MITTEILUNGSBLATT

DER

Medizinischen Universität Innsbruck

Internet: http://www.i-med.ac.at/mitteilungsblatt/

Studienjahr 2011/2012 | Ausgegeben am 21. März 2012 | 26. Stück

Das Mitteilungsblatt erscheint jeweils am 1. und 3. Mittwoch jeden Monats.
Eigentümer, Herausgeber, Vervielfältigung, Vertrieb und für den Inhalt verantwortlich:
Univ.-Prof. Dr. Herbert Lochs, Rektor der Medizinische Universität Innsbruck, Innrain 52, A-6020 Innsbruck.

106. Betriebsvereinbarung „Zutrittskontrollsysteme“

gem. § 96a Abs. 1 Z 1 Arbeitsverfassungsgesetz (ArbVG), § 9 Abs. 2 lit. f Bundes-Personalvertretungsgesetz (PVG) und der Rahmenbetriebsvereinbarung über die Verwendung personenbezogener Daten über die Einführung und den Betrieb eines oder mehrerer Zutrittskontrollsysteme,

abgeschlossen zwischen

1. der Medizinischen Universität Innsbruck als Arbeitgeberin, vertreten durch das Rektorat, und
2. als Arbeitnehmer/innen/vertretung
   a. dem Betriebsrat für das wissenschaftliche Personal an der Medizinischen Universität (§ 135 Abs. 4 UG 2002) und
   b. dem Betriebsrat für das allgemeine Universitätspersonal der Medizinischen Universität Innsbruck (§ 135 Abs. 5 UG 2002).

Präambel

(1) Zwischen den Vertragsparteien besteht Übereinstimmung darüber, dass es der Universität möglich sein muss, besonders schutzbedürftige Räume und Anlagen (EDV-Räume, Tierversuchsräume, Hörsäle, Seminarräume, Seziersäle, Leichenräume, Parkplätze, etc.) mit elektronischen Zutrittssystemen auszustatten und in weiterer Folge auch rekonstruieren zu können, wer zu welchem Zeitpunkt unter Verwendung des Identifikationsmedium (z.B. Karte oder Schlüssel) eine oder mehrere Räumlichkeiten betreten hat.
(2) Die Zutrittskontrollsysteme sollen soweit irgend möglich den Umfang der Musteranwendung MA002 Zutrittskontrollsysteme gem. Standard- und Muster-Verordnung 2004 (StMV 2004), BGBl. II Nr. 312/2004, nicht überschreiten.
(3) Alle Vertragspartner anerkennen ihre gesetzlichen Verpflichtungen bezüglich des Datenschutzes (DSG 2000, StGB, etc.) und bekennen sich zu einem verantwortungsvollen Umgang mit personenbezogenen Daten.

§ 1 Zielsetzung

(1) Die Medizinische Universität Innsbruck setzt Zutrittskontrollsysteme ein, um die Sicherheit der Mitarbeiterinnen, Mitarbeiter und Studierenden der Universität zu gewährleisten, das Eigentum, die Infrastruktur, Versuchstiere, etc. vor Beschädigung, Einbruch und Diebstahl sowie schädigendem Verhalten zu schützen.
(2) Die Installierung und der Betrieb eines oder mehrerer Zutrittskontrollsysteme soll gewährleisten, dass der Zutritt (die Zufahrt) zu Bereichen der Medizinischen Universität Innsbruck ständig oder zu bestimmten Zeiten auf autorisierte Personen beschränkt werden kann.
(3) Übereinstimmung besteht auch darüber, dass durch den Einsatz eines oder mehrerer Zutrittskontrollsysteme die Menschenwürde der Mitarbeiterinnen und Mitarbeiter der Universität nicht verletzt und nur im geringst möglichem Ausmaß berührt werden darf. In diesem Zusammenhang sichert die Medizinische Universität zu, dass durch den Einsatz eines oder mehrerer Zutrittskontrollsysteme keinerlei unmittelbare oder mittelbare Leistungskontrolle oder Zeiterfassung der Mitarbeiterinnen und Mitarbeiter der Medizinischen Universität Innsbruck erfolgen wird.

§ 2 Geltungsbereich

(1) Diese Betriebsvereinbarung gilt
   a. persönlich für alle von den abschließenden Betriebsräten vertretenen Arbeitnehmerinnen und Arbeitnehmern der Medizinischen Universität Innsbruck und des Amtes der Medizinischen Universität Innsbruck.
      Nicht vom Anwendungsbereich erfasst sind Studierende und sonstige Personen, (z.B. Fremdfirmen) die über ein Identifikationsmedium an der Medizinischen Universität Innsbruck verfügen;
   b. sachlich für die Verwendung von Stamm- und Bewegungsdaten von Zutrittskontrollsystemen an der Medizinischen Universität Innsbruck.
   c. Zeitlich: siehe § 16.

Systemdarstellung

§ 3 Befassung der innerbetrieblichen Datenschutzkommission

(1) Wie in der „Rahmenbetriebsvereinbarung über die Verwendung personenbezogener Daten“ vorgesehen, ist der innerbetrieblichen Datenschutzkommission der Medizinischen Universität Innsbruck (i-med.dsk) jede Neueinführung und wesentliche Änderung einer Datenanwendung und damit jede Neueinführung und wesentliche Änderung eines Zutrittsystems zu melden. Die Inhalte ergeben sich aus der Checkliste für Informationsaufbereitung nach Anhang 2 der „Rahmenbetriebsvereinbarung über die Verwendung personenbezogener Daten“.
(2) In Bezug auf Zutrittssysteme hat die in Anhang 2 der „Rahmenbetriebsvereinbarung über die Verwendung personenbezogener Daten“ vorgesehene Projektbeschreibung insbesondere folgende Informationen zu enthalten:
    a. Die zum Einsatz kommenden Systeme und Programme;
    b. die Standorte der einzelnen Elemente der Zutrittssysteme und der zugehörigen Peripheriegeräte. (z. B.: Videoüberwachung, Aufzeichnungsgeräte, etc.);
    c. die Parametrisierung (Öffnungszeiten der Türen, Schranken, Berechtigungen, etc.);
    d. die zur Anwendung kommenden Auswertungen (Listen auf Bildschirm, Listen für Druckerausgaben u.ä.);
    e. die Aufbewahrungsdauer der erfassten Daten;
    f. die zugriffsberechtigten Mitarbeiterinnen und Mitarbeiter des Zutrittssystems inklusive der jeweiligen Berechtigungen (z.B. Vollberechtigung, Teilberechtigung für nur gewisse Parameter, etc.);
    g. die beabsichtigte Datenübermittlung aus anderen Datenanwendungen in die zu meldende Datenanwendung.

§ 4 Hard- und Softwareausstattung

(1) Die zum Einsatz kommenden Programme/Systeme inkl. Systembeschreibungen sind jeweils im Meldungsformular bzw im Anhang 1 zum Meldungsformular einvernehmlich von den Vertragspartnern anzuführen.
(2) Die technische Anknüpfung der Zutrittsterminals bzw Schlösser mit den jeweiligen Steuerrechnern ist zu beschreiben.
(3) Die Aufstellungsorte der einzelnen Zutrittskontrollsysteme und der dazugehörigen Terminals/Schlösser sind im Meldungsformular bzw in dessen Anhang 6 zu dokumentieren.
(4) Die Parametrisierung jedes einzelnen Terminals (Türöffnungszeiten, Berechtigungen, Meldungen, etc.) ist im Meldungsformular bzw im Anhang 7 zum Meldungsformular ersichtlich zu machen.
(5) Die Parametrisierung am jeweiligen PC/Laptop muss die gleichen Werte aufweisen, wie die Parametrisierung der dazugehörigen Terminals/Schlösser.
(6) Abänderungen, mit Ausnahme der eigentlichen Zugangsberechtigung, bedürfen der Zustimmung der innerbetrieblichen Datenschutzkommission.

§ 5 Verarbeitete Daten

(1) Die verarbeiteten Daten der einzelnen Zutrittskontrollsysteme sind im Meldungsformular bzw im Anhang 2 zum Meldungsformular taxativ aufzulisten. Werden codierte Schlüssel verwendet, so sind diese zu erläutern.
(2) Fotos, die im Rahmen der Zutrittskontrollsysteme Verwendung finden, dürfen explizit nur mit schriftlicher Zustimmung der/des Betroffenen für andere Zwecke verwendet werden.
(3) Der gesamte Datenbestand des jeweiligen Zutrittskontrollsystems wird nur mit dem im Meldungsformular resp. im Meldungsformular
(4) Meldungsformular, Anhang 1 des Meldungsformulars beschriebenen System verarbeitet.
(5) (4) Der Datenbestand der Zutrittskontrollsysteme inkl. der Datensicherung ist vor einer nachträglichen Veränderung der Daten nach dem aktuellen Stand der Technik zu schützen.

§ 6 Zugriffsberechtigungen

Die zugriffsberechtigten Mitarbeiterinnen und Mitarbeiter sind für jedes Zutrittskontrollsystem getrennt im Meldungsformular bzw im Anhang 3 des Meldungsformulars mit ihren Berechtigungen taxativ anzuführen.

§ 7 Datenspeicherung

(1) Alle erfassten Bewegungsdaten der Zutrittskontrollsysteme sind nach vier Monaten aus dem jeweiligen System zu löschen. Eine längerfristige Speicherung ist nur im begründeten Einzelfall (§ 12 Abs 1) und nur mit vorheriger Befassung und nachweislicher Zustimmung der Betriebsräte und der innerbetrieblichen Datenschutzkommission zulässig.
(2) Alle in Zusammenhang mit den Zutrittskontrollsystemen ermittelten Daten werden für den Zeitraum von maximal vier Monaten gespeichert, spätestens mit 5. des nachfolgenden Monats sind die Daten des ältesten Monats zu löschen.
(3) Eine Übermittlung/Verarbeitung der Bewegungs- oder Protokolldaten an/durch andere Anwendungen ist unzulässig.
(4) Eine Auslagerung auf andere, insbesondere bewegliche Datenträger (Disketten, CD-ROMs, Streamer) ist - außer zum Zwecke der Datensicherung für den Zeitraum gem. § 7 (1) - unzulässig und vor nachträglichen Veränderungen zu schützen (vgl § 5 Abs 4).

§ 8 Datenverbund

(1) Zur Übernahme von Daten aus bereits bestehenden EDV-Systemen in die Zutrittssysteme kann eine vorübergehende Vernetzung erfolgen. Diese Datenübertragung ist als Datentransfer zum jeweiligen Zutrittskontrollsystem zu gestalten und diese Schnittstelle(n) sind im Meldungsformular bzw im Anhang 4 zum Meldungsformular zu dokumentieren.
(2) Auslagerungen und Übernahmen von Daten aus dem jeweiligen Zutrittskontrollsystem auf andere EDV-Systeme erfolgen nicht. Auf den aufgebauten Datenstock des jeweiligen Zutrittskontrollsystems wird nur über das jeweilige, gemäß dieser Betriebsvereinbarung beschriebene System durch die lt. § 6 autorisierten Personen unter Anwendung von §12 dieser BV zugegriffen.

§ 9 Datenausgabe

Die zur Anwendung kommenden Auswertungen (Listen auf Bildschirm, Listen für Druckerausgaben) sind im Meldungsformular bzw im Anhang 5 zum Meldungsformular zu beschreiben. Den Betriebsräten ist jederzeit Zugang zu den erfolgten Auswertungen gewähren.

§ 10 persönliche Karte/ codierter Schlüssel

(1) Zutrittssysteme kommen grundsätzlich als „Schlüsselsysteme“ zur Anwendung, d.h. die Berechtigungen der Mitarbeiterinnen und Mitarbeiter werden nur überprüft und Zutritte nicht aufgezeichnet.
(2) Abweichend von Abs. 1 ist eine Aufzeichnung der Zutritte zulässig, wenn glaubhaft gemacht werden kann, dass dies zur Zielerreichung notwendig ist. Dazu sind entsprechende Beschlüsse der Betriebsräte und der i-med.dsk notwendig.
(3) Zur Bedienung des Zutrittskontrollsystems erhält jede Mitarbeiterin bzw jeder Mitarbeiter ein persönliches Identifikationsmedium oder mehrere persönliche Identifikationsmedien (z.B. Karte, Chip, Schlüssel, etc.).
(4) Bei Verlust oder bei Beschädigung/Bruch eines Identifikationsmediums ist die Arbeitgeberin bzw die zuständige Abteilung unverzüglich in Kenntnis zu setzen und eine Verlustmeldung bei der Behörde zu erstatten.
(5) Bei Auflösung des Dienstverhältnisses sind die Identifikationsmedien am letzten Arbeitstag bei der Arbeitgeberin bzw der ausgebenden Stelle zurückzugeben.

§ 11 System- und Anwendungsänderungen

Jegliche Veränderung – ausgenommen sind Listen- und Maskenlayoutveränderungen – ist der innerbetrieblichen Datenschutzkommission zur Genehmigung vorzulegen und gemäß dieser Betriebsvereinbarung zu dokumentieren. Die Arbeitgeberin hat die erste Meldung an das Datenverarbeitungsregister abschriftlich den Betriebsräten zur Kenntnis zu bringen.

§ 12 Auswertung von Bewegungsdaten

(1) Eine Auswertung der Bewegungsdaten aus Zutrittssystemen findet auf Ersuchen der betroffenen Mitarbeiterin oder des betroffenen Mitarbeiters, zur Analyse und Korrektur von technischen Problemen oder bei Verdacht auf unberechtigten Zutritt, Zutrittsversuch, Zufahrt oder eine strafbare Handlung statt. Einem Verdacht wird nur nachgegangen, wenn
   a. ein Verlust eines Identifikationsmediums gemeldet wurde bzw der Verbleib eines solchen nicht geklärt werden konnte;
   b. Eigentum der Medizinischen Universität oder der Mitarbeiterinnen oder Mitarbeiter abhanden gekommen oder beschädigt worden ist;
   c. bewegliche Sachen, die sich im Gewahrsam der Medizinischen Universität oder der Mitarbeiterinnen und Mitarbeiter befinden, abhanden gekommen oder beschädigt worden sind;
   d. deutliche Hinweise auf einen Einbruch oder Einbruchsversuch oder eine andere strafbare Handlung vorliegen.

(2) Im Verdachtsfall sind das Rektorat und der zuständige Betriebsrat (unverzüglich) zu informieren. Die Auswertung der Bewegungsdaten erfolgt auf Wunsch einer der beiden und im Beisein beider Seiten. Der nicht betroffene Betriebsrat und die innerbetriebliche Datenschutzkommission sind zu informieren.

(3) Jede Einsichtnahme in Aufzeichnungen personenbezogener Bewegungsdaten der Zutrittssysteme ist unter Angabe der Einsicht nehmenden Personen, des Datums und des Grundes der Einsichtnahme zu protokollieren, Den Betriebsräten ist jederzeit Einsicht in die Protokolle zu gewähren. Die Arbeitgeberin informiert die Betriebsräte vierteljährlich automatisch über erfolgte Einsichtnahmen.

(4) Zur Überprüfung der ordnungsgemäßen Verwendung der Daten (iSd § 14 DSG 2000) ist dreimal jährlich eine routinemäßige Kontrolle der Protokolldaten durchzuführen. Diese ist durch die oder den Datenschutzbeauftragte/n – soweit bestellt – oder sonst durch die innerbetriebliche Datenschutzkommission zu initiieren und erfolgt durch eine/n Systemadministrator/in. Die oder der Datenschutzbeauftragte – soweit bestellt – oder die/der Vorsitzende der Kommission hat den Termin zur routinemäßigen Kontrolle sowohl mit den Betriebsräten als auch mit dem zuständigen Rektoratsmitglied zu koordinieren; jede Seite hat das Recht, eine/n Vertreter/in zur Kontrolle zu entsenden. Es sind zumindest die Protokolle eines Monats, höchstens aber jene seit der letzten Kontrolle zu sichten.

(5) Soweit eine Auswertung der Bewegungsdaten nicht auf Ersuchen einer Mitarbeiterin oder eines Mitarbeiters erfolgt ist, so ist die betroffene Mitarbeiterin oder der betroffene Mitarbeiter nachweislich und unverzüglich über die erfolgte Auswertung und deren Ergebnis in Kenntnis zu setzen, soweit und sobald nicht zwingende Gründe der Strafverfolgung dagegen sprechen.

§ 13 Meldungsformular samt Anhängen 1-7

Das zu verwendende Meldungsformular samt dessen Anhängen 1-7 ist als Anhang Bestandteil dieser Betriebsvereinbarung.

§ 14 Rechte der Belegschaft

(1) Die betroffenen Arbeitnehmer und Arbeitnehmerinnen sind unter Fortzahlung des Entgeltes während der Arbeitszeit über die technischen Grundzusammenhänge, Zweck und Wirkungsweisen des sie betreffenden Zutrittskontrollsystems, sowie über die Regelungen dieser Betriebsvereinbarung zu informieren.

(2) Personelle Konsequenzen, die auf Informationen beruhen, die unter Verletzung dieser Betriebsvereinbarung gewonnen werden, sind rechtsunwirksam.

§ 15 Rechte der Betriebsräte

(1) Jeder Betriebsrat für sich hat bzw die Betriebsräte gemeinsam haben das Recht, jederzeit die Einhaltung der Betriebsvereinbarung zu kontrollieren und Auskünfte über die einzelnen Zutrittskontrollsysteme zu erhalten.

(2) Jeder Betriebsrat für sich hat bzw die Betriebsräte gemeinsam haben das Recht, sich jederzeit die Datenarten gem. § 5 bzw Anhang 2 der einzelnen Zutrittskontrollsysteme ausdrucken zu lassen.

(3) Um die notwendigen Qualifikationen zur Wahrnehmung ihrer Kontrollrechte zu erlangen, werden den Betriebsräten vom Arbeitgeber bzw der zuständigen Abteilung der zentralen Verwaltung geeignete Informationsmittel zur Verfügung gestellt.

(4) Jeder Betriebsrat für sich hat bzw die Betriebsräte gemeinsam haben weiters das Recht, während der Arbeitszeit unter Fortzahlung des Entgeltes an Anwenderschulungen bezüglich der einzelnen Zutrittskontrollsysteme teilzunehmen. Die Arbeitgeberin ist verpflichtet, jährlich Anwenderschulungen anzubieten. Diese Bildungsveranstaltungen sind nicht auf die Bildungsfreistellung anzurechnen.
(5) Darüber hinaus können die Betriebsräte Experten ihres Vertrauens zur Unterstützung beiziehen.

§ 16 Schlussbestimmungen

(1) Diese Vereinbarung wird befristet bis xx.xx.xxxx abgeschlossen und tritt nach Unterzeichnung und mit Veröffentlichung im Mitteilungsblatt der Medizinischen Universität in Kraft.
(2) Während dieser Zeit besteht eine Phase der beiderseitigen Prüfung der Anwendbarkeit dieser Betriebsvereinbarung, innerhalb derer – auf Wunsch einer Vertragsseite – ergänzende Gespräche mit dem Ziel einer einvernehmlichen Abänderungen geführt werden können.
(3) Sollte bis acht Wochen vor Ablauf der Befristung keine Vertragsseite gegenüber der anderen Vertragspartei ausdrücklich und schriftlich auf einem Auslaufen der Betriebsvereinbarung mit Fristende bestehen, verlängert sich die Betriebsvereinbarung um weitere zwölf Monate.

Innsbruck, am 20.03.2012

Für das Rektorat der Medizinischen Universität Innsbruck:

Univ.-Prof. Dr. Herbert Lochs
Rektor

Univ.-Prof. Dr. Doris Balogh
Vizerektorin für Personal, Personalentwicklung und Gleichbehandlung

Ao. Univ. Prof. Dr. Martin Tiefenthaler
Vorsitzender des BR für das wissenschaftliche Personal

ADir. Monika Viehweider
Vorsitzende des BR für das allgemeine Universitätspersonal

Anhang

Meldungsformular

Meldungsformular, Anhang 1: Systembeschreibung(en)

Meldungsformular, Anhang 2: Datenkatalog(e)

Meldungsformular, Anhang 3: Zugriffsberechtigungen

Meldungsformular, Anhang 4: Schnittstelle Personaldatenübergabe

Meldungsformular, Anhang 5: Auswertungen auf Bildschirm und Drucker

Meldungsformular, Anhang 6: Aufstellungsorte

Meldungsformular, Anhang 7: Terminalparametrisierung

Anhang zur Betriebsvereinbarung Zutrittskontrollsysteme an der Medizinischen Universität Innsbruck

Meldung eines Zutrittskontrollsystems
für

Haus / Department / Institut / Sektion

Zutrittskontrollsysteme an der Medizinischen Universität Innsbruck unterliegen insbesondere folgenden Rechtsgrundlagen:

1. Datenschutzgesetz 2000
2. § 96a Abs. 1 Z.1 Arbeitsverfassungsgesetz
3. § 9 Abs. 2 lit. f Bundes-Personalvertretungsgesetz
4. Rahmenbetriebsvereinbarung über die Verwendung personenbezogener Daten
5. Betriebsvereinbarung „Zutrittskontrollsysteme“

Bitte füllen Sie nur die fett umrandeten Felder aus!

Name, Telefonnummer und E-Mail-Adresse der Sachbearbeiterin/des Sachbearbeiters

Verantwortliche/Verantwortlicher

Akad.Grad/Titel	
Vorname Nachname	
Position	
Organisationseinheit	
Tel / Fax / E-Mail	
Datum, Unterschrift	

Hard- und Softwareausstattung
(Anhang 1 gemäß Betriebsvereinbarung „Zutrittskontrollsysteme“)

Hersteller:	
Name des Schließsystems:	
Verwendete Software:	
Beilagen:	
Sonstige Angaben:	

Verarbeitete Daten
(Anhang 2 gemäß Betriebsvereinbarung „Zutrittskontrollsysteme“)
Die vorgegebene nummerierte Aufzählung entspricht den Angaben der Musteranwendung „MA 002 Zutrittskontrollsysteme“.
Bitte kreuzen Sie nur die verwendeten Datenarten an; Ergänzungen fügen Sie bitte unten an.

Betroffene Personengruppen:		**Nr.**	**Datenarten:**	**Empfängerkreise**
Zutrittsberechtigte	☐	01	Ordnungsnummer	–
	☐	03	Vor- und Familienname, akad. Grad/Standesbezeichnung	–
	☐	04	Geschlecht	–
	☐	05	Beziehung des Betroffenen zum Auftraggeber (Mitarbeiter, Kunde, sonstiger Besucher)	–
	☐	06	Telefon-, Faxnummer, und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben, sofern die zur raschen Verständigung des Betroffnen erforderlich ist	–

	☐	07	Lichtbild des Betroffenen, sofern die als zusätzliche Sicherheitsmaßnahme erforderlich ist	–
	☐	08	Zutrittscode	–
	☐	09	Vom Berechtigten einzugebender Berechtigungscode	–
	☐	10	Daten der Zutrittsberechtigung, insbesonders die Bereiche und Zeiten, für die die Berechtigung gilt, die Sicherheitsstufe, ebenso besondere Befugnisse wie z.B. das Recht, mit einem Fahrzeug in den geschützten Bereich einzufahren	–
	☐	11	Gültigkeitsdauer der Zutrittsberechtigung	–
	☐	12		
	☐	13		
	☐	14		
	☐	15		
	☐	16		

Beabsichtige Übermittlungen aus diesem Zutrittskontrollsystem
An wen (Empfängerkreis) und auf Grund welcher Rechtsgrundlage werden verarbeitete Daten übermittelt? (Werden Daten an Empfänger im Ausland weitergegeben, ist zusätzlich der Empfängerstaat anzuführen.)
Falls das Zutrittskontrollsystem die Teilnahme an einem Informationsverbundsystem darstellt, ist anzugeben, welche teilnehmenden Auftraggeber dem gleichen Informationsverbundsystem angehören.
Versehen Sie bitte für die Zuordnung der Übermittlungen (in der letzten Spalte „Verarbeitete Daten“) jeden Empfängerkreis mit einer fortlaufenden Nummer.

Empfängerkreis		Rechtsgrundlage für die Übermittlung
Nr.	Bezeichnung	

Zugriffsberechtigte Mitarbeiterinnen und Mitarbeiter
(Anhang 3 gemäß Betriebsvereinbarung „Zutrittskontrollsysteme“)

Akad.Grad/Titel	Vorname	Nachname	Organisationseinheit	Kontakt (Tel, Fax, E-Mail)

Datenverbund zur Datenübernahme
(Anhang 4 gemäß Betriebsvereinbarung „Zutrittskontrollsysteme“)

☐ Eine Datenübernahme aus bereits bestehenden EDV-Systemen findet nicht statt.
☐ Eine Datenübernahme aus bereits bestehenden EDV-Systemen findet statt. Details der Schnittstelle:

Datenausgabe
(Anhang 5 gemäß Betriebsvereinbarung „Zutrittskontrollsysteme“)
Die zur Anwendung kommenden Auswertungen (Listen auf Bildschirm, Listen für Druckerausgaben) als Bildschirmausdruck/Musterausdruck beilegen.

	Liegen bei	Liegen nicht bei
Bildschirmausdrucke	☐	☐
Musterausdrucke	☐	☐

Standorte und Parametrisierung
(Anhänge 6 und 7 gemäß Betriebsvereinbarung „Zutrittskontrollsysteme“)

Typ (Kamera, Schloss, Terminal, etc.)	**Standort**	**Parameter**				
		Türoffen-/Betriebeszeiten	Berechtigungen	Meldungen		

Stellungnahme der i-med.dsk

☐	Das gegenständliche System unterliegt der Musteranwendung „MA 002 Zutrittskontrollsysteme“
☐	Das gegenständliche System unterliegt nicht der Musteranwendung „MA 002 Zutrittskontrollsysteme“. Das System ist vor Inbetriebnahme beim Datenverarbeitungsregister (DVR) zu melden.
	Datum, Unterschrift

Zustimmung der Betriebsräte
gem. § 96a Abs. 1 Z. 1 ArbVG und § 9 Abs. 2 lit. f PVG

	JA	NEIN	Beschluss vom	Unterschrift
Betriebsrat für das wissenschaftliche Personal	☐	☐		
Betriebsrat für das allgemeine Personal	☐	☐		