Konzept einer elektronischen Schließanlage

1. Geltungsbereich

Dieses Konzept gilt für den Einsatz der neu beschafften elektronischen Schließanlage von SimonsVoss an den Standorten Iserlohn und Soest der Fachhochschule Südwestfalen sowie für den Betrieb der dazu notwendigen Managementsoftware „Locking System Management“ (LSM).

2. Zweckbestimmung

Elektronische Schließanlagen werden zu den Zwecken eingesetzt,

- den Zutritt zu Gebäuden, Bereichen und Räumen der FH SWF, ggf. auch nur zeitlich begrenzt, auf berechtigte Personen einzuschränken,
- Unbefugten den Zutritt zu Gebäuden, Bereichen und Räumen der FH SWF zu verwehren, um die darin befindlichen Werte vor Diebstahl, Zerstörung oder Manipulation zu schützen.
- Potentiellen Schadensereignissen vorzubeugen (z.B. indem Fehlbedienungen an den Aussentüren vorgebeugt wird).

Elektronische Schlüssel (Transponder) dürfen ausschließlich die für den Zutritt notwendigen Informationen enthalten und verarbeiten. Auch innerhalb der Managementsoftware dürfen lediglich die für die Verwaltung der Schließanlagen und Transponder erforderlichen Daten verarbeitet werden. Personenbezogene Daten dürfen nur innerhalb der Managementsoftware verarbeitet werden, außerhalb der Managementsoftware dürfen nur Identifikationsnummern zum Einsatz kommen. Die Zuordnung zu Personen erfolgt getrennt vom Schloss und Schließmedium in einem separaten Datenbankbereich innerhalb der Software.

Anfallende Daten auf dem Transponder dürfen nur verarbeitet werden, soweit sie für die Bedienung der Schließanlage und zur Fehleranalyse erforderlich sind. Dabei findet eine Übertragung von Namen nicht statt. Darüber hinaus dürfen die Daten nur zur Aufklärung von Straftaten in einem polizeilichen Ermittlungsverfahren verwendet werden. Die Entscheidung hierzu trifft die*der Kanzler*in oder die*der oder im Vertretungsfall die*der Verwaltungsdirektor*in. Sie dürfen nicht zu Zwecken einer Verhaltens- oder Leistungskontrolle oder zu Zwecken dienstlicher Beurteilungen oder Disziplinarmaßnahmen verarbeitet werden.

3. Systembeschreibung

Die elektronische Schließanlage arbeitet mit Lesestationen an den Eingängen, die mit einem zentralen System (Client Server Lösung) vernetzt sind, welches in der FH gehostet wird. Die funktionsbezogenen Standardprofile sind auf dem jeweiligen zentralen System, in den zugehörigen Lesestationen sowie auf den Transpondern gespeichert und enthalten folgende Angaben:

- Identifikationsnummer des Transponders (TID; wird automatisch vom System generiert)
- Identifikationsnummer der Tür
- Gültigkeit des Transponders/Zustand;
- Zugangsberechtigungen;
- Berechtigungszeitraum.

Der Beschlag bzw. das digitale Schloss verarbeitet die folgenden Angaben:

- Identifikationsnummer des Transponders (TID);
- Identifikationsnummer der Tür
- Datum, Uhrzeit des Öffnens/ Schließens.

Die Identifikation der zutrittsberechtigten Person erfolgt über das Aktivierungsterminal mittels des kontaktlosen oder kontaktbehafteten Transponder. Beim Einsatz kontaktloser Schlüssel ist der Leseabstand aus Sicherheitsgründen auf unter 20 cm begrenzt.

In der zentralen Managementsoftware LSM werden die folgenden Daten verarbeitet:

- Vorname (Pflichtfeld);
- Nachname (Pflichtfeld);
- Arbeitsbereich/Organisationseinheit/Abteilung;
- Ort/Gebäude;
- Zugangsberechtigungen für Räume und Gebäude;
- Berechtigungszeitraum für die Schließung und Gültigkeit des Transponders;
- Datum, Uhrzeit des Öffnens/Schließens;
- Identifikationsnummer des Transponders (TID);
- Identifikationsnummer der Tür
- Raumnummer bzw. Nummer des digitalen Schlosses
- Seriennummer des Transponders;
- Typ des Transponders (G 2);
- Bei anlassbezogenem Auslesen der Daten (s. Ziff. 11.1 und Anlage 3): Datum, Uhrzeit des Öffnens/ Schließens in Verbindung mit den weiteren o. g. Daten;
- Nur für Export: Person, Person History und Person Log;
- Benutzername, Kennwort und UserLog;
- Transpondergruppe.

Die Schließanlage besteht aus den folgenden Baugruppen:

- Zentrale Managementsoftware „Locking System Management“;
- SmartHandle (digitaler Türbeschlag), elektronische Zylinder und SmartRelais (Aktivierungsterminal);
- Transponder.

4. Betreiberverantwortung

Verantwortlich für die Vorgaben zur Installation, den Betrieb der elektronischen Schließanlage und den Zugriff auf die gespeicherten Daten ist das Dezernat 7 Gebäudemanagement, im Folgenden Dezernat 7, der FH SWF. Die Betreiberverantwortung kann mit Verfügung der*des Kanzlerin*s auf andere Organisationseinheiten übertragen werden.

5. Änderungen und Erweiterungen der Schließanlage

Erweiterungen oder Änderungen der Schließanlage bedürfen der Zustimmung der*s Kanzler*in und der Personalräte.

Ersatzbeschaffungen oder der Austausch von bestehenden Baugruppen, auch gegen neuere Versionen, gelten nicht als Änderung oder Erweiterung der Schließanlage, sofern dadurch nicht andere/weitere Daten verarbeitet werden.

6. Definitionen der Schließanlage

6.1 GHS (Generalhauptschlüssel)

Der GHS hat die Berechtigung, alle Türen eines Standortes der FH SWF zu öffnen und zu schließen.

Für die Feuerwehren, externen Dienstleister*innen und die*den Vorarbeiter*in der Reinigungskräfte gibt es noch einen untergeordneten GHS, der nur für die jeweilige Liegenschaft berechtigt ist.

Einen GHS erhalten folgende Personen:

- Kanzler*in,
- Rektor*in,
- Verwaltungsdirektor*in,
- Mitarbeiter*innen des für den Standort zuständigen Sachgebiets des Dezernates 7.

6.2 Außentüren

Die Haupteingänge werden morgens und abends durch das Dezernat 7 bzw. von diesem Beauftragte Personen (Reinigungskräfte/Wachdienst) geöffnet bzw. abgeschlossen. Die Schließzeiten richten sich nach den offiziellen Öffnungszeiten der Gebäude lt. Anlage zur Hausordnung.

Professor*innen können eine entsprechend begründete „Außentürschließung“ über die*den Dekan*in bei der*dem Kanzler*in oder einer durch sie*ihn beauftragte Person beantragen und erhalten damit Schließberechtigungen für Außentüren im jeweiligen Bereich (der Bereich/die betroffenen Außentüren sind im Antrag zu definieren).

Im Einzelfall können auch andere Mitarbeiter*innen, deren Aufgabe es verlangt, diese Außentürschließberechtigung für die Dauer der dienstlichen Notwendigkeit zu erhalten, einen Antrag unter folgenden Bedingungen stellen:

- Begründung, warum der Zugang notwendig ist
- Beantragung über die*den Vorgesetzte*n
- Zustimmung der*des Kanzlerin*s oder einer von ihr*ihm beauftragten Person.

6.3 Innentüren

Die Schließberechtigung für Innentüren wird gemäß Ziff. 7 erteilt. Gegebenenfalls weitere erforderliche Zutrittsberechtigungen müssen vom Raumverantwortlichen beantragt werden.

6.4 Technikräume

Die Schließberechtigung für Technikräume wird Mitarbeiter*innen des Dezernats 7 und Handwerker*innen erteilt.

Gegebenenfalls weitere erforderliche Zutrittsberechtigungen müssen vom Raumverantwortlichen beantragt werden (z.B. um Zutritt zu Servern zu erhalten).

7. Erteilung von Schließberechtigungen und Gültigkeit von Transpondern

Die Erteilung einer Schließberechtigung erfolgt ausschließlich auf Antrag per E-Mail, in dem die dienstlichen und organisatorischen Notwendigkeiten durch den jeweils zuständigen Raumverantwortlichen mittels Unterschrift ausdrücklich bestätigt werden.

Die Transponder werden durch die jeweilig zuständigen Sachgebiete des Dezernat 7 programmiert, ausgegeben und durch den Nutzer an einem Aktivierungsterminal validiert. Jeder Transponder der nach einem Ereignis (z.B. geänderte Schließberechtigung, gesperrte Transponder) neu validiert wird, verteilt durch seine Benutzung den aktuellsten Stand automatisch, an die Türen die er begeht, weiter.

Die personalisierten Transponder dürfen nicht an andere Beschäftigte, Studierende oder Dritte weitergegeben werden. Transponder die nicht personalisiert werden (z.B. kurzzeitiger Laborzugang für Studierende), können vom jeweiligen Verantwortlichen, mit den entsprechenden Schließberechtigungen, per E-Mail beim Dezernat 7 angefordert werden. Nach Übergabe an den*die Raumverantwortliche*n und Absprache mit Dezernat 7, können diese an den Aktivierungsterminals aktiviert werden.

Aus Sicherheitsgründen sind die Transponder vor der erstmaligen Verwendung und nach Ablauf ihrer Gültigkeit (siehe folgende Ziffern) und bei Änderungen der Schließberechtigung an einem Aktivierungsterminal neu zu aktivieren (siehe Ziff. 9).

7.1 Professor*innen

- Sein/ihr Büro
- Allgemein nutzbare Räume in seinem/ihrem Bereich (z.B. Teeküchen, Kopierräume)
- Organisationseinheitsspezifische Räume (z.B. Archive, Besprechungsräume)
- Alle Seminarräume, Hörsäle und PC-Pools des Fachbereichs
- **Notwendige** Labore, Messräume
  Die*Der jeweilige Raumverantwortliche entscheidet, wer Zugang hat (Sicherheitsunterweisung)
- Weitere Räume können bei dienstlicher Notwendigkeit über den*die Raumverantwortliche*n beantragt werden.

Dekan*in
- wie Professor*in mit der Ergänzung, dass der/die Dekan*in für alle Labore usw., die in die Zuständigkeit seines/ihres Fachbereichs fallen, berechtigt ist.

Der Transponder für Professor*innen ist 16 Stunden gültig.

7.2 Beschäftigte in den Fachbereichen

Wissenschaftliche Mitarbeiter*innen, Lehrkräfte für besondere Aufgaben und in der Lehre/Forschung eingesetzte Beschäftigte in Technik und Verwaltung

- Sein/ihr Büro
- Allgemein nutzbare Räume in seinem/ihrem Bereich (z.B. Teeküchen, Kopierräume)
- Organisationseinheitsspezifische Räume (z.B. Archive, Besprechungsräume)
- Alle Seminarräume, Hörsäle und PC-Pools des Fachbereichs
- **Notwendige** Labore, Messräume
  Die*Der jeweilige Raumverantwortliche entscheidet, wer Zugang hat (Sicherheitsunterweisung)
- Weitere Räume können bei dienstlicher Notwendigkeit über den*die Raumverantwortliche*n beantragt werden

Mitarbeiter*innen des Dekanats
+ Zugang zum Büro der*des Dekans*in und weitere gewünschte (wird von der*dem Dekan*in definiert).

Lehrbeauftragte und Dienstvertragsnehmer*innen im Verbundstudium

- Alle Seminarräume, Hörsäle und PC-Pools des Fachbereichs
- **Notwendige** Labore, Messräume
  Die*Der jeweilige Raumverantwortliche entscheidet, wer Zugang hat (Sicherheitsunterweisung)
- Weitere Räume können bei dienstlicher Notwendigkeit über den*die Raumverantwortliche*n beantragt werden

wissenschaftliche und studentische Hilfskräfte

- **Notwendige** Labore, Messräume

Die*Der jeweilige Raumverantwortliche entscheidet, wer Zugang hat (Sicherheitsunterweisung)
- Weitere Räume können bei dienstlicher Notwendigkeit über den*die Raumverantwortliche*n beantragt werden

Der Transponder für die in Ziff. 7.2 aufgeführten Mitarbeiter*innen ist 16 Stunden gültig.

7.3 Studierende

- **Notwendige** Labore, Messräume
  Der jeweilige Raumverantwortliche entscheidet, wer Zugang hat (Sicherheitsunterweisung)
- Weitere Räume können bei dienstlicher Notwendigkeit über den*die Raumverantwortliche*n beantragt werden

Der Transponder für Studierende ist für 16 Stunden gültig.

7.4 Mitarbeiter*innen in zentralen Einheiten und in der Verwaltung

Hierunter fallen alle Mitarbeiter*innen in den Dezernaten, Stabsstellen und zentralen Einheiten.

Mitarbeiter*innen

- Zugang zu seinem/ihrem Büro
- Allgemein nutzbare Räume in seinem/ihrem Bereich (z.B. Teeküchen, Kopierräume)
- Organisationseinheitsspezifische Räume (z.B. Archive, Besprechungsräume)
- Weitere Räume können bei Bedarf von der*dem jeweiligen Raumverantwortlichen beantragt werden

Sachgebiets- und Bereichsleiter*innen

+ alle Berechtigungen ihres*seines Sachgebiets oder Bereiches
Hinweis: Zugang für Sachgebiets- und sonstige Leitungen zum Büro der*des Dezernent*innen, die diese*n vertreten

Dezernent*innen und sonstige Vorgesetzte mehrerer Bereiche

+ alle Berechtigungen ihrer*seiner Sachgebiete bzw. Bereiche

Der Transponder für in Ziff. 7.4 aufgeführte Mitarbeiter*innen ist 16 Stunden gültig.
Die Transponder der Mitarbeiter*innen des (Technischen Betriebsdienstes) müssen unbegrenzt gültig sein, um in Notsituationen (z.B. Stromausfall) jederzeit das Gebäude betreten zu können.

7.5 Wachdienst/Feuerwehr/Aufzugsnotrufdienstleister

Die Wachdienste, die Feuerwehr und der Aufzugsnotrufdienstleister erhalten den GHS der entsprechenden Liegenschaft.

Der Transponder des Wachdienstes ist 16 Stunden gültig.
Die Transponder der Feuerwehr und des Aufzugsnotrufdienstleisters sind unbegrenzt gültig.

7.6 Reinigungspersonal

Reinigungskräfte
- Zugang zu allen Räumen einer Liegenschaft, in der sie zu reinigen haben.

Ausgenommen hiervon sind sämtliche Technikräume, IT-Räume und Archive, die nur 2x jährlich mit Begleitung gereinigt werden und Sonderbereiche, die nur von unterwiesenen Personen betreten werden dürfen. Hier erhalten nur die unterwiesenen Reinigungskräfte Zugang.

Der Transponder der Reinigungskräfte ist 16 Stunden gültig.

7.7 Mitarbeiter*innen Mensa

Die Mitarbeiter*innen der Mensa erhalten Zugang zu allen relevanten Küchenräumen und zum Speisesaal inkl. Zugangstüren und Außentüren.

Nachträgliche Anpassungen können sich aus Vorgaben des Studierendenwerkes ergeben.

Der Transponder für die Mitarbeiter*innen Mensa ist 16 Stunden gültig.

7.8 Externe Dienstleister*innen (Handwerker*innen, Lieferant*innen etc.)

Diese Personenkreise können bei Bedarf einen zeitlich begrenzten Zugang zu den erforderlichen Bereichen bekommen.

Die Transponder können täglich im zuständigen Sachgebiet des Dezernats 7 abgeholt werden und müssen vor dem Verlassen der Hochschule wieder zurückgegeben werden. Für die Rückgabe gibt es einen Schlüsselrückgabekasten.

Die Transponder für externe Dienstleister*innen sind 12 Stunden gültig.

8. Beantragung und Transponderausgabe

Jede zutrittsberechtigte Person erhält kostenfrei einen Transponder. Die Ausgabe des Transponders erfolgt gegen Unterschrift im zuständigen Sachgebiet des Dezernats 7.

Die Ausgabe ist vorab von der*dem Raumverantwortlichen per E-Mail zu beantragen.
Die E-Mail ist an die folgende Adresse zu richten:
Standort Iserlohn: schliessberechtigungen-iserlohn@fh-swf.de
Standort Soest: schliessberechtigungen-soest@fh-swf.de
Die Anträge und Ausgaben der Transponder und Schließberechtigungen sind im zuständigen Sachgebiet des Dezernats 7 zu dokumentieren.

9. Aktivierungsterminals

Nach der Ausgabe des Transponders, bei Berechtigungsänderungen sowie nach Ablauf seiner Gültigkeitsdauer muss der Transponder neu aktiviert werden. Dies erfolgt an einem der Aktivierungsterminals, welche sich an den Außentüren befinden.

Eine Übersicht aller Aktivierungsterminals befindet sich in der Anlage 2.

10. Verlust des Transponders

10.1 Verlust durch Mitarbeiter*innen und Studierende der FH SWF

Der Verlust des Transponders ist unverzüglich der*dem Raumverantwortlichen sowie dem zuständigen Sachgebiet des Dezernats 7 zu melden.

Es müssen daraufhin folgende Sicherheitsmaßnahmen ausgeführt werden:

1. Es wird vom zuständigen Sachgebiet des Dezernats 7 ein neuer Transponder erstellt und zusammen mit einer Liste der vom Verlust betroffenen Türen an die*den Mitarbeiter*in ausgehändigt.

2. Die*der Mitarbeiter*in ist verpflichtet, den neuen Transponder umgehend an einem Aktivierungsterminal zu aktivieren.

Der Verlust des Transponders wird dem*der Mitarbeiter*in / Studierenden zum jeweils geltenden Selbstkostenpreis in Rechnung gestellt (z.Zt. 25 EUR).

10.2 Verlust durch Wachdienst/Feuerwehr/Reinigungskräfte/Mensa/Externe Dienstleister*innen

Der Verlust des Transponders ist unverzüglich dem zuständigen Sachgebiet des Dezernats 7 zu melden. Dieses wird alle notwendigen Sicherheitsmaßnahmen veranlassen.

Der Verlust des Transponders (Ersatzbeschaffung) sowie zusätzlich der zeitliche Aufwand des zuständigen Sachgebiets des Dezernats 7 für die Neuprogrammierung der Türen werden dem Unternehmen mit 40 EUR brutto/ je angefangene Stunde in Rechnung gestellt.

11. Datenschutz

Der*die Kanzler*in stellt sicher, dass die datenschutzrechtlichen Grundsätze gem. Art. 5 DSGVO eingehalten werden und sorgt für die entsprechenden organisatorischen und technischen Maßnahmen (s. Anlage 3 und VVT).

Betroffene Personen stehen die sogenannten Betroffenenrechte gem. Art. 12 ff. DSGVO zu:

Recht auf Auskunft, Berichtigung und ggf. Vervollständigung;

Recht auf Datenübertragbarkeit, sodass die konkreten Daten in einem geeigneten Format zur Verfügung gestellt werden, sofern die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden.

Recht auf Widerspruch, aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben. Die Verarbeitung kann dann nur aus zwingenden schutzwürdigen Gründen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder wegen der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen fortgesetzt werden.

Recht auf Löschung, falls die erhobenen Daten für die angegebenen Zwecke nicht mehr notwendig sind, falls ein berechtigter Widerspruch eingelegt wird, falls die Daten unrechtmäßig gespeichert wurden oder falls die Löschung nach rechtlicher Verpflichtung erforderlich ist;

Recht auf Einschränkung der Verarbeitung, soweit die Richtigkeit bestritten wird, die Verarbeitung unrechtmäßig ist, eine Löschung abgelehnt wurde, die Daten nicht mehr für die Verarbeitungszwecke benötigt werden oder ein Widerspruch eingelegt wurde.

Eine automatisierte Einzelentscheidung nach Art. 22 DSGVO, insbesondere ein Profiling findet nicht statt.

Der Kreis der im Dezernat 7 zugriffsberechtigten Personen für die Verwaltungsdaten der Schließanlage (Managementsystem) wird unter Beachtung der Zweckbestimmung festgelegt. Der Zugriff auf die Daten durch unberechtigte Dritte ist durch technische und organisatorische Maßnahmen zu verhindern (s. Anlage 3).

11.1 Auslesen der Schließungen

Grundsätzlich erfolgt keine Zutrittskontrolle und keine Speicherung von Schließungen/Ereignissen.

Ausgenommen hiervon bleiben Gebäudeaussentüren, bei diesen erfolgt eine Speicherung der Schließereignisse für die Dauer von 7 Tagen. Sofern im Bedarfsfall (s. 2. Zweckbestimmung) ein Auslesen erforderlich wird, erfolgt dies mit einem Lesegerät am Schloss. Hierbei zeigt das Lesegerät keine Daten an. Die Anzahl der auszulesenden Ereignisse kann am Lesegerät begrenzt werden. Das Lesegerät wird anschließend mit der Software gekoppelt, um die Ereignisse zu übertragen. Erst in einem weiteren Schritt kann eine Zuordnung zwischen Transponder-ID und Person, nur durch ein zweigeteiltes Passwort (Admin/ Personalrat), gemeinsam vorgenommen werden.

11.2 Rechte der Beschäftigten

Mit Aushändigung des Transponders sind der*dem Beschäftigten Rechte und Pflichten durch das Gebäudemanagement mitzuteilen.

Jede Person erhält auf Antrag schriftlich oder elektronisch Informationen über alle auf dem Transponder und in der Managementsoftware zu ihrer*seiner Person aktuell gespeicherten Daten. Darüber hinaus besteht für die*den Raumverantwortliche*n die Möglichkeit, Auskunft über die Schließberechtigten zu den Räumen im eigenen Verantwortungsbereich zu erhalten.

Personelle Maßnahmen, die auf Informationen beruhen, die unter Verletzung dieses Konzepts gewonnen wurden, sind unwirksam und rückgängig zu machen.

11.3 Rechte der Personalräte und der*des Datenschutzbeauftragten

Die Personalräte und die*der Datenschutzbeauftragte haben das Recht, die Einhaltung dieses Konzepts zu überprüfen und zu diesem Zweck Stichproben zu machen. Dazu ist ihnen nach vorheriger Anmeldung der erforderliche Zugang zu allen Stellen unter Beteiligung der Dienststelle zu gewähren, an denen Komponenten der Schließanlage installiert sind und/oder Daten für die Schließanlage erhoben, gespeichert, verarbeitet und/oder genutzt werden.

Die Personalräte und die*der Datenschutzbeauftragte können nach vorheriger Anmeldung auf allen Ebenen des Managementsystems die vereinbarte Verwendung und die Einhaltung des Datenschutzes unter Beteiligung der Dienststelle kontrollieren. Dazu können sie auch in alle vom Managementsystem gespeicherten Daten und Protokolle Einblick nehmen. Alle zum Managementsystem gehörenden Handbücher und Systemunterlagen sind ihnen auf Wunsch in der aktuellen Version zeitweise zu überlassen.

Die Personalräte und die*der Datenschutzbeauftragte haben das Recht, alle Personen, die mit der Verarbeitung und Nutzung von Daten des Managementsystems beschäftigt sind unter Beteiligung der Dienststelle, bezüglich der rechtmäßigen, vereinbarten Verwendung zu befragen. Diese sind gegenüber den Personalräten zur wahrheitsgemäßen Auskunft berechtigt und verpflichtet. Auf Verlangen haben sie Funktionen zu Prüfzwecken vorzuführen.

Die Rechte aus Punkt 11.3 Unterabsatz 1-3 können von den Personalräten und der*dem Datenschutzbeauftragten unter Beteiligung der Dienststelle ausgeübt werden.

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

Bei Zugriff auf den Datenbestand um Zutritts- und Begehungslisten auszulesen, werden die Personalräte und die*der Datenschutzbeauftragte durch die Dienststelle informiert (s. Anlage 3).

Anlage 1

Die Standorte untergliedern sich in folgende Liegenschaften:

Standort Iserlohn

Frauenstuhlweg 31 – Campus
Baarstr. 5 – Etagenanmietung für die Verwaltung
Baarstr. 6 – Hauptsitz Hochschulverwaltung

Standort Soest

Lübecker Ring 2, - Campus
Welver-Merklingsen, Im Südfeld 1 - Versuchsgut
Arnsberger Str. 7 – Raumanmietung FB M-A
Detmolder Straße 7
Mawicker Str. 3, Ense- Gerlingen - Versuchsgut

Anlage 2

Aufstellorte der Aktivierungsterminals:

Standort Iserlohn

Frauenstuhlweg

H-Gebäude, Haupteingang, Außen neben der Eingangstür
Z-Gebäude, Eingang gegenüber K-Gebäude, Außen neben der Eingangstür
K-Gebäude, Eingang gegenüber C-Gebäude, Außen neben der Eingangstür
LFM-Gebäude, Außen neben der Eingangstür

Baarstraße

Baarstraße 6, Haupteingang, Außen neben der Eingangstür
Baarstraße 5, Haupteingang, Außen neben der Eingangstür

Standort Soest

Lübecker Ring

Gebäude 1, Außen neben der Eingangstür 01-1
Gebäude 2, Außen neben der Eingangstür 02-1
Gebäude 3, Außen neben der Eingangstür 03-2
Gebäude 4, Außen neben der Eingangstür 04-2
Gebäude 6, Außen neben der Eingangstür 06-1
Gebäude 9, Außen neben Feuerwehrschlüsselkasten
Gebäude 12, Außen neben der Eingangstür 12-1
Gebäude 13, Außen neben der Tür 13-2
Gebäude 14, Außen neben der Eingangstür 14-2
Gebäude 20, Außen neben der Eingangstür 20-2

Welver-Merklingsen

Gebäude 1, Außen neben der Eingangstür

Detmolder Straße

Gebäude 25, Außen neben der Eingangstür

Ense-Gerlingen

Außen neben der Eingangstür

Anlage 3

Organisation Zugriffsberechtigte

Die Zutritts- und Begehungslisten dürfen nur nach Eintritt oder zur Verhinderung eines (potentiellen) Schadensereignisses nach Entscheidung durch den*die Kanzler*in oder im Vertretungsfall durch die*den Verwaltungsdirektor*in im Einvernehmen mit den Personalräten und der*s Datenschutzbeauftragten in protokollierter Zusammenarbeit mit den Anlagenbediener*innen des Dezernates 7 eingesehen werden.

Je Standort sind zwei Anlagenbediener*innen des Dezernats 7 vorgesehen, deren Zuständigkeit sich aus dem Geschäftsverteilungsplan ergibt.

Die Einsichtnahme in die hinterlegten Daten ist durch ein mind. achtstelliges Passwort (entsprechend der Passwort Policy der FH SWF) geschützt. Das für den jeweiligen Standort bestimmte Passwort besteht aus zwei min. vierstelligen Teilpasswörtern, die nur im Zusammenhang funktionieren. Die beiden Teilpasswörter sind organisatorisch zum einen den Anlagenbediener*innen eines Standorts und zum anderen den Personalräten zugeordnet.