

Richtlinie Informationssicherheit für Auftragnehmer der MHH

Informationssicherheitsbeauftragte:r der MHH - Informationssicherheit@MH-Hannover.de
Medizinische Hochschule Hannover - Carl-Neuberg-Str. 1 - 30625 Hannover

Inhalt

1.	Generelle Information	2
1.1.	Ziel und Zweck des Dokumentes	2
1.2.	Geltungsbereich	3
1.3.	Freigabe / Revision	3
2.	Informationssicherheit in Lieferantenbeziehungen	3
3.	Verpflichtungserklärung	3
3.1.	Zuverlässigkeit in Lieferantenbeziehungen	3
3.2.	Änderung oder Beendigung von Lieferantenverträgen	4
3.3.	Informationssicherheitsbewusstsein, -ausbildung und -schulung.....	4
4.	Organisatorische Anforderungen.....	4
4.1.	Organisation der Informationssicherheit	4
4.2.	Benachrichtigung über sicherheitsrelevante Vorfälle	4
4.3.	Benachrichtigung über sicherheitsrelevante Risiken	4
4.4.	Dokumentation	4
4.5.	Asset-Management	5
4.6.	Personalsicherheit	5
4.7.	Physische und umgebungsbezogene Sicherheit	5
4.8.	Sichere Anmeldeverfahren.....	5
4.9.	Audits / Überprüfungen	6
4.10.	Aufrechterhaltung der Informationssicherheit	6
4.11.	Meldungen vom Bundesamt für Sicherheit in der Informationstechnik (BSI)	6
5.	Technische Anforderungen	6
5.1.	Schwachstellenmanagement	6
5.2.	Patchmanagement	7
5.3.	Maßnahmen gegen Schadsoftware	7
5.4.	(IT-) Systemhärtung	7
5.5.	Fernzugang.....	7
5.6.	Anforderungen an Softwareentwicklungsprozesse.....	8
5.7.	Einsatz kryptographischer Lösungen.....	8

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.

Die Bewertungsergebnisse fließen in die Risikobewertung der MHH 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.

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 die:den Informationssicherheitsbeauftragte:n (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 ist im Geltungsbereich Bereitstellung, Betrieb, Support und Wartung der zentralen IT-Basisinfrastruktur nach ISO / IEC 27001:2013 zertifiziert.

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.

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.

Daten mit hoher Vertraulichkeitsstufe, sowie Patientendaten, sollten innerhalb von zertifizierten Cloudumgebungen, bspw. nach BSI Cloud Computing Compliance Criteria Catalogue (C5), verarbeitet werden.

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 Auftragnehmers einzuhalten. Einzelheiten dazu werden im Vertrag zur Auftragsverarbeitung festgelegt.

Der Auftragnehmer und dessen Mitarbeitenden verpflichten sich zur Vertraulichkeit im Umgang mit den Werten der MHH. Alle Mitarbeitenden 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 Mitarbeitenden, 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.

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.

Sämtliche durch den Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind in geeigneter Form zu dokumentieren.

Nachweise zur Informationssicherheitsorganisation bzw. zu umgesetzten Informationssicherheitsmaßnahmen des Auftragnehmers müssen vom Auftragnehmer auf Nachfrage der MHH erbracht werden. Nachweise können bspw. in Form von Dokumentationen, Richtlinien, Berichten, Schulungszertifikaten, Protokollen oder Konfigurationsdateien erbracht werden.

4.2. Benachrichtigung über sicherheitsrelevante Vorfälle

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

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

4.3. Benachrichtigung über sicherheitsrelevante Risiken

Der Auftragnehmer ist verpflichtet, validierte und relevante Informationen zu Risiken in seiner Organisation in Bezug auf die Informationssicherheit oder den Datenschutz, die potenziell einen negativen Effekt auf materielle und immaterielle gelieferte Dienstleistungen oder das Informationssicherheitsniveau der MHH haben könnten, unverzüglich 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 Patchlevel)
- 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 oder an den Produkten durchgeführt werden, wird vom Auftragnehmer erwartet, diese kurzfristig 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

Jede:r, die:der im Namen des Auftragnehmers agiert, die:der entfernten oder lokalen Zugriff auf (IT-) Systeme der MHH haben muss, muss Informationen zu ihrer: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. Insbesondere sind die Anforderungen aus 3.3. Informationssicherheitsbewusstsein, -ausbildung und -schulung zu berücksichtigen.

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.

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 / Überprüfungen

Der Auftragnehmer stimmt zu, dass die MHH oder ein anderer beauftragter Dritter, der nicht in einem Wettbewerbsverhältnis mit dem Auftragnehmer stehen darf, im Auftrag der MHH die Organisation in Bezug auf den Datenschutz bzw. 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, sofern das Sicherheitsniveau abgesenkt wird.

Die MHH behält sich vor, anlassbezogen bzw. regelmäßig eine Selbstbewertung des Auftragnehmers zu Themen des Datenschutzes und der Informationssicherheit einzufordern, welche kurzfristig durch den Auftragnehmer zurückzumelden ist.

4.10. Aufrechterhaltung der Informationssicherheit

Der Auftragnehmer bestimmt die Anforderungen an die Informationssicherheit und zur Aufrechterhaltung des Informations-sicherheitsmanagements 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 muss von Seiten des Auftragnehmers in regelmäßigen Abständen geprüft werden. Die Prüfungen müssen dokumentiert werden.

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

Die MHH betreibt eine kritische Infrastruktur gem. BSI-Gesetz und ist verpflichtet Meldungen 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. Der Umfang des Schwachstellenmanagements umfasst jede potenzielle Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität und Vertraulichkeit der Werte (materielle oder immaterielle) oder auf eine bei der MHH operierende Dienstleistung des Auftragnehmers nehmen kann.

5.2. Patchmanagement

Sicherheitspatches 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 Sicherheitspatches sind zeitnah, jedoch maximal 4 Wochen nach Veröffentlichung / Freigabe, durch den Hersteller zu installieren.

Alle Sicherheitspatches müssen geeignet geplant, genehmigt und dokumentiert werden. Sicherheitspatches müssen vorab geeignet getestet werden bspw. sind Sicherheitspatches auf ihre Kompatibilität mit anderen Softwareprodukten 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 Schadcodedefinitionen 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.
- Für die MHH müssen stets Administrationsberechtigungen auf dem jeweiligen (IT-) System eingerichtet werden.
- 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 Standardkennwort geändert werden kann.
- Der Auftragnehmer muss im Rahmen seiner Möglichkeiten sicherstellen, dass seine Lösungen frei von „Backdoors“ sind, die Sicherheitsmechanismen überwinden können.

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 Werte 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 Kryptographiealgorithmen 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 hoher Vertraulichkeitsstufe über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.