Informationssicherheitsrichtlinie für Auftragnehmer der Grosskraftwerk Mannheim AG

Stand: 24. März 2023

Grosskraftwerk Mannheim Aktiengesellschaft

§ 1 Einleitung

1.1 Die Versorgung seiner Kunden und Partner mit den vertraglich zugesagten Energiemengen hat für das Grosskraftwerk Mannheim (nachstehend „GKM“) höchste Priorität. Zudem unterliegen viele Geschäftsprozesse des GKM gesetzlichen Verpflichtungen und Auflagen, wie zum Beispiel dem IT-Sicherheitsgesetz zum Schutz kritischer Infrastrukturen.

1.2 Daraus abgeleitet haben der Schutz der Vertraulichkeit, Integrität und Authentizität von Informationen sowie der Schutz der Verfügbarkeit von Anwendungen und Systemen für GKM einen großen Stellenwert.

1.3 Aus diesen Gründen hat GKM grundlegende Informationssicherheitsanforderungen und -vorgaben für die Zusammenarbeit mit Lieferanten und Dienstleistern (nachfolgend „Auftragnehmer“ genannt) festgelegt.

1.4 Die nachfolgenden Bestimmungen werden in die Verträge mit Auftragnehmern einbezogen und Vertragsbestandteil. Sie gelten ausschließlich. Hiervon abweichende, entgegenstehende oder ergänzende allgemeine Geschäftsbedingungen des Auftragnehmers werden nicht Vertragsinhalt. GKM widerspricht einer Einbeziehung abweichender allgemeiner Geschäftsbedingungen des Auftragnehmers. Sie gelten nur dann und nur insoweit, als GKM ihrer Geltung ausdrücklich zugestimmt hat. Das Zustimmungserfordernis gilt in jedem Fall, insbesondere auch dann, wenn GKM - gegebenenfalls in Kenntnis der allgemeinen Geschäftsbedingungen des Auftragnehmers - ihnen nicht ausdrücklich widerspricht bzw. den Vertrag mit dem Auftragnehmer vorbehaltlos ausführt.

§ 2 Geltungsbereich

2.1 Die Vorgaben und Regelungen dieses Dokumentes gelten verbindlich für alle Auftragnehmer des GKM. Werden vom Auftragnehmer Subunternehmer eingesetzt, so sind diese vom Auftragnehmer auf die Einhaltung dieser Richtlinie vertraglich zu verpflichten.

2.2 Je nach Art des Auftrages können im Rahmen der Auftragsvergabe zusätzliche informationssicherheitsspezifische Regelungen zugrunde gelegt werden. Wenn GKM mit dem Auftragnehmer nicht ausdrücklich etwas anderes vereinbart, gilt die Informationssicherheitsrichtlinie in ihrer jeweils zum Zeitpunkt des Vertragsschlusses mit dem Auftragnehmer gültigen, jedenfalls jedoch in der ihm zuletzt in Textform (§ 126 b BGB) mitgeteilten Fassung als Rahmenvereinbarung auch für künftige Verträge mit dem Auftragnehmer, ohne dass GKM in jedem Fall wieder auf sie hinweisen müsste. Über Änderungen der Richtlinie wird GKM den Auftragnehmer in diesem Fall unverzüglich informieren.

§ 3 Vertrauliche Informationen

3.1 „Vertrauliche Informationen“ im Sinne dieser Richtlinie sind sämtliche Informationen, die GKM oder externe Berater dem Auftragnehmer mündlich, schriftlich, digital verkörpert oder in anderer Form mitteilen bzw. offenlegen. Als vertrauliche Informationen gelten insbesondere

3.1.1 Geschäftsgeheimnisse, Produkte, Herstellungsprozesse, Knowhow, Erfindungen, geschäftliche Beziehungen, Geschäftsstrategien, Businesspläne, Finanzplanung, digital verkörperte Informationen (Daten). Zu diesen Informationen zählen auch unternehmensinterne Dokumente und Dokumentationen wie Verzeichnisse, Systembeschreibungen, Handbücher und Richtlinien, Arbeitsanweisungen und Protokolle.

