Medizinische Hochschule Hannover

Richtlinie Informationssicherheit für Auftragnehmer der MHH

Ansprechpartner	Informationssicherheitsbeauftragter der MHH Medizinische Hochschule Hannover Carl-Neuberg-Str. 1 30625 Hannover Informationssicherheit@MH-Hannover.de

Vertraulichkeitsstufe	Öffentlich

Erstellt von:	Geprüft von:	Genehmigt von:
Gomm, Georg	09.03.2023, Wortmann, Marcus 14.03.2023, Barke, Joachim	14.03.2023, Gomm, Georg

Inhalt

1. Generelle Information

1.1. Ziel und Zweck des Dokumentes

Auftragnehmer, deren Leistungen in Form von Software, Hardware oder Dienstleistungen erbracht werden, müssen bezüglich der Qualität ihrer Arbeit und der Einhaltung von Maßnahmen zur Informationssicherheit regelmäßig beurteilt werden. Zusätzlich sind in dieser Richtlinie die Mindestanforderungen an die Auftragnehmer der MHH definiert, die zur Bewertung herangezogen werden.

Bei unzureichenden Bewertungsergebnissen muss die Aufrechterhaltung des Lieferantenverhältnisses diskutiert werden. Die Bewertungsergebnisse fließen in die Risikobewertung des Informationssicherheitsbeauftragten mit ein. Je nach Bewertungsergebnis müssen gegebenenfalls die Lieferantenbeziehungen verändert werden, von Anpassung der Vereinbarungen bis hin zur Beendigung von Vertragsverhältnissen und Wechsel der Lieferanten.

Dieses Dokument ist für Auftragnehmer mit Zugriff auf Informationswerte der MHH bestimmt.

Erstellt von:	Geprüft von:	Genehmigt von:
Gomm, Georg	09.03.2023, Wortmann, Marcus 14.03.2023, Barke, Joachim	14.03.2023, Gomm, Georg

1.2. Geltungsbereich

Die hier getroffenen Regelungen gelten für das Informationssicherheitsmanagementsystem (ISMS) der Medizinischen Hochschule Hannover (MHH) gemäß der Informationssicherheitsleitlinie.

1.3. Freigabe / Revision

Das vorliegende Dokument tritt mit seiner Freigabe durch den Informationssicherheitsbeauftragten (ISB) im Namen des Präsidiums der MHH in Kraft.

Dieses Dokument sowie die sich daraus ergebenden Sicherheitsmaßnahmen unterliegen der Dokumentenlenkung.

2. Informationssicherheit in Lieferantenbeziehungen

Die von den Auftragnehmern getroffenen technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes und der Informationssicherheit müssen mindestens das Niveau der technischen und organisatorischen Maßnahmen der MHH erreichen.

Die MHH empfiehlt Auftragnehmern mit datenschutzrechtlicher bzw. informationssicherheitstechnischer Relevanz, ein Managementsystem für den Datenschutz bzw. die Informationssicherheit umzusetzen. Dabei können anerkannte Standards wie zum Beispiel die ISO/IEC 27001 oder der BSI IT-Grundschutz als Grundlagen dienen. Entsprechende Managementsysteme sind für Auftragnehmer für Produkte und Dienstleistungen in diesen Kategorien jedoch nicht verbindlich, sofern sie nicht im Rahmen von Ausschreibungen oder Verträgen explizit gefordert sind.

Sofern Auftragnehmer die Umsetzung eines Managementsystems im obigen Sinne für sich reklamieren, so muss der Geltungsbereich des jeweiligen Managementsystems die gelieferte Dienstleistung bzw. das Produkt vollständig einschließen.

Anforderungen in Ausschreibungen bzw. Verträgen gelten unabhängig von den Anforderungen dieser Richtlinie.

3. Verpflichtungserklärung

Der Auftragnehmer verpflichtet sich in Bezug auf die Lieferantenbeziehung mit der MHH zur Einhaltung der Informationssicherheit. Dabei müssen vor allem die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität gewahrt werden.

Die zur Gewährleistung der Informationssicherheit und zur Umsetzung der gesetzlichen Anforderungen im Bereich des Datenschutzes erforderlichen Aufgaben und Pflichten der MHH sind in einer Leitlinie zur Informationssicherheit festgehalten.

Für den Fall, dass sich die Dienstleistung auf die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten bezieht, sind die entsprechenden Vorschriften des Datenschutzes von Seiten des Dienstleisters einzuhalten. Einzelheiten dazu werden im Vertrag zur Auftragsverarbeitung festgelegt.

Der Auftragnehmer und deren Mitarbeitende verpflichten sich zur Vertraulichkeit im Umgang mit den Werten der MHH. Alle Mitarbeitende des Auftragnehmers, die für die MHH tätig sind, müssen zur Vertraulichkeit verpflichtet werden.

3.1. Zuverlässigkeit in Lieferantenbeziehungen

Der Auftragnehmer verpflichtet sich, sich stets um eine zuverlässige Anlieferung von Produkten und Erfüllung von Dienstleistungen ohne zeitlichen Verzug zu bemühen. Unregelmäßigkeiten in der Lieferantenbeziehung, bezogen auf die Produktlieferkette oder zeitliche und qualitative Erfüllung der Dienstleistung laut Vertrag sind der MHH unverzüglich mitzuteilen.

3.2. Änderung oder Beendigung von Lieferantenverträgen

Änderungen bei der Bereitstellung von Dienstleistungen / in den Dienstleistungsangeboten / bei der Dienstleistungserbringung sind rechtzeitig anzukündigen und sollten durch den Auftragnehmer nicht ohne Abstimmung mit der MHH erfolgen. Möglicherweise ist daraufhin die Anpassung eines Vertrages inkl. einer erneuten Risikobewertung erforderlich.

3.3. Informationssicherheitsbewusstsein, -ausbildung und -schulung

Der Auftragnehmer muss sicherstellen, dass alle Mitarbeitende, die im Zusammenhang mit der gelieferten Dienstleistung bzw. des gelieferten Produktes Zugriff auf Informationswerte der MHH erhalten können, in angemessenem Umfang zur Informationssicherheit und zum Datenschutz geschult und sensibilisiert worden sind. Der Nachweis über die Schulung bzw. Sensibilisierung seiner Mitarbeitenden muss vom Auftragnehmer auf Nachfrage erbracht werden können.

Bei Bedarf besteht die Möglichkeit, dass Mitarbeitende des Auftragnehmers an internen Schulungen zur Informationssicherheit und zum Datenschutz der MHH teilnehmen können.

4. Organisatorische Anforderungen

4.1. Organisation der Informationssicherheit

Der Auftragnehmer hat dem Antrag der MHH nachzukommen, Informationen seiner Sicherheitsorganisation offenzulegen, auf dessen Basis die MHH eine Bewertung des Auftragnehmers durchführen kann. Diese Einschätzung ist ein interner Prozess, der die MHH dabei unterstützt, die Metriken und Reife der Sicherheitsorganisation des Auftragnehmers zu beurteilen. Der Auftragnehmer soll, falls vorhanden, ein ISO/IEC 27001-Zertifikat oder Äquivalente sowie weitere Dokumente wie Berichte und Vorschriften etc. in diesem Kontext bereitstellen.

4.2. Benachrichtigung über sicherheitsrelevante Vorfälle

Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle, in Bezug auf die Informationssicherheit oder den Datenschutz, in seiner Organisation, die potenziell einen negativen Effekt auf materielle und immaterielle gelieferte Dienstleistungen oder das Informationssicherheitsniveau der MHH haben könnten, umgehend ohne Zeitverzug der MHH an IT-Service@mh-hannover.de zu melden.

Der Auftragnehmer muss im Falle eines Vorfalls auf Nachfrage der MHH angemessene Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie einen Abschlussbericht über die durchgeführten Maßnahmen zur Beseitigung des Vorfalls bereitstellen.

4.3. Benachrichtigung über sicherheitsrelevante Risiken

Der Auftragnehmer ist verpflichtet, Risiken in Bezug auf die Informationssicherheit oder den Datenschutz in seiner Organisation, die potenziell einen negativen Effekt auf materielle und immaterielle gelieferte Dienstleistungen oder das Informationssicherheitsniveau der MHH haben könnten, umgehend ohne Zeitverzug der MHH zu melden. Im Rahmen von Medizinprodukten sollte sich die Risikobetrachtung anhand der ISO 80001 orientieren.

4.4. Dokumentation

Der Auftragnehmer muss, Bedienabläufe, die im Zusammenhang mit der zu erbringenden Dienstleistung stehen, in angemessenem Umfang dokumentieren und dem Auftraggeber diese Dokumentation auf Anfrage vorlegen.

Es wird vom Auftragnehmer erwartet, dass dieser jegliche Dokumentation zur Verfügung stellt, die die Nutzung der angebotenen Dienstleistung erleichtert. Der gebräuchliche Umfang einer derartigen Dokumentation, wenn auch nicht auf diese beschränkt, inkludiert die folgenden Punkte:

- Liste der Hardware
- Liste der Software (inklusive Betriebssystem und Patch-Level)
- Überblick über die Systemarchitektur (kann Teil der Designdokumentation sein)
- Kommunikationsmatrix
- Existierende Benutzerkonten und Rollen sowie deren Berechtigungen
- Beschreibung von proprietären (nicht in der Industrie standardisierten) Sicherheitsmechanismen
- Weitere Dokumentationen, spezifiziert als Teil des Liefergegenstandes oder Auftrages, die die Sicherheit der Dienstleistung gewährleisten.

Sollten Änderungen an der Dienstleistung durchgeführt werden, wird vom Auftragnehmer erwartet, diese in die Dokumentation einzupflegen.

4.5. Asset-Management

Der Auftragnehmer muss alle Assets / Komponenten in seinem Informationssystem dokumentieren, die einen Bezug zu (IT-) Systemen der MHH zwecks Wartung oder Betriebszugang haben können. Die Verantwortung für die Aufrechterhaltung der entsprechenden Sicherheitskontrollen dieser Assets muss zugewiesen werden. Zum Schutz der Assets kann der Auftragnehmer die Anwendung spezifischer Sicherheitsmaßnahmen delegieren, jedoch bleibt der Auftragnehmer für den angemessenen Schutz der Assets, die in Bezug zum Informationssystem der MHH stehen, verantwortlich.

4.6. Personalsicherheit

Jeder, der im Namen des Auftragnehmers agiert, der entfernten oder lokalen Zugriff auf (IT-) Systeme der MHH haben muss, muss Informationen zu seiner Identität bereitstellen. Der Auftragnehmer stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall eintritt.

Sollte der Auftragnehmer mit Subunternehmern zusammenarbeiten, um den Vertrag mit der MHH zu erfüllen, muss der Auftragnehmer diesen ausdrücklich als Subunternehmer identifizieren und er muss sicherstellen, dass der Subunternehmer die gleichen Anforderungen erfüllt.

Der Auftragnehmer beauftragt nur qualifiziertes Personal, die über entsprechende Kenntnisse und Fähigkeiten bzgl. Installation, Soft- oder Hardware, Wartung oder Betrieb der Lösung verfügen und deren Zuverlässigkeit durch geeignete Prüfungen, z.B. durch nationale Behörden, festgestellt wurde.

4.7. Physische und umgebungsbezogene Sicherheit

Der Auftragnehmer hat dafür Sorge zu tragen, dass der unbefugte Zutritt in Räume, Büros und Einrichtungen, in denen Informationen der MHH verarbeitet werden, ausgeschlossen ist. Dies gilt weiterhin auch für Anlieferungs- und Ladebereiche, über die unbefugte Personen die Räumlichkeiten betreten könnten. Besonderen Bedeutung sollte Büroräumen, in denen Supporttätigkeiten in Form von Fernzugriffsverbindungen durchgeführt werden, zugesprochen werden.

Von Seiten des Auftragnehmers müssen Richtlinien erstellt werden, die aufgeräumte Arbeitsumgebungen sowie Bildschirmsperren bei Nichtbenutzung regeln.

4.8. Sichere Anmeldeverfahren

Der Zugriff des Auftragnehmers auf (IT-) Systeme der MHH darf ausschließlich über die von der MHH vorgegebenen Prozeduren und autorisierten Zugänge erfolgen.

Falls der Zugang über zwei Faktoren unter Verwendung eines Zugangstokens autorisiert wird, so muss der Auftragnehmer sicherstellen, dass der Zugriff auf den Token ausschließlich von dazu autorisierten Mitarbeitenden ausgeübt werden kann. Der Token muss, sofern dieser nicht verwendet wird, ständig unter Verschluss gehalten werden.

4.9. Audits

Der Auftragnehmer stimmt zu, dass die MHH oder ein anderer beauftragter Dritter, der nicht in einem Wettbewerbsverhältnis mit dem Auftragsnehmer stehen darf, im Auftrag der MHH die Organisation in Bezug auf die Informationssicherheit des Auftragnehmers auditieren darf. Dies kann einmal oder mehrmals geschehen. Die Prüfungen werden auf der Grundlage der von dem Auftragnehmer zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden jeweils einvernehmlich vereinbart.

Zusätzlich muss der Auftragnehmer die Abweichungen von den vereinbarten Sicherheitsanforderungen zeitnahe melden.

4.10. Aufrechterhaltung der Informationssicherheit

Der Auftragnehmer bestimmt die Anforderungen an die Informationssicherheit und zur Aufrechterhaltung des Informationssicherheitsmanagements in Abhängigkeit der beauftragten Dienstleistung und stellt sicher, dass die Dienstleistung gegen widrige Situationen (Notfall, Krise oder Katastrophe) in angemessenem Umfang abgesichert ist. Der Verfügbarkeitsbedarf der beauftragten Dienstleistung kann dazu in Abstimmung mit der MHH bestimmt werden. Der Auftragnehmer legt Prozesse, Verfahren und Maßnahmen fest, dokumentiert diese und setzt sie um, um das erforderliche Niveau an Informationssicherheit auch in widrigen Situationen aufrechterhalten zu können. Die Wirksamkeit der Maßnahmen soll von Seiten des Auftragnehmers in regelmäßigen Abständen geprüft werden. Die Prüfungen sollen dokumentiert werden.

4.11. Meldung vom Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die MHH betreibt eine kritische Infrastruktur gem. BSI-Gesetz und ist verpflichtet Meldung vom BSI über Schwachstellen, Gefährdungen, Vorfälle etc. entgegenzunehmen und zeitnahe zu behandeln. Sofern Produkte des Auftragnehmers im Rahmen von BSI-Meldungen thematisiert werden, behält sich die MHH vor eine Stellungnahme zu der entsprechenden BSI-Meldung von dem Auftragnehmer einzuholen. Die Stellungnahme muss u.a. eine Risikoabschätzung seitens des Auftragnehmers, einen Maßnahmenplan zur Behandlung inkl. verbindlicher zeitlicher Planung zum weiteren Vorgehen enthalten. Die Stellungnahme muss zeitnah, unter Berücksichtigung der gesetzlichen Fristen für Datenschutzvorfälle gemäß DSGVO bzw. Informationssicherheitsvorfälle, bei der MHH eingehen.

5. Technische Anforderungen

5.1. Schwachstellenmanagement

Die Produkte des Auftragnehmers müssen regelmäßig auf Schwachstellen geprüft werden und in Bezug auf die Kritikalität und die geschäftlichen Auswirkungen hin untersucht werden.

Sind vom Auftragnehmer entwickelte Software-, Firmware- oder Hardware-Komponenten betroffen, ist der Auftragnehmer verpflichtet, umgehend die Schwachstellen per E-Mail an IT-Service@mh-hannover.de zu melden und diese bzgl. möglicher funktionaler und sicherheitsrelevanter Auswirkungen zu bewerten. Eine mögliche Bewertung der Kritikalität kann z.B. auf Basis der Schutzbedarfsanalyse durch die MHH festgelegt werden. Der Umfang des Schwachstellenmanagements umfasst jede potenzielle Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität und Vertraulichkeit der Vermögenswerte (materielle oder immaterielle) oder auf eine bei der MHH operierende Dienstleistung des Auftragnehmers nehmen kann.

5.2. Patchmanagement

Sicherheitspatche zur Behebung von kritischen Schwachstellen sind innerhalb von 8 Werktagen nach Veröffentlichung / Freigabe durch den Hersteller zu installieren. Hierbei sind als kritisch solche Schwachstellen anzusehen, die vom BSI als solche benannt bzw. nach dem Common Vulnerability Scoring System (CVSS, deutsch: „Allgemeines Bewertungssystem für Schwachstellen") mit einem Wert von mindestens 8,0 eingestuft wurden. Weitere Sicherheitspatche sind zeitnah, jedoch maximal 4 Wochen nach Veröffentlichung / Freigabe durch den Hersteller zu installieren.

Alle Sicherheitspatche müssen geeignet geplant, genehmigt und dokumentiert werden. Sicherheitspatche müssen vorab geeignet getestet werden bspw. sind Sicherheitspatche auf ihre Kompatibilität mit anderen Software-Produkten zu testen.

Der Auftragnehmer wird für jede im Patchzyklus adressierte Schwachstelle einen Bericht erstellen und der MHH zur Verfügung stellen. Dieser muss detaillierte oder aggregierte Daten unter Berücksichtigung der Kritikalitätsstufe und der betroffenen Bereiche (Verfügbarkeit, Integrität und/oder Vertraulichkeit) enthalten.

5.3. Maßnahmen gegen Schadsoftware

Der Auftragnehmer muss sicherstellen, dass auf allen (IT-) Systemen, die mittelbar oder unmittelbar im Zusammenhang mit der Dienstleistungserbringung verwendet werden, in angemessenem Umfang Maßnahmen zur Abwehr von Schadsoftware getroffen werden. Softwareprodukte zur Abwehr von Schadsoftware und Schadcode-Definitionen sind ständig aktuell zu halten. Davon betroffen sind im Besonderen solche Geräte, die für Supporttätigkeiten für oder bei der MHH Verwendung finden.

5.4. (IT-) Systemhärtung

Der Auftragnehmer verpflichtet sich, die von ihm gelieferten (IT-) Systeme zu härten, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren.

Dabei gelten folgende Anforderungen:

- Minimale Installationsprinzipien. / Installation muss mit MHH Administrationsberechtigungen erfolgen.
- Nicht benötigte Freigaben (einschließlich der Standardverwaltungsfreigaben) müssen entfernt werden.
- Jeder nicht benötigte Netzwerkzugang (TCP/IP- oder UDP-Port) muss deaktiviert sein. Die Nutzung jedes Zugangs muss in der Dokumentation erläutert werden.
- Insofern zusätzlich vereinbart, müssen die durch die MHH vorgegebenen allgemeinen Konfigurationsstandards und Sicherheitsvorschriften eingehalten werden.
- Der Auftragnehmer stellt sicher, dass jedes Standardpasswort in allen möglichen Fällen geändert werden kann.
- Der Auftragnehmer muss im Rahmen seiner Möglichkeiten sicherstellen, dass seine Lösungen frei von „Backdoors" sind, die Sicherheitsmechanismen überwinden können.
- Der Auftragnehmer verpflichtet sich, dass er hinsichtlich seiner Produkte mit geeigneten Maßnahmen und Protokollen nachweist, dass alle in diesem Abschnitt genannten Anforderungen eingehalten werden.

5.5. Fernzugang

Fernzugänge des Auftragnehmers zum Netzwerk bzw. zu (IT-) Systemen der MHH werden unter den folgenden Bedingungen gestattet:

- Der Auftragnehmer muss sicherstellen, dass bei Fernzugängen die Vertraulichkeit, Verfügbarkeit und Integrität der Assets und Services der MHH gewährleistet sind. Dies beinhaltet auch die nachträgliche Verwendung von Informationen, von denen der Auftragnehmer während eines Fernzugriffes Kenntnis erlangt hat. Er ist für alle Aktionen der Benutzerkonten mit Fernzugangsfunktion auf (IT-) Systemen des Auftraggebers verantwortlich.
- Jeder Nutzer eines Fernwartungszugangs muss ein personalisiertes Benutzerkonto besitzen. Ausnahmen sind zu dokumentieren. Bei Ausnahmen muss die komplette Rückverfolgbarkeit der Nutzung eines Benutzerkontos (wer, wann) festgehalten und der MHH auf Verlangen ausgehändigt werden.
- Nicht mehr benötigte Zugänge müssen unverzüglich der MHH gemeldet werden, so dass diese gesperrt werden können.
- Die von der MHH zur Verfügung gestellten Fernwartungszugänge sind anzuwenden.

5.6. Anforderungen an Softwareentwicklungsprozesse

Insofern Auftragnehmer Software für die MHH entwickeln, müssen die Prinzipien des Security by Design eingehalten und sich an den allgemein anerkannten Industriestandards orientieren.

5.7. Einsatz kryptographischer Lösungen

Um sicherzustellen, dass keine veralteten und als unsicher bekannten Kryptographielösungen in den Produkten verwendet werden, wird der Auftragnehmer eine schriftliche Richtlinie etablieren und mit der MHH abstimmen, die die zulässigen Kryptographie-algorithmen definiert. Diese Richtlinie sollte sich an gängige Industriestandards halten (z.B. BSI TR-02102) und regelmäßig überprüft werden.

Der Einsatz der kryptographischen Absicherung der Kommunikation ist insbesondere notwendig, wenn Daten mit hohem Schutzbedarf über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.