RUHR-UNIVERSITÄT BOCHUM

RUB

NR. 1306 | 18.06.2019

AMTLICHE BEKANNTMACHUNG

Dienstvereinbarung über den Einsatz von Elektronischen Zutrittssystemen der Ruhr-Universität Bochum

vom 24.05.2019

Dienstvereinbarung über den Einsatz von Elektronischen Zutrittssystemen der Ruhr-Universität Bochum

vom 24. Mai 2019

zwischen dem
Personalrat der Ruhr-Universität Bochum, vertreten durch den Vorsitzenden, und der Ruhr-Universität Bochum, vertreten durch die Kanzlerin,

sowie zwischen dem
Personalrat der wissenschaftlich/künstlerisch Beschäftigten der Ruhr-Universität Bochum, vertreten durch den Vorsitzenden, und der Ruhr-Universität Bochum, vertreten durch den Rektor

wird gemäß § 70 Personalvertretungsgesetz für das Land Nordrhein-Westfalen (Landespersonalvertretungsgesetz - LPVG NW -) folgende Dienstvereinbarung abgeschlossen:

§ 1 Geltungsbereich

Diese Dienstvereinbarung regelt den Einsatz von elektronischen Zutrittssystemen sowie den Betrieb der dazu notwendigen Verwaltungssoftware an der Ruhr-Universität Bochum. Sie gilt für Beschäftigte der Ruhr-Universität Bochum im Sinne der §§ 5 und 104 LPVG NW. Die Ruhr-Universität Bochum wird die Regelungen dieser Dienstvereinbarung auch auf die Beschäftigten anwenden, die nicht von Personalräten vertreten werden.

§ 2 Begriffsbestimmung

(1) Ein Schließplan umfasst die Schließberechtigungen in einem bestimmten Bereich. Er ergibt sich aus der Festlegung von Türen und Zeiten, zu denen die elektronischen Schlüssel für diesen Bereich Zugang gewähren. Für einen einzelnen Schlüssel ergibt sich daraus ein Zutrittsprofil.

(2) Bereiche können als sicherheitskritisch eingestuft werden, wenn sie mit einem besonderen Risiko verbunden sind. Die Einstufung eines Gebäudes, Bereiches oder Raumes als sicherheitskritisch wird im IT-Ausschuss mit dem Ziel der Einigung verhandelt und bedarf der Zustimmung durch die Personalräte.

§ 3 Zweckbestimmung

(1) Elektronische Zutrittssysteme werden eingesetzt, um

a) den Zutritt zu Gebäuden, Bereichen und Räumen der Ruhr-Universität – ggf. zeitlich begrenzt – für berechtigte Personen zu ermöglichen,

b) Unbefugten den Zutritt zu Gebäuden, Bereichen und Räumen der Ruhr-Universität zu verwehren, um die darin befindlichen Werte vor Diebstahl, Zerstörung oder Manipulation zu schützen.

(2) Alle Systemkomponenten dürfen ausschließlich die für diese Zwecke notwendigen Informationen enthalten und verarbeiten.

(3) Eine Datenspeicherung über Schließvorgänge, die von Beschäftigten der Ruhr-Universität vorgenommen werden, ist grundsätzlich unzulässig. In sicherheitskritischen Bereichen ist eine Datenaufzeichnung von Schließvorgängen zulässig. Weitere Ausnahmen, die bestimmte Standorte oder bestimmte Schlüssel oder Schlüsselgruppen betreffen, bedürfen im Einzelfall der Zustimmung durch die Personalräte.

(4) Für als sicherheitskritisch eingeschätzte Gebäude, Bereich und Räume kann die zusätzliche Eingabe einer PIN vorgesehen werden.

(5) Bei der Vergabe der Schließberechtigungen zu Räumlichkeiten mit möglichen Gefährdungen, z.B. Laborbereich, ist darauf zu achten, dass Zugangsvoraussetzungen – wie beispielsweise notwendige vorherige Einweisungen – vorliegen.

§ 4 Systemdokumentation

(1) Die Zutrittssysteme arbeiten mit Lesestationen an den Eingängen, die mit einem zentralen System vernetzt sind. Die Identifikation einer Person als zutrittsberechtigt erfolgt gegenüber der Lesestation mittels eines kontaktlosen oder kontaktbehafteten elektronischen Schlüssels. Findet ein kontaktloser Schlüssel Einsatz, so ist der Leseabstand aus Sicherheitsgründen in der Regel auf unter 20 cm zu begrenzen.

(2) Für jeden Schlüssel wird auf dem jeweiligen zentralen System und/oder in den zugehörigen Lesestationen ein Zutrittsprofil gespeichert, das nicht mehr als folgende Angaben enthält:
- Identifikationscode,
- Notwendige Kontaktinformationen zum/r Schlüsselinhaber/in,
- Gültigkeit,
- Räumliche und zeitliche Zutrittsbeschränkungen.

(3) In sicherheitskritischen Bereichen kann nach Ablauf eines für das Einzelsystem festzulegenden Zeitraumes, der zum regulären Eintritt in den jeweiligen Bereich angemessen ist, das fehlerhafte Offenstehen einer Tür über eine Anzeige an zentraler Stelle kenntlich gemacht und protokolliert werden.

(4) Das Verlassen von Räumen außerhalb sicherheitskritischer Bereiche erfolgt ohne erneute Identifikation nur durch mechanisches Öffnen einer Tür. Für sicherheitskritische Bereiche können hierzu spezielle Regeln vereinbart werden. In allen Bereichen sind für Notfälle deutlich erkennbare Paniköffnungen von innen und Rettungszugänge von außen in ausreichendem Umfang vorzusehen.

(5) Jedes einzelne Zutrittssystem wird wie folgt dokumentiert:
a) Auflistung der Hardwarekomponenten des Zutrittssystems einschließlich des Installationsplans,
b) Auflistung der Softwarekomponenten des Zutrittssystems,
c) Ggf. Angabe der sicherheitskritischen Bereiche und Angabe dazu, ob dort die Eingabe einer PIN notwendig ist,
d) Angabe der System-Administratoren des Zutrittssystems und deren Vertreter und Nennung der Fakultäts- und Gruppenadministratoren,
e) Verzeichnis der Berechtigungen zur Vergabe von Zutrittsprofilen,
f) Verzeichnis der Berechtigungen zur Weitergabe von Administrationsrechten an Gruppenadministratoren.

§ 5 Inbetriebnahme

(1) Zur Inbetriebnahme eines elektronischen Zutrittssystems gemäß dieser Dienstvereinbarung sind die in §4 Absatz 5 genannten Dokumentationen dem IT-Ausschuss zugänglich zu machen. Dies gilt auch für die Inbetriebnahme eines Systems mit neuen oder veränderten Merkmalen und für erhebliche Erweiterungen bestehender Zutrittssysteme ohne Veränderung von Leistungsmerkmalen. Bei neuen oder veränderten Merkmalen ist zusätzlich eine Stellungnahme des behördlichen Datenschutzbeauftragten erforderlich.

§ 6 Rechte und Pflichten der Beschäftigten

(1) Jede/r zutrittsberechtigte Beschäftigte erhält einen elektronischen Schlüssel kostenfrei. Mit Aushändigung des Schlüssels sind dem/der Beschäftigten das Zutrittsprofil sowie die Namen der zuständigen Administratoren mitzuteilen. Spätere Änderungen sind dem/der Beschäftigten umgehend anzuzeigen.

(2) Jede/r Beschäftigte erhält auf Wunsch Informationen über alle auf dem Schlüssel und in der Verwaltungssoftware zu ihrer/seiner Person aktuell gespeicherten Daten, sowie über Veränderungen seiner Schließberechtigungen innerhalb der letzten 12 Monate.

(3) Die Beschäftigten sind verpflichtet, nach Kenntnisnahme des Verlustes eines elektronischen Schlüssels dessen Sperrung unverzüglich zu veranlassen. Sie werden über die Wege zur Sperrung informiert.

(4) Die Beschäftigten sind verpflichtet, mit persönlichen Identifikationscodes sorgfältig umzugehen und diese nicht weiterzugeben.

§ 7 Administratoren

(1) System-Administratoren und deren Vertretungen richten das System ein, administrieren Schließberechtigungen einer Schließanlage und delegieren weitere Vergaberechte an *Fakultäts-* und *Gruppenadministratoren* (Mandanten). Zur Unterstützung ihrer Arbeit erhalten alle Administratoren die notwendigen Dokumentationen und Hinweise.

(2) Die durch die Fakultät benannten Fakultätsadministratoren verwalten die weiteren an die Gruppenadministratoren zu vergebenden Administrationsrechte der Schließung für die ihrer Fakultät zugeordneten Räume

(3) Der/die Kanzler/in kann Gruppenadministratoren benennen, die die Schließungsrechte für bestimmte Raumgruppen (z.B. Hörsäle, Technikräume, Außentüren, Dachausstiege) verwalten bzw. analog zu Fakultätsadministratoren delegieren.

(4) Erhaltene Administrationsrechte können das Recht beinhalten, diese voll oder teilweise weiter zu delegieren.

(5) Administratoren haben Einsicht in alle Schließberechtigungen, die von ihnen selber oder von ihnen nachgeordneten Administratoren vergeben wurden. Zusätzlich sind sie über „Funktional-Berechtigungen“ (z.B. für Feuerwehr, Reinigungsdienst, Betreiber) zu informieren.

(6) Die Administratoren sind verpflichtet, mit ihren persönlichen Identifikationscodes und Zugangscodes sorgfältig umzugehen und diese nicht weiterzugeben.

(7) Die Administratoren haben sich bei der Vergabe von Schließberechtigungen an die Grundsätze zu Schließplänen (§ 8 dieser Dienstvereinbarung) zu orientieren und diese einzuhalten.

§ 8 Schließpläne

(1) Schließberechtigungen sind weder willkürlich noch diskriminierend so zu vergeben, dass die Beschäftigten ihre Aufgaben bestmöglich erfüllen können.

(2) Der Schließplan für die Außenhülle eines Gebäudes wird spezifisch für jedes Gebäude erstellt. Ein Nutzungskonzept kann die Zugänglichkeit für bestimmte Zeiten einschränken. Der Schließplan für Lehrstühle und Einrichtungen ist so zu gestalten, dass alle Räume mit allgemeinem Charakter (Sozialräume, Teeküchen, Besprechungszimmer) grundsätzlich für alle dort Beschäftigten zugänglich sind.

(3) Ein/e Mitarbeiter/in, deren Schließberechtigung eingeschränkt wurde, kann dazu eine schriftliche Begründung vom betreffenden Administrator verlangen.

(4) Alle Veränderungen der Schließberechtigungen werden für die Dauer von 6 Jahren gespeichert.

§ 9 Rechte der Personalräte

(1) Zutrittsrechte der Personalräte zu Gebäuden, Bereichen und Räumen bleiben unberührt.

(2) Die Personalräte haben das Recht, aktuelle Informationen zu den Administratoren im System abzufragen.

§ 10 Schlussbestimmungen

Diese Vereinbarung tritt am Tage ihrer Unterzeichnung in Kraft. Sie kann von jeder Seite mit sechsmonatiger Frist gekündigt werden. In diesem Fall wirkt sie bis zum Abschluss einer neuen Vereinbarung insgesamt nach. Sollte sich ein Teil dieser Dienstvereinbarung als rechtsunwirksam herausstellen, bleiben die anderen Teile in Kraft.

Bochum, den 24.05.2019

für die Dienststelle:

Der Rektor
Prof. Dr. Axel Schölmerich

Die Kanzlerin
Dr. Christina Reinhardt

für die Personalräte:

für den Personalrat der
wissenschaftlich/künstlerisch Beschäftigten

Der Vorsitzende
Dr. Michael Jost

für den Personalrat

Der Vorsitzende
Frank Markner