3.1.2 alle sinn- und werthaltigen Daten über die Beschäftigten, externe / freie Mitarbeiter, Praktikanten etc. des GKM sowie über Kunden, Interessenten, Lieferanten, Geschäftspartner, Berater und sonstige Personen und Stellen, mit denen GKM in Verbindung steht und über die von GKM in Ausübung der Geschäftstätigkeit Daten erhoben, gespeichert, verarbeitet oder genutzt oder im GKM generiert oder dem GKM von diesen Stellen im Zusammenhang mit der Ausübung der Geschäftstätigkeit überlassen werden.

3.1.3 jegliche Unterlagen und Informationen des GKM, die Gegenstand technischer und organisatorischer Geheimhaltungsmaßnahmen sind und als vertraulich gekennzeichnet oder nach der Art der Information oder den Umständen der Übermittlung als vertraulich anzusehen sind.

3.2 Unerheblich ist in diesem Zusammenhang, auf welchen Trägermedien die Informationen und Daten gespeichert sind. Unter die Vertraulichkeit fallen deshalb alle

3.2.1 codierten und uncodierten Daten in Datenbanken und Dateien,

3.2.2 elektronischen Dokumente, unabhängig von der Art des Informationsträgers (PC, CD / DVD, USB-Sticks, Speicherkarten oder sonstige mobile Datenträger),

3.2.3 papierbasierten Dokumente,

3.2.4 Informationen auf Tonträgern und das gesprochene Wort sowie

3.2.5 Bilder, unabhängig von der Art des Informationsträgers.

3.3 Keine vertraulichen Informationen sind solche Informationen,

3.3.1 die der Öffentlichkeit vor der Mitteilung oder Übergabe durch GKM bekannt oder allgemein zugänglich waren oder dies zu einem späteren Zeitpunkt ohne Verstoß gegen eine Geheimhaltungspflicht werden,

3.3.2 die dem Auftragnehmer bereits vor Offenlegung durch GKM und ohne Verstoß gegen eine Geheimhaltungspflicht nachweislich bekannt waren,

3.3.3 die von dem Auftragnehmer ohne Nutzung oder Bezugnahme auf vertrauliche Informationen selber gewonnen wurden oder

3.3.4 die dem Auftragnehmer von einem berechtigten Dritten ohne Verstoß gegen eine Geheimhaltungspflicht übergeben oder zugänglich gemacht werden.

§ 4 Vertraulichkeitsverpflichtung

4.1 Der Auftragnehmer ist verpflichtet, alle vertraulichen Informationen gegenüber Dritten, einschließlich Behörden, streng vertraulich zu behandeln und geheim zu halten und sie ohne die vorhergehende schriftliche Zustimmung des GKM nicht an Dritte ganz oder teilweise weiterzugeben oder diesen offenzulegen.

4.2 Der Auftragnehmer ist verpflichtet, die vertraulichen Informationen ausschließlich im Zusammenhang mit seiner Tätigkeit bei GKM zu nutzen. Die vertraulichen Informationen dürfen nicht zu einem anderen als dem vorgenannten Zweck, insbesondere nicht zu Wettbewerbszwecken, genutzt werden. In diesem Zusammenhang ist der Auftragnehmer verpflichtet, keine der vertraulichen Informationen zum Gegenstand von gewerblichen Schutzrechten zu machen oder in sonstiger Weise direkt oder indirekt zur Erlangung von Schutzrechen zu nutzen.

4.3 Der Auftragnehmer ist verpflichtet, alle erforderlichen und geeigneten Vorkehrungen und Maßnahmen zu treffen, damit die erlangten Vertraulichen Informationen jederzeit wirksam gegen Verlust sowie gