in die Daten ist nur bei Anwesenheit folgender Personen zulässig:

- Vertreter des Verantwortlichen für die Datenverarbeitung,
- ein Personalratsmitglied, sofern es um Belange von Personen geht, die unter das Personalvertretungsgesetz fallen,
- behördlicher Datenschutzbeauftragter,
- bei polizeilichen Ermittlungen ggf. ein Vertreter der Polizei.

(4) Vor der Einsichtnahme in die gespeicherten Daten ist der Anlass durch die in § 6 Abs. 2 genannten berechtigten Personen zu prüfen. Jede Einsichtnahme wird unter Nennung des Zwecks und der anwesenden Personen dokumentiert.

(5) Die Absätze 1 bis 4 gelten nicht für Zugriffe auf die Datenbank zu Wartungs- und Reparaturzwecken durch den Administrator.

§ 6 Inkrafttreten

(1) Diese Dienstvereinbarung tritt mit ihrer Unterzeichnung in Kraft und ersetzt die bisherigen Dienstvereinbarungen.

(2) Sie kann von jedem Vertragspartner mit einer Frist von zwölf Monaten zum Monatsende gekündigt werden.

§ 7 Salvatorische Klausel

(1) Sofern einzelne Bestimmungen dieser Vereinbarung unwirksam sind oder werden, wird davon die Wirksamkeit der übrigen Bestimmungen nicht berührt.

(2) Sollte den Vertragschließenden dieser Vereinbarung eine eventuelle Unwirksamkeit bekannt werden, verpflichten sie sich, schnellstmöglich eine neue Regelung zu treffen,

die dem gewollten Sinn und Zweck der unwirksamen Bestimmung soweit wie möglich entspricht.

(3) Sollten Tatbestände durch diese Vereinbarung nicht geregelt sein, die den Vertragschließenden dieser Vereinbarung bekannt werden, so verpflichten sie sich, umgehend eine Regelung ergänzend zu vereinbaren, die den Grundsätzen dieser Vereinbarung entspricht.

(4) Jede Änderung und Ergänzung dieser Dienstvereinbarung bedarf der Schriftform. Dies gilt auch für die Abbedingung des Schriftformerfordernisses selbst.

i.V. H. Gross

Prof. Dr. Gross

Die Präsidentin

Andreas Gläser

Andreas Gläser

Vorsitzender des Personalrats

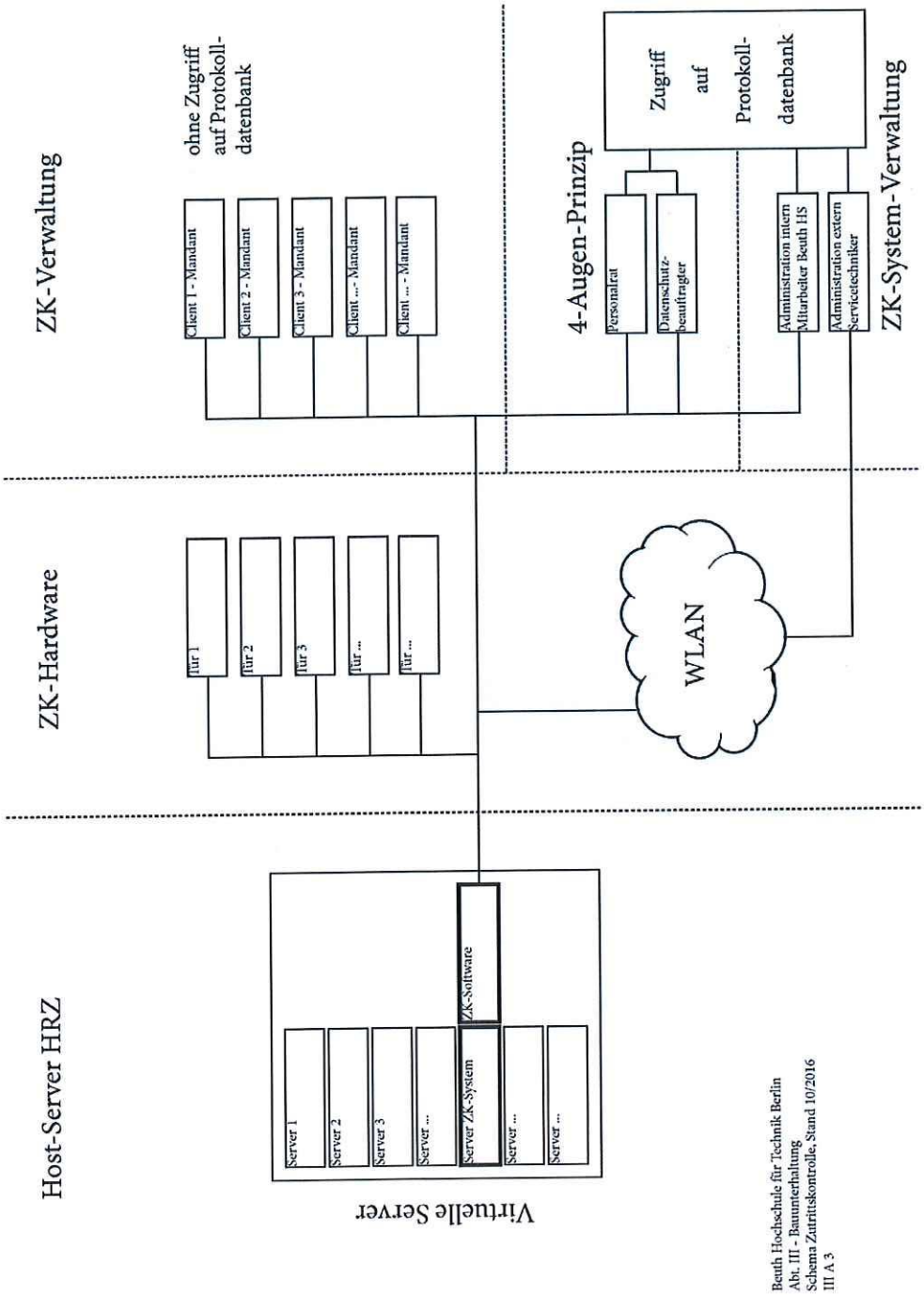
Abkürzungen

DSB Datenschutzbeauftragter PR Personalrat ZK Zutrittskontrolle

Anlage 1 zur

Dienstvereinbarung über den Betrieb von Zutrittskontrollanlagen an der Beuth Hochschule für Technik Berlin

Schema Zutrittskontrolle



Standorte Zutrittskontrolle (Online System)

Haus Beuth (A)

- Außentür Haupteingang Lütticher Straße 38
- Innentür 1. OG Zugang Raum A 111
- Innentür 4. OG Zugang Raum A 410
- Treppenhaus B Zugang 4. OG
- Treppenhaus S Zugang 3. OG
- Innentür 3. OG Zugang Raum A 324
- Innentür 3. OG Zugang Raum A 326
- Innentür 3. OG Zugang Raum A 327
- Innentür 3. OG Zugang Raum A 328
- Innentür 3. OG Zugang Raum A 340 links
- Innentür 3. OG Zugang Raum A 340 rechts

Haus Gauß (B)

- Außentür Haupteingang Luxemburger Straße 22a
- Außentür Eingang Amrumer Straße
- Innentür 5. OG Raum B 527

Haus Grashof (C)

- Außentür Haupteingang Luxemburger Straße 10
- Innentür KG Zugang Raum C 018
- Innentür EG Zugang Pförtnerloge

Haus Bauwesen (D)

- Außentür Haupteingang Luxemburger Straße 9
- Außentür Nebeneingang Ostender Straße - ITW
- Außentür Nebeneingang Ostender Straße - Poststelle
- Außentür Nebeneingang Genter Straße
- Innentür EG Zugang Raum E 38/a/b
- Innentür EG Zugang Raum E 32/33/34
- Innentür 2. OG Zugang Raum D 221
- Innentür 2. OG Zugang Raum D 222
- Innentür 2. OG Zugang Raum D 224
- Innentür 3. OG Flur-Bereich V3/306 Räume D 342 bis 349
- Innentür 3. OG Zugang Raum D 343
- Innentür 3. OG Zugang Raum D 346 links
- Innentür 3. OG Zugang Raum D 346 rechts
- Innentür 3. OG Zugang Raum D 349
- Innentür 2. OG Flur-Bereich V2/305 Räume D 242 bis 249

Präsidialgebäude

- Außentür Haupteingang Lütticher Straße 37

Haus K

- Außentür rechts Haupteingang
- Innentür 1. OG Zugang Raum K 111

Forum Seestraße F

- Haupteingang 2. OG Treppenhaus
- Treppenhaus T53 Zugang 2. OG
- Treppenhaus T53 Zugang 5. OG
- Treppenhaus T53 Zugang 3. OG
- Treppenhaus T57 Zugang EG
- Treppenhaus T57 Zugang 4. OG
- Treppenhaus T56 Zugang 4. OG

Haus Schwedenstraße S

- Tor Hofeinfahrt
- Außentür EG Hofseite
- Treppenhaus C Zugang 4. OG
- Treppenhaus C Zugang 5. OG
- Treppenhaus B Zugang 5. OG
-

Außenanlage

- Parkplatz 1 Schrankenanlage
-

Parkhaus Triftstraße

- Parkhaus Schrankenanlage
-

Standorte Zutrittskontrolle (Offline System):

Haus Beuth (A)

- Innentür EG Zugang Raum A 49
- Innentür 1. OG Zugang Raum A 136
- Innentür 1. OG Zugang Raum A 137
- Innentür 1. OG Zugang Raum A 137a
- Innentür 1. OG Zugang Raum A 138
-

Haus Gauß (B)

- Fehlanzeige

Haus Grashof (C)

- Innentür EG Zugang Raum C 25

Haus Bauwesen (D)

- Innentür 4. OG Zugang Raum D 429
- Innentür 4. OG Zugang Raum D 430
- Innentür 4. OG Zugang Raum D 432
- Innentür 4. OG Zugang Raum D 433
- Innentür 4. OG Zugang Raum D 438
- Innentür 4. OG Zugang Raum D 439

Standorte ähnlicher Systeme (Online/Offline System):

- Haus Grashof/Gewächshaus