Zutritts- und Schließordnung der Hochschule für öffentliche Verwaltung und Rechtspflege (FH), Fortbildungszentrum des Freistaates Sachsen (HSF Meißen) vom 23. November 2026

Inhaltsverzeichnis

Abschnitt 1 – Allgemeines

§ 1 Geltungsbereich
§ 2 Zweck
§ 3 Begriffe

Abschnitt 2 - Zuständigkeiten

§ 4 Schließberechtigte Stellen
§ 5 Ausgabe- und Rückgabestellen
§ 6 Datenschutz und Mitbestimmung

Abschnitt 3 – Raumkategorien und Zutrittsberechtigungen

§ 7 Raumkategorien
§ 8 Berechtigungsgruppen
§ 9 Berechtigungsmatrix
§ 10 Zutrittszeiten
§ 11 Befristete Berechtigungen
§ 12 Sonderfälle

Abschnitt 4 – Schließsysteme

§ 13 Eingesetzte Systeme
§ 14 Notöffnungssysteme und Rettungswege

Abschnitt 5 - Zutrittsmedien und Verfahren

§ 15 Ausnahmeregelungen und Sonderberechtigungen
§ 16 Ausgabe
§ 17 Sorgfaltspflichten
§ 18 Verlust und Sperrung
§ 19 Rückgabe

Abschnitt 6 - Zutrittsdaten und Datenschutz

§ 20 Verarbeitete Daten und Umfang der Protokollierung
§ 21 Speicherdauer und Löschung
§ 22 Zugriff und Auswertung
§ 23 Keine Leistungs- und Verhaltenskontrolle

Abschnitt 7 – Schlussvorschriften

§ 24 Ausschluss von der Nutzung
§ 25 Vertraulichkeit der Berechtigungsmatrix
§ 26 Inkrafttreten

Abschnitt 1 – Allgemeines

§ 1 Geltungsbereich

(1) Diese Zutritts- und Schließordnung (nachfolgend Ordnung) gilt für alle Gebäude, Räume, Zufahrten und Außenanlagen im Geltungsbereich der Haus- und Campusordnung der HSF Meißen, soweit diese mit einer Schließanlage ausgestattet sind oder in Zukunft mit solchen Systemen ausgestattet werden. Soweit für angemietete oder von der HSF Meißen vermietete Objekte eigene Schließ- oder Zutrittsregelungen gelten, gehen diese dieser Ordnung vor.
(2) Diese Ordnung ergänzt die Haus- und Campusordnung und die Brandschutzordnung der HSF Meißen. Regelungen zum Brandschutz und zur Rettung von Personen gehen dieser Ordnung vor.
(3) Diese Ordnung gilt für alle Personen, denen von der HSF Meißen ein Zutrittsmedium überlassen oder auf sonstige Weise Zutritt gewährt wird.

§ 2 Zweck

(1) Diese Ordnung regelt die Zutrittsberechtigungen und Zutrittszeiten sowie die Vergabe, Nutzung und Verwaltung von Schlüsseln und elektronischen Zutrittsmedien.
(2) Sie dient dem Schutz von Eigentum und sensiblen Daten vor unbefugtem Zugang, Diebstahl, Beschädigung und Missbrauch, der Aufrechterhaltung eines geordneten Lehr-, Forschungs- und Verwaltungsbetriebs sowie der Festlegung einer nach Aufgaben abgestuften Zutrittsstruktur.
(3) Der Zutritt wird nur so weit beschränkt, wie es zur Erfüllung dieser Zwecke erforderlich ist. Die Belange von Lehre, Forschung, Studium und Fortbildung sind angemessen zu berücksichtigen.

§ 3 Begriffe

Im Sinne dieser Ordnung sind:
1. *Schließanlage*: die Gesamtheit aller mechanischen und elektronischen Schließeinrichtungen,
2. *Zutrittsmedien*: mechanische Schlüssel und elektronische Identifikationsmittel (wie Transponder, RFID-Karten, Chipkarten, BLE-Technik u.a.),
3. *Raumkategorie*: Gruppe gleichartiger Räume oder Zugänge nach § 7,
4. *Nutzergruppe*: Personenkreis mit gleichen Zutrittsrechten nach § 8,
5. *Zeitprofile*: Festlegung der Zeiten, in denen ein Zutritt möglich ist,
6. Generalschlüssel: Berechtigung, die den Zutritt zu allen Raumkategorien ermöglicht,
7. *Zutrittsdaten*: bei Nutzung eines elektronischen Zutrittsmediums erhobene Daten (Medium, Tür, Zeitpunkt, Ergebnis),
8. *Stammdaten*: zur Verwaltung der Berechtigungen gespeicherte Daten der Zutrittsmedieninhaberinnen und -inhaber.

Abschnitt 2 – Zuständigkeiten

§ 4 Schließberechtigte Stellen

(1) Schließberechtigte Stellen im Sinne dieser Regelung sind die Leitung des Referats Allgemeine Verwaltung, die zuständige Sachgebietsleitung Bau, Liegenschaften und Technik, die Leitung der Haustechnik sowie alle weiteren Bediensteten, deren Zuständigkeit sich aus den Aufgabenübertragungen des Geschäftsverteilungsplans für diesen Bereich ergibt.
(2) Die schließberechtigten Stellen führen den Schließplan und verwalten die Schließanlage; sie richten Berechtigungen ein und sperren sie. Änderungen an der Schließanlage dürfen nur durch sie oder auf deren Veranlassung realisiert werden. Die Berechtigungen werden mindestens einmal jährlich überprüft. Nicht mehr benötigte Rechte werden entzogen. Das Ergebnis wird dokumentiert.

§ 5 Ausgabe- und Rückgabestellen

(1) Die Funktion der Ausgabe- und Rückgabestellen wird von der Rezeption (zugleich Tagungsbüro, Haus 3) sowie von den im Geschäftsverteilungsplan außerhalb der Rezeption für diesen Bereich ausgewiesenen Bediensteten wahrgenommen.
(2) Die Ausgabestelle gibt ein Medium nur aus, wenn die schließberechtigte Stelle die Berechtigung eingerichtet hat. Sie lässt den Empfang quittieren.
(3) Die Rückgabestelle prüft bei der Rückgabe die Vollständigkeit und den Zustand des Mediums und quittiert den Erhalt bei Bedarf.

§ 6 Datenschutz und Mitbestimmung

(1) Die oder der Datenschutzbeauftragte ist vor Einführung und wesentlicher Änderung von Verfahren der Zutrittskontrolle zu beteiligen.
(2) Der Personalrat sowie weitere gesetzliche Interessenvertretungen sind nach den gesetzlichen Vorschriften zu beteiligen. Die Beschäftigten werden über Zweck, Umfang und Dauer der Datenverarbeitung informiert.

Abschnitt 3 – Raumkategorien und Zutrittsberechtigungen

§ 7 Raumkategorien

(1) Die Räume und Zugänge der HSF Meißen werden folgenden Raumkategorien zugeordnet:

1. Außentüren je Haus (1- 9)
2. Beratungsräume/Besprechungsräume
3. Büros
4. Dachzugangstür Haus 3
5. IT-Lehrsäle

6. Kleingruppenräume ICM
7. Lehrsäle, Seminarräume und Kleingruppenräume Campus
8. Lehrsäle ICM
9. Reinigungsräume
10. Schranke (Rülingstraße)
11. Schranke (Herbert-Böhme-Straße)
12. Tor BOH Parkplatz
13. Serverräume
14. Sporteingang Haus 4
15. Technikräume
16. Tor BOH Wirtschaft
17. Übernachtungszimmer

(2) Eine Kategorie kann mehrere Räume oder Zugänge umfassen. Zugangsrechte werden grundsätzlich je Kategorie vergeben.

1. Bei Raumkategorien mit **Sammelberechtigung** (z. B. Außentüren, Lehrsäle, Beratungsräume) schließt die Zuweisung der Kategorie das Zutrittsrecht für alle dieser Kategorie zugeordneten Räume und Zugänge ein.
2. Bei Raumkategorien mit **Individualberechtigung** (z. B. eigene Büros) umfasst die Zuweisung der Kategorie für die berechtigte Person ausschließlich den konkret zugewiesenen Raum (Einzelberechtigung).

§ 8 Berechtigungsgruppen

(1) Zutrittsrechte werden an folgende Nutzergruppen vergeben:

1. Generalschlüsselberechtigte (Kanzler, RLVA, SGL BLT, Lt. + Haustechnik)
2. Generalschlüssel Feuerwehr und Notfall
3. IT
4. Bedienstete HSF
5. externe Dozenten
6. externe Firmen
7. Telekommunikationsanbieter
8. Reinigung
9. Wachschutz
10. Studierende grundständig
11. Studierende berufsbegleitend
12. ÜN Haus 3

(2) Rechte werden der Rolle zugeordnet, nicht der einzelnen Person.

§ 9 Berechtigungsmatrix

(1) Die Zutrittsrechte ergeben sich aus der Berechtigungsmatrix in der Anlage zu dieser Ordnung. Sie regelt den Umfang der Rechte sowie die Raum- und Nutzergruppenzuordnungen.
(2) Über Änderungen der Matrix entscheidet die schließberechtigte Stelle. Der örtliche Personalrat ist unverzüglich über Änderungen zu informieren.

§ 10 Zutrittszeiten

(1) Der Zutritt zu den Liegenschaften und Räumen der Dienststelle wird über differenzierte, nutzergruppen- und raumbezogene Zeitprofile gesteuert. Die konkreten Zeitfenster der jeweiligen Profile ergeben sich aus der Berechtigungsmatrix.
(2) Für Veranstaltungen oder zeitlich befristete Projekte kann die schließberechtigte Stelle temporäre Sonderprofile einrichten.

§ 11 Befristete Berechtigungen

(1) Gäste, Externe, Aushilfen und beauftragte Firmen erhalten Zutrittsrechte nur befristet und für die erforderlichen Bereiche, längstens für die Dauer des Auftrags.
(2) Die Anmeldung erfolgt durch die einladende Organisationseinheit, spätestens zwei Werktage vorher.

§ 12 Sonderfälle

(1) Die Feuerwehr erhält Zugang über das Feuerwehrschlüsseldepot.
(2) Generalschlüssel werden nur in dem für den Betrieb notwendigen Umfang ausgegeben. Über die Ausgabe entscheidet die schließberechtigte Stelle.

Abschnitt 4 – Schließsysteme

§ 13 Eingesetzte Systeme

1. Mechanische Zylinder bieten keine Zeitprofile und keine Protokollierung. Bei Schlüsselverlust ist die Notwendigkeit eines Zylindertauschs zu prüfen.
2. Elektronische Offline-Zylinder (Intrakey/Secanda) sind batteriebetrieben; Rechte und Sperrlisten werden über das Zutrittsmedium oder durch Programmierung vor Ort übertragen. Änderungen wirken erst mit der nächsten Aktualisierung des Zutrittsmediums (also insbesondere der RFID-Zutrittstransponder).
3. Online-Systeme (Intrakey/Secanda) sind über Kabel oder Funk an die zentrale Verwaltung angebunden. Rechte- und Sperränderungen wirken sofort; Ereignisse werden zentral erfasst.
4. Hybride Systeme kombinieren Online-Systeme (Wandleser) mit elektronischen Offlinezylindern.

§ 14 Notöffnung und Rettungswege

(1) Rettungswege müssen jederzeit ohne Medium in Fluchtrichtung nutzbar sein.
(2) Notöffnungen sind der schließberechtigten Stelle zu melden.

Abschnitt 5 - Zutrittsmedien und Verfahren

§ 15 Ausnahmeregelungen und Sonderberechtigungen

(1) Über den standardmäßigen, rollenbezogenen Zutritt hinaus können in begründeten Fällen erweiterte Zutrittsberechtigungen beantragt werden.
(2) Genehmigt werden Anträge durch die schließberechtigte Stelle.

§ 16 Ausgabe

(1) Alle Zutrittsmedien bleiben Eigentum der Dienststelle. Die Ausgabe erfolgt personalisiert und bedarfsorientiert. Die Ausgabestelle lässt sich den Empfang des Zutrittsmediums schriftlich quittieren.
(2) Die Erstausgabe von Zutrittsmedien erfolgt kostenfrei. Geht ein Zutrittsmedium verloren oder wird es durch unsachgemäßen Gebrauch unbrauchbar, wird für den Ersatz im Regelfall eine Pauschale gemäß der Organisationsverfügung Gebührenfestlegung und Beglaubigungen an der Hochschule Meißen (FH) und Fortbildungszentrum in ihrer jeweils gültigen Fassung fällig. Die Erhebung etwaiger Folgekosten (z. B. Tausch von Zylindern) im Einzelfall bleibt unberührt.

§ 17 Sorgfaltspflichten

(1) Wer ein Zutrittsmedium besitzt, trägt die persönliche Verantwortung für dessen sichere Aufbewahrung und ordnungsgemäße Nutzung. Zutrittsmedien sind nur persönlich zu nutzen und dürfen nicht weitergegeben, verliehen oder vervielfältigt werden. Der Zutritt Unberechtigter durch Mitnahme ist zu unterlassen.
(2) Festgestellte Mängel an Schließzylindern, Türen, Toren oder Fenstern, die ein ordnungsgemäßes Verschließen behindern, sind unverzüglich an der Rezeption (zugleich Tagungsbüro, Haus 3) oder die Haustechnik zu melden.

§ 18 Verlust und Sperrung

Der Verlust ist unverzüglich an der Rezeption (zugleich Tagungsbüro, Haus 3) zu melden. Das Medium wird daraufhin unverzüglich gesperrt. Bei Verlust eines Schlüssels bewertet die schließberechtigte Stelle das Risiko und veranlasst gegebenenfalls einen Zylindertausch.

§ 19 Rückgabe

(1) Zutrittsmedien sind spätestens am letzten Tag des Beschäftigungs- bzw. Studienverhältnisses an den Rückgabestellen abzugeben, bei Wechsel der Organisationseinheit auf Verlangen.
(2) Die Personalstelle und das Studierendensekretariat melden Austritte an die schließberechtigte Stelle, die die Rechte deaktiviert.

Abschnitt 6 - Zutrittsdaten und Datenschutz

§ 20 Verarbeitete Daten und Umfang der Protokollierung

(1) Zur Verwaltung der Berechtigungen werden folgende Stammdaten der Medieninhaberinnen und Medieninhaber verarbeitet: Name, Vorname, Organisationseinheit bzw. Funktion, Berechtigungsgruppe, Kennung des Zutrittsmediums, zugewiesene Berechtigungen und Zeitprofile sowie Ausgabe-, Rückgabe- und Ablaufdatum.
(2) Zutrittsdaten werden nur an Online- und Offlinekomponenten (§ 13 Nr. 2 - 4) protokolliert. Bei mechanischen Zylindern (§ 13 Nr. 1) erfolgt keine personenbezogene Protokollierung. Protokolliert werden die Kennung des Mediums, die Tür, der Zeitpunkt und das Ergebnis des Zutrittsversuchs. Die Protokolle enthalten keine Klarnamen. Zutrittsereignisse sind in pseudonymisierter Form gespeichert. Die Zuordnung einer Kennung zu einer Person erfolgt nur im Rahmen einer Auswertung nach § 22 und erfordert gesondert geschützte Zuordnungsdaten.
(3) Die Verarbeitung personenbezogener Daten der Beschäftigten im Zusammenhang mit dem elektronischen Schließsystem richtet sich nach der Datenschutz-Grundverordnung (DSGVO) und den hierzu erlassenen spezialgesetzlichen Regelungen des Bundes- und Landesrechts, insbesondere nach Art. 6, Art. 9 und Art. 88 DSGVO. Soweit Beschäftigtendaten verarbeitet werden, erfolgt dies auf der Grundlage von Art. 6 Abs. 1 DSGVO (insbesondere Buchst. c und e – Erfüllung rechtlicher Pflichten der Dienststelle sowie Wahrnehmung einer Aufgabe im öffentlichen Interesse) in Verbindung mit den einschlägigen spezialgesetzlichen Befugnissen des sächsischen Landesrechts, insbesondere dem Sächsischen Datenschutzdurchführungsgesetz (SächsDSDG) und den an die DSGVO angepassten bereichsspezifischen Regelungen, soweit sie eine Verarbeitung von Beschäftigtendaten zur Aufgabenerfüllung der Dienststelle erlauben. Dabei werden die Mitbestimmungsrechte des Personalrates beachtet.
(4) Die Stammdaten der Medieninhaber und die Zutrittsdaten dürfen ausschließlich zur Verwaltung der Berechtigungen, zur Gewährleistung der Zutrittskontrolle und Gebäudesicherheit (Schutz von Personen, Sachen und Daten), zur technischen Fehleranalyse des Schließsystems sowie zur Aufklärung konkreter Sicherheitsvorfälle verarbeitet werden.

§ 21 Speicherdauer und Löschung

(1) Die Stamm- und Zutrittsdaten werden nur so lange gespeichert, wie es für die Zwecke nach § 20 Abs. 4 erforderlich ist. Da sicherheitsrelevante Vorkommnisse oder Medienverluste im Dienstbetrieb – insbesondere während Urlaubsphasen, der vorlesungsfreien Zeit oder bei Liegenschaften mit geringer Nutzungsfrequenz – oft erst verzögert festgestellt werden, gelten, sofern keine überwiegenden schutzwürdigen Interessen oder rechtlichen Aufbewahrungspflichten nach Absatz 2 entgegenstehen, folgende Speicherfristen:
1. Die Stammdaten der Medieninhaber sowie die Aus- und Rückgabequittungen werden spätestens drei Monate nach Rückgabe des Mediums bzw. nach der Beendigung des Beschäftigungs- oder Studienverhältnisses gelöscht, soweit eine Speicherung zur Nachweisführung nicht mehr erforderlich ist.

2. Bei Online-Schließsystemen (§ 13 Nr. 3) werden Zutrittsereignisse automatisiert zentral gespeichert und spätestens 30 Tage nach ihrer Erhebung automatisch gelöscht.
3. In Offline-Zylindern lokal gespeicherte Zutrittsdaten werden durch das technische System im Ringspeicher (FIFO-Prinzip) bei Erreichen der Kapazitätsgrenze von maximal 512 Einträgen automatisch fortlaufend überschrieben. Ältere Einträge gelten mit der Überschreibung als gelöscht. Eine Auslesung von Offline-Zylindern erfolgt grundsätzlich nur bei einem konkreten, dokumentierten Sicherheitsvorfall oder zur technischen Fehleranalyse.
Im Übrigen wird auf § 22 verwiesen.
(2) Liegt ein konkreter Sicherheitsvorfall vor, insbesondere ein Diebstahl, Einbruch, unbefugter Zutritt, Verlust eines Zutrittsmediums, Sabotage oder ein begründeter Verdacht hierauf, dürfen die für die Aufklärung erforderlichen Zutrittsdaten über die regelmäßigen Löschfristen nach Absatz 1 hinaus gespeichert werden. Die Speicherung ist auf die tatsächlich betroffenen Personen, Medien, Türen, Zeiträume und Zylinder zu beschränken. Die Daten sind spätestens einen Monat nach Abschluss der Aufklärung zu löschen, es sei denn, ihre weitere Speicherung ist zur Wahrnehmung berechtigter Interessen, zur Geltendmachung, Ausübung oder Abwehr von Rechtsansprüchen oder aufgrund gesetzlicher Pflichten erforderlich.

§ 22 Zugriff und Auswertung

(1) Zugriff auf Zutrittsdaten haben nur die schließberechtigten Stellen. Der Zugriff auf gesonderte Zuordnungsdaten der pseudonymen Medienkennungen ist auf den für diese Aufgabe im Geschäftsverteilungsplan ausdrücklich bestimmten, eng begrenzten Personenkreis beschränkt.
(2) Das Auslesen von Offline-Zylindern vor Ort erfordert neben dem technischen Auslesegerät zwingend den Einsatz einer zusätzlichen, personengebundenen Identifikationskarte, die sich ausschließlich im Besitz der Leitung des Referats Allgemeine Verwaltung (Tresor auf Ebene 3) und damit räumlich getrennt vom Auslesegerät (gesicherte Aufbewahrung auf Ebene 1) befindet. Nach dem Auslesen sind vor der Aufhebung der Pseudoanonymisierung die ausgelesenen Datensätze der Offline-Zylinder zu löschen, sofern diese älter als 30 Tage sind.
(3) Eine Auswertung der nach § 21 Abs. 2 gesicherten Zutrittsdaten (Auflösung einer pseudonymisierten Mediumkennung zu einer Person) erfolgt ausschließlich zur Aufklärung von Straftaten oder bei konkreten sicherheitsrelevanten Vorfällen im Vier-Augen-Prinzip nach Zustimmung des Personalrats. Eine anlasslose Auswertung sowie verdachtsunabhängige Routinekontrollen sind unzulässig.
(4) Jede Auswertung wird mit Anlass, Umfang und Beteiligten dokumentiert.

§ 23 Keine Leistungs- und Verhaltenskontrolle

Zutrittsdaten werden nicht zur Leistungs- oder Verhaltenskontrolle, zur Arbeitszeiterfassung oder für Bewegungsprofile verwendet.

Abschnitt 7 – Schlussvorschriften

§ 24 Ausschluss von der Nutzung

(1) Wer gegen diese Ordnung schwerwiegend oder wiederholt verstößt, kann zeitweise oder dauerhaft, teilweise oder vollständig von der Nutzung des Zutrittssystems ausgeschlossen werden.
(2) Weitergehende Maßnahmen nach der Haus- und Campusordnung sowie dienst-, arbeits- oder studienrechtliche Maßnahmen bleiben unberührt.

§ 25 Vertraulichkeit der Berechtigungsmatrix

(1) Die Berechtigungsmatrix enthält sicherheitsrelevante Angaben und wird daher nicht veröffentlicht.
(2) Jede Person erhält Auskunft über die für sie geltenden Berechtigungen und Zutrittszeiten. Die nicht veröffentlichte Berechtigungsmatrix kann von Personen mit berechtigtem Interesse bei der schließberechtigten Stelle eingesehen werden. Der Personalrat und die oder der Datenschutzbeauftragte haben auch ohne Nachweis eines berechtigten Interesses jederzeit ein Einsichtsrecht.

§ 26 Inkrafttreten

Diese Ordnung wurde unter Wahrung der Mitbestimmungsrechte des Personalrats gemäß den Vorschriften des Sächsischen Personalvertretungsgesetzes (SächsPersVG) vereinbart. Diese Ordnung tritt mit dem Tag ihrer Bekanntmachung durch Aushang und auf der Website der HSF Meißen in Kraft.

Meißen, den 23. November 2026

gez. Frank Degenkolbe
Kanzler

Anlage: Berechtigungsmatrix **(nicht öffentlich)**