

Datenschutz- und Informationssicherheitskonzept der BITMARCK

Fachkonzept

Version: 6

Stand: 09.09.2025

Klassifizierung: A0 - Öffentlich

Dokumentenverantwortliche(r):

Hennemann, Matthias; Eller, Martin; Ohnesorg, Patrick; Ahmadi, Tareq;

Codierung: FK-00066 - BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK

Dokumentinformationen

Klassifizierung	A0 - Öffentlich	Gültig bis	09.09.2027
		Status	Gültig
Dateiname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BIT-MARCK		

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

Inhaltsverzeichnis

Dokumentinformationen	2
1 Einleitung und Rahmenbedingungen	4
1.1 Wirkungsbereich	4
1.2 Verantwortliche Ansprechpartner	5
1.3 Überwachung der Durchführung	5
2 Technische und organisatorische Maßnahmen	6
2.1 Zutrittskontrolle	7
2.2 Zugangskontrolle	8
2.3 Zugriffskontrolle	9
2.4 Weitergabekontrolle	10
2.5 Eingabekontrolle	11
2.6 Auftragskontrolle	11
2.7 Verfügbarkeitskontrolle	11
2.8 Trennungsgebot	12
3 Weitere Maßnahmen	13
3.1 Maßnahmenbereich Personal	13
3.1.1 Einarbeitung neuer Mitarbeitender ^{(v)(i)(b)}	13
3.1.2 Datenschutz- und Geheimhaltungsverpflichtung ^{(v)(b)}	13
3.1.3 Regelmäßige Informationen ^{(a)(b)}	13
3.1.4 Verfahrensweise beim Ausscheiden von Mitarbeitenden ^{(v)(b)}	13
3.2 Datenschutzmanagement	14
3.3 Weitergehende Maßnahmen	14
3.3.1 Sichtschutz	14
3.3.2 Brandschutz	14
3.3.3 Allgemeine Sicherungsmaßnahmen	14
3.3.4 Systeme zur Angriffserkennung, Vorfallerkennung und -bearbeitung	14
3.4 Informationssicherheitsmanagementsystem (ISMS)	15

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

1 Einleitung und Rahmenbedingungen

Die folgenden sicherheitstechnischen Festlegungen repräsentieren, in Verbindung mit der Datenschutzleitlinie und der Informationssicherheitsleitlinie, das Datenschutz- und Informationssicherheitskonzept der BITMARCK.

Die BITMARCK legt hiermit die Standards fest, nach denen alle Formen von papiergebundenen und elektronischen Informationen während der Verarbeitung derselben behandelt, geschützt und gegebenenfalls, nach Erbringung der mit dem jeweiligen Kunden vereinbarten Dienstleistung, vernichtet werden.

Insbesondere setzt die BITMARCK den branchenspezifischen Sicherheitsstandard der gesetzlichen Krankenversicherung (B3S GKV/PV) in der jeweils gültigen Fassung um.

Im weiteren Verlauf werden die technischen und organisatorischen Maßnahmen beschrieben, die die BITMARCK an ihren Standorten durchführt, um die Anforderungen des B3S, des SGB, des BDSG, und des Art. 32 der DSGVO zu erfüllen.

In diesem Dokument werden unter dem Begriff „Daten“ alle sensiblen Daten verstanden, die im Rahmen der Auftragsverarbeitung verarbeitet werden. Hierbei handelt es sich insbesondere um personenbezogene Daten, Sozialdaten sowie sensible Betriebs- und Geschäftsgeheimnisse. Die hier festgelegten Standards gelten gleichermaßen bei der Verarbeitung sonstiger personenbezogener Daten im Unternehmen wie z.B. Personaldaten der Mitarbeitenden, Kunden- und Lieferantendaten.

1.1 Wirkungsbereich

Die folgenden Festlegungen werden für die gesamte Verarbeitung und somit für alle von der BITMARCK übernommenen Aufträge und Aufgaben umgesetzt.

Da aufgrund unterschiedlichster Auftragspezifikationen Aufträge mit verschiedenen Schutzbedarfen verarbeitet werden, ist der Wirkungsbereich der in diesem Dokument definierten Standards durch entsprechende Einzelvereinbarungen mit den Auftraggebern geregelt. Dies kann insbesondere dann der Fall sein, wenn Subunternehmer an der Leistungserbringung beteiligt sind.

Weiterhin können die Sicherheitsanforderungen auf Wunsch der Auftraggeber erhöht oder im Einzelfall auf ausdrückliche Anweisung des Auftraggebers verringert werden, soweit dies in einer Anlage zur entsprechenden Auftragsdokumentation von beiden Seiten schriftlich gefordert und bestätigt wird.

Eine Verringerung der Standards ist jedoch nur dann möglich, wenn die korrespondierenden gesetzlichen Regelungen nicht unterschritten werden.

Zweckentsprechende Erhöhungen der Sicherheitsstandards, die aus einzelnen Aufträgen resultieren, aber Einfluss auf die gesamte Verarbeitung von Daten innerhalb der BITMARCK haben, werden ohne weitere Genehmigung der einzelnen Auftraggeber im Gesamtinteresse

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

aller Auftraggeber umgesetzt und finden in einer Aktualisierung des vorliegenden Dokuments Berücksichtigung.

1.2 Verantwortliche Ansprechpartner

Die Gesamtverantwortung, insbesondere für die Festlegung und Umsetzung der Inhalte des Datenschutzkonzeptes, übernimmt die Geschäftsführung der BITMARCK. Überwachend und beratend unterstützen die Datenschutzbeauftragten, sowie die Informationssicherheitsbeauftragten.

1.3 Überwachung der Durchführung

Für die Durchführungsüberwachung sind die Datenschutzbeauftragten, die die Aufgaben gemäß Art. 39 DSGVO wahrnehmen, in Zusammenarbeit mit den Informationssicherheitsbeauftragten zuständig. Die Geschäftsführungen unterstützen bei der Umsetzung dieser Überwachungstätigkeiten.

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

2 Technische und organisatorische Maßnahmen

Die Schutzziele des Datenschutzes und der Informationssicherheit werden in der Leitlinie zur Informationssicherheit wie folgt definiert:

- **Verfügbarkeit**

Informationen müssen stets im erforderlichen Umfang zur Verfügung stehen.

Informationsverarbeitende Anwendungen samt zugehöriger Verfahren und Prozesse, sowie die zugehörige technische und räumliche Infrastruktur, müssen gegen organisationsbedingte, technische und umweltbedingte Ausfälle geschützt werden.

Dieses Schutzziel folgt auch unmittelbar aus dem B3s, sowie aus Art. 32 Abs. 1b der DSGVO.

- **Integrität**

Informationen werden nur in der vorgeschriebenen Verfahrensweise verarbeitet und dürfen nicht durch menschliches oder technisches Fehlverhalten oder vorsätzlich verfälscht, unberechtigt gelöscht oder zerstört bzw. manipuliert werden.

Informationsverarbeitende Anwendungen samt zugehöriger Verfahren und Prozesse müssen eine auftragskonforme und korrekte Verarbeitung sicherstellen.

Dieses Schutzziel folgt auch unmittelbar aus dem B3s, sowie aus Art. 32 Abs. 1b der DSGVO.

- **Vertraulichkeit**

Informationen müssen vor unbefugter Preisgabe geschützt werden. Geheimhaltungsvorschriften und Datenschutzvorgaben müssen eingehalten werden. Dies gilt insbesondere für die bei BITMARCK verarbeiteten Sozialdaten, wie auch für die daraus resultierenden Informationen über Geschäftsgeheimnisse der Kunden.

Dieses Schutzziel ergibt sich auch unmittelbar aus dem Sozialdatenschutz gemäß §35 SGB I sowie aus dem B3s und aus Art. 32 Abs. 1b der DSGVO.

- **Authentizität**

Authentizität ist der Zustand, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Dieses Schutzziel ergibt sich aus dem B3S, sowie §8a (1) BSIG und speziell für Kritis-Betreiber auch aus §7 Abs. 7 (2) BSI-KritisV.

Darüber hinaus ergibt sich aus Art. 32 Abs. 1b der DSGVO als weiteres Schutzziel die **Bestandbarkeit** (engl. Resilience), die von ihrer Ausprägung her jedoch nicht auf Informationen, sondern auf informationsverarbeitende Prozesse anzuwenden ist.

verantwortlich	Hennemann, Matthias; Eller, Martin; Ohnesorg, Patrick; Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

Weiterhin folgt aus Art. 32 Abs. 1a der DSGVO, dass als Maßnahmen zum Schutz der verarbeiteten Informationen **Pseudonymisierung** und **Verschlüsselung** zum Einsatz kommen sollen.

Im weiteren Verlauf werden die bei der BITMARCK zur Anwendung kommenden Maßnahmen aufgeführt. Die oben genannten Schutzziele und Maßnahmen werden hierbei wie folgt referenziert:

Schutzziel / Maßnahme	Abkürzung
Verfügbarkeit	(a)
Integrität	(i)
Vertraulichkeit	(v)
Belastbarkeit	(r)
Pseudonymisierung	(p)
Verschlüsselung	(e)
Authentizität	(t)
Branchenspezifischer Sicherheitsstandard (B3S)	(b)

2.1 Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Maßnahmen zur Zutrittskontrolle

- Alle Außentüren sind verschlossen. Ein Zutritt zu den Geschäftsräumen ist nur den zutrittsberechtigten Personen und Dritten nur in Begleitung einer zutrittsberechtigten Person möglich^{(v)(b)}.
- Alle Gebäude sind durch Einbruchmeldeanlagen gesichert, die Wachdiensten aufgeschaltet sind. Diese übernehmen auch die Überwachung der Gebäude außerhalb der Geschäftszeiten^{(v)(b)}.
- Die Zutrittsberechtigungen sind im Zutrittsberechtigungssystem hinterlegt. Zutritte erfolgen mit Hilfe von Token und unterliegen einer regelmäßigen Prüfung durch den Datenschutz- bzw. Informationssicherheitsbeauftragten^{(v)(t)(b)}.
- Der Zutritt zu den Datenverarbeitungsanlagen (Serverräumen) ist nur einem begrenzten Personenkreis möglich (z.B. Administratoren). Diese Zutritte erfolgen mit

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

Codekarten und Pin bzw. mit biometrischer Identifikation und unterliegen einer regelmäßigen Prüfung durch den Datenschutz- bzw. Informationssicherheitsbeauftragten^{(v)(a)(b)}.

- Für die Vergabe von Berechtigungen an Mitarbeitende sind die Vorgesetzten verantwortlich. Die Steuerung der Zutrittsberechtigungen und deren Entzug erfolgt zentral^{(v)(t)(b)}.
- Alle Zutritte werden protokolliert, so dass überprüft werden kann, wer zu welchem Zeitpunkt wo Zutritt hatte. Die Zutrittsregelung berücksichtigt den Zutritt in definierte Sicherheitszonen^{(v)(b)}.
- Für betriebsfremde Personen (z.B. Wartungspersonal, Besucher) bestehen Zutrittsregelungen. Sie sind nur mit Genehmigung, Protokollierung und Aushändigung von Ausweisen zugangsberechtigt. Die Zutrittsregelung ist in einer Richtlinie einheitlich für die BITMARCK geregelt^{(v)(t)(b)}.
- Die Einhaltung der Zutrittsschutzmaßnahmen wird im Rahmen interner Audits vom Datenschutzbeauftragten und dem Informationssicherheitsbeauftragten regelmäßig überprüft^{(v)(b)}.

2.2 Zugangskontrolle

Ziel der Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, nutzen können.

Maßnahmen zur Zugangskontrolle

- Alle Server und PC-Arbeitsplätze, die zur Verarbeitung personenbezogener Daten genutzt werden, sind in eigenständigen und segmentierten Netzwerken zusammengefasst^{(v)(t)(b)}.
- Alle Server und PC-Arbeitsplätze sind Zugangsgeschützt. Benutzer können auf gespeicherte Daten nur zugreifen oder Daten nur speichern, sofern sie dazu berechtigt sind^{(v)(i)(t)(b)}.
- Zur Anmeldung/Identifizierung gegenüber dem System muss der Benutzer seine UserID und sein persönliches Passwort eingeben^{(v)(t)(b)}.
- Passwörter haben mind. 12 Zeichen. In der Richtlinie Berechtigungsmanagement ist geregelt, wie die persönlichen Passwörter aller Mitarbeitenden zu gestalten sind. Nach 5 Fehleingaben erfolgt eine automatische, zeitlich begrenzte Sperrung. Für Zugriffe über unsichere Netze ist zusätzlich eine 2-Faktor-Authentifizierung obligatorisch^{(v)(b)}.
- Passwörter sind stets geheim zu halten^{(v)(b)}.

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

- PC-Arbeitsplätze müssen durch den Anwender beim Verlassen gesperrt werden. Mittels zentraler Domain Policies ist zudem festgelegt, dass die Sperre des Arbeitsplatzes nach spätestens 15 Minuten der Inaktivität des Arbeitsplatzes automatisch erfolgt ^{(v)(b)}.
- Sichere Konfiguration der Betriebssysteme: Nicht benötigte Software wird deinstalliert oder – falls nicht möglich, zum Beispiel bei Systemdiensten – deaktiviert. Dies gilt sowohl für Server als auch für die Clients ^{(a)(i)(r)(b)}.
- Unbenutzte Schnittstellen (USB, Firewire, E-SATA, PCMCIA) oder Laufwerke (CD, DVD, Blue-Ray, Speicherkarten-Slots) werden deaktiviert. Eine Freischaltung ist zu begründen und zu beantragen ^{(v)(r)(b)}.
- Der Internet-Zugang und das interne Netzwerk (Intranet) sind gegen ungewollte oder gezielte unberechtigte Zugriffe von außen abgeschottet (Firewall) und überwacht (EDR-Systeme, Systeme zur Angriffserkennung) ^{(v)(r)(b)}.
- Die Wirksamkeit der Maßnahmen zur Zugangskontrolle wird regelmäßig mit Hilfe von Schwachstellenscannern, internen wie externen Penetrationstests und regelmäßigen Red-Teaming Maßnahmen überprüft. ^{(v)(r)(b)}.
- Die Übertragungsleitungen sind abgesichert (siehe Punkt Weitergabekontrolle) ^{(v)(i)(b)}.

2.3 Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, zu gewährleisten, dass nur die zur Benutzung der Datenverarbeitungssysteme Berechtigten auf die jeweiligen personenbezogenen Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen zur Zugriffskontrolle

- Zugriffe erfolgen auf Basis von Rechte- und Rollenkonzepten ^{(v)(b)}.
- Die Zugriffskontrolle auf IT-Komponenten (Server, Rechner, etc.) erfolgt durch Benutzerkennungen und Passwörter, für Zugriffe über unsichere Netze ist zusätzlich eine 2-Faktor-Authentifizierung obligatorisch ^{(v)(t)(b)}.
- Berechtigungen sind in zentralen Verzeichnissen hinterlegt, wobei der Zugriff auf diese IT-Systeme selbst nur durch die besonders dazu berechtigten und autorisierten Personen erfolgen kann ^{(v)(t)(b)}.
- Zugriffe werden protokolliert ^{(i)(b)}.
- Ein administrativer Zugriff auf die Server ist nur mit gesonderter Authentifizierung der Benutzer möglich ^{(v)(i)(t)(b)}.

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

- Es bestehen beschränkte und maschinell kontrollierte Zugriffsrechte auf Software und Speichermedien durch Benutzerkennungen und Passwörter. Jeder Mitarbeitende erhält nur die Berechtigungen, die für die Erfüllung seiner Tätigkeiten erforderlich sind^{(v)(i)(b)}.
- Alle Systeme unterliegen einem geregelten Patch-Management^{(a)(i)(r)(b)}.

2.4 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen zur Weitergabekontrolle

- Bei der Weitergabe personenbezogener Daten über öffentliche Netze ist eine Verschlüsselung zwingend vorgesehen, dies kann zum Beispiel durch eine Verschlüsselung von Archivfiles (zip) mit starker Verschlüsselung (AES \geq 256 Bit) oder einer höheren Verschlüsselungsstufe durch eine PGP-Verschlüsselung realisiert werden. Insbesondere kommen die Richtlinien für den Datenaustausch im Gesundheits- und Sozialwesen (www.datenaustausch.de) zur Anwendung. Maßgebend ist die Kundenanforderung im Einzelfall, die ausdrücklich erfolgen muss^{(i)(v)(e)}.
- Der Datenaustausch zwischen den BITMARCK-Standorten erfolgt verschlüsselt und auf sicherem Weg (z. B. VPN, MPLS)^{(i)(v)(e)(t)(b)}.
- Alle Datenübertragungen werden protokolliert. Bei Dateneingang wird die Datenübertragung auf ihre Vollständigkeit und ihre Richtigkeit hin überprüft^{(i)(b)}.
- Es besteht eine differenzierte Datenverwaltung (Kunde; Projekt), um zu gewährleisten, dass die Daten sauber getrennt gehalten werden und damit keine Möglichkeit der Verwechslung, Vermischung oder zufälligen Löschung besteht^{(a)(i)}.
- Datenträger werden nur an autorisierte Personen übergeben^(v).
- Die datenschutzgerechte Entsorgung nicht mehr benötigter bzw. verwendeter Datenträger und Informationen sind durch zertifizierte Entsorgungsfachbetriebe gewährleistet^(v).
- Sofern Testumgebungen auf Basis von Echtdaten bestehen, sollen die Testdaten pseudonymisiert werden. Maßgebend ist in diesem Fall die Kundenanforderung^(p).

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

2.5 Eingabekontrolle

Ziel der Eingabekontrolle ist es, nachträglich feststellen zu können, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen zur Eingabekontrolle

- Das Einloggen in die Verarbeitungssysteme ist ausschließlich autorisierten Mitarbeitende möglich (Protokollierung in den Logfiles); die Authentifizierung der User erfolgt durch Benutzername und Kennwort^{(v)(t)}.
- Manuelle Änderungen an Daten erfolgen nur im Einzelfall und nur nach ausdrücklicher Beauftragung durch den Kunden⁽ⁱ⁾.

2.6 Auftragskontrolle

Ziel der Auftragskontrolle ist es zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen zur Auftragskontrolle

- Sämtliche Verträge, Auftragsbestätigungen liegen schriftlich vor und enthalten sämtliche Pflichten, Aufgaben und Vorgaben von Auftraggeber und Auftragnehmer⁽ⁱ⁾.
- Die mit der Auftragsbearbeitung befassten Mitarbeitenden werden auf die Auftragspezifikation des Kunden und die sich daraus ergebenden Verfahrens- und Arbeitsanweisungen hingewiesen⁽ⁱ⁾.
- Die Arbeitsergebnisse werden durch die Fachabteilungen überwacht⁽ⁱ⁾.
- Lieferanten und Dienstleister werden auf ihre Kritikalität in Bezug auf den Datenschutz und die Informationssicherheit bewertet. Bei Bedarf werden Vereinbarungen zum Schutz der Lieferkette in die Vertragsgestaltung mit aufgenommen^(b).
- Die Vorgaben des Datenschutz- und Informationssicherheitskonzepts werden regelmäßig durch interne und externe Audits überprüft^{(i)(b)}.

2.7 Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen zur Verfügbarkeitskontrolle

- Alle Gebäude verfügen über Brandmeldeanlagen mit Aufschaltung zur Feuerwehr^{(a)(b)}.
- Alle wichtigen Hardware-/System-Komponenten sind redundant ausgelegt^{(a)(r)(b)}.

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

- Alle Serverräume sind mit redundanter Klimaanlage, Brandmeldeanlage zur Feuerwehr, Wasserdetektoren und stellenweise einer Löschgasanlage ausgestattet^{(a)(b)}.
- Notstromversorgung in allen Rechenzentren durch eine USV (Unterbrechungsfreie Stromversorgung) sowie eine NEA (Netzersatzanlage)^{(a)(b)}.
- Regelmäßige Tests der Notstromversorgung durch Simulation eines Stromausfalls^{(r)(b)}.
- Es erfolgt eine tägliche Datensicherung^{(a)(b)}.
- Regelmäßige Überprüfungen der Sicherheitsverfahren^{(a)(r)(b)}.
- Firmenweit kommt eine EDR-Software zum Einsatz (Endpoint Detection and Response)^{(a)(r)(b)}.
- Notfallhandbuch/-konzepte sind erstellt^{(a)(b)}.
- Die Datenlöschung erfolgt entsprechend der Kundenanforderung in datenschutzge-rechter Form^(a).
- In der Produktion werden nur geprüfte und freigegebene Softwarekomponenten und IT-Verfahren eingesetzt^{(a)(r)(t)(b)}.

2.8 Trennungsgebot

Ziel der Trennungskontrolle ist es zu gewährleisten, dass zu unterschiedlichen Zwecken er-hobene Daten getrennt verarbeitet werden (Zweckbindung).

Maßnahmen zur Trennungskontrolle

- Die Datenbestände der Kunden und deren Projekte werden in den Datenbanken lo-gisch getrennt, so dass eine Verwechslung oder Vermischung von Datenbeständen oder eine zufällige Löschung ausgeschlossen ist⁽ⁱ⁾.
- Die Zugriffsberechtigungen sind über Rollenkonzepte und Verzeichnisstrukturen ge-regelt^{(v)(b)}.

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Pat- rick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

3 Weitere Maßnahmen

3.1 Maßnahmenbereich Personal

3.1.1 Einarbeitung neuer Mitarbeitender^{(v)(i)(b)}

Neu eingestellte Mitarbeitende werden im Rahmen der Einarbeitung auch zur Einhaltung der Maßnahmen bzgl. Datenschutz, IT- und Informationssicherheit geschult.

3.1.2 Datenschutz- und Geheimhaltungsverpflichtung^{(v)(b)}

Nach Einweisung und Schulung sind alle Mitarbeitende verpflichtet, eine Verpflichtung auf das Daten-, Sozial- und Fernmeldegeheimnis zu unterschreiben. Die Verpflichtung wird in der jeweiligen Personalakte hinterlegt. Konsequenzen aus Pflichtverletzungen werden den Mitarbeitenden deutlich gemacht. Jeder Mitarbeitende wird mit Beginn seiner Tätigkeit auf die Einhaltung der Vertraulichkeit sowie auf § 88 TKG verpflichtet. Die Mitarbeitenden werden regelmäßig zu Datenschutz- und Informationssicherheitsthemen sensibilisiert.

3.1.3 Regelmäßige Informationen^{(a)(b)}

Alle Mitarbeitende werden regelmäßig auf den neuesten Stand des Datenschutzes und die Maßnahmen zur Gewährleistung der Informationssicherheit im Unternehmen gebracht.

Regelmäßige Maßnahmen zur Awarenessbildung und -haltung im Themenbereich der Informations- und IT-Sicherheit sind etabliert^(b).

Zuständige Mitarbeitende werden auf mögliche aktuelle Sicherheitslücken aktiv hingewiesen und mit neuen Bestimmungen vertraut gemacht. Die Gesetzestexte zu den datenschutzrechtlichen Bestimmungen werden den Mitarbeitenden auf Anfrage zur Verfügung gestellt.

3.1.4 Verfahrensweise beim Ausscheiden von Mitarbeitenden^{(v)(b)}

Mitarbeitende, die das Unternehmen verlassen, unabhängig vom Grund, werden abschließend mündlich und schriftlich auf den Fortbestand der Geheimhaltungs- und Datenschutzbestimmungen hingewiesen. Dabei werden eventuelle Konsequenzen bei Zuwiderhandlungen dargestellt. Überdies werden beim Ausscheiden sämtliche Maßnahmen gemäß dem Verfahren „Mitarbeitendenaustritt“ ergriffen (z.B. Entzug von Zugangsberechtigungen).

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

3.2 Datenschutzmanagement

Es gibt ein Datenschutzmanagementsystem, welches u.a. folgende Punkte umfasst:

- Betroffenenrechte
- Privacy by design / Privacy by default
- Dienstleistercheck
- Umgang mit Datenschutzvorfällen
- PDCA-Zyklus

3.3 Weitergehende Maßnahmen

3.3.1 Sichtschutz

Alle ebenerdigen Fenster sind mittels Spezialfolien oder Jalousien gegen Einsichtnahme Unbefugter gesichert^(v).

3.3.2 Brandschutz

Die Brandschutzverordnung der Feuerwehr wird durch Brandschutzbegehungen überprüft und die hierbei gemachten Auflagen umgesetzt. In allen Räumen herrscht Rauchverbot^{(a)(b)}.

3.3.3 Allgemeine Sicherungsmaßnahmen

Die Mitarbeitenden sind gehalten nach Abschluss der Arbeiten auf geschlossene Fenster, Sichern aller Türen etc. zu achten und für die Sicherung des Gebäudes in dem Bereich zu sorgen, in dem Ihre Abteilung liegt. Ein Wachdienst prüft zusätzlich nach Dienstschluss den Verschluss aller Fenster und Eingangstüren.^{(v)(b)}

3.3.4 Systeme zur Angriffserkennung, Vorfallerkennung und -bearbeitung

Die IT-Server und -Clients der BITMARCK werden mit Hilfe von EDR-Systemen überwacht, Protokolldaten werden in einem zentralen Logmanagement gesammelt und ausgewertet. Die Auswertung erfolgt unterstützt durch ein System zum Security Information und Event Monitoring (SIEM)^(b).

Erkannte Sicherheitsvorfälle werden nach einem dokumentierten und strukturierten Verfahren unter Berücksichtigung bestehender Meldepflichten bearbeitet. Im Bedarfsfall stellen vorhandene interne und externe Ressourcen zur Durchführung forensischer Untersuchungen zur Verfügung^(b).

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				

3.4 Informationssicherheitsmanagementsystem (ISMS)

Die Themen Datenschutz und Informationssicherheit besitzen in der BITMARCK einen hohen Stellenwert und sind essentieller Bestandteil unserer Unternehmensstrategie. Sie unterliegen einem ständigen Verbesserungsprozess und werden den jeweils aktuellen Datenschutzbestimmungen angepasst. Dies ist in einer Leitlinie zur Informationssicherheit dokumentiert^(b).

Das Risikomanagement der Informationssicherheit erfolgt nach einem All-Gefahren-Ansatz und orientiert sich an den Vorgaben der ISO27005 und des BSI^(b).

Folgende Einheiten der BITMARCK sind zertifiziert nach der internationalen Norm ISO27001^{(a)(i)(v)(r)(b)}:

- BITMARCK Holding GmbH

○ Geltungsbereich:

Das ISMS der BITMARCK Holding GmbH gilt für Beratung, Projektmanagement, Rechenzentrumsbetrieb, IT-Services und Dienstleistungen im Gesundheitswesen, die Clearingstelle und Telematikdienstleistungen, sowie für alle innerhalb der Unternehmensgruppe erbrachten Verwaltungsdienstleistungen und Shared-Services, den damit verbundenen Mitarbeitenden, Technologien und Services.

○ In den Geltungsbereich sind eingeschlossen:

▪ **BITMARCK GmbH**, Kruppstr. 64, 45145 Essen

Beratung, Projektmanagement, Rechenzentrumsbetrieb, IT-Services, Dienstleistungen im Gesundheitswesen, die Clearingstelle und Telematikdienstleistungen

▪ **BITMARCK GmbH**, Putzbrunner Str. 93, 81739 München

Beratung, Projektmanagement, Rechenzentrumsbetrieb, IT-Services, Dienstleistungen im Gesundheitswesen und Telematikdienstleistungen

▪ **BITMARCK GmbH**, Hammerbrookstr. 38, 20097 Hamburg

Rechenzentrumsbetrieb, IT-Services, IT-Dienstleistungen und -Services insbesondere für das Gesundheitswesen und Telematikdienstleistungen

verantwortlich	Hennemann, Matthias;Eller, Martin;Ohnesorg, Patrick;Ahmadi, Tareq;	Version	6	Speicherdatum	08.09.2025
Klassifizierung	A0 - Öffentlich	Gültig	09.09.2025	Status	Gültig
Dokumentname	BMH_FK_O_Datenschutz- und Informationssicherheitskonzept der BITMARCK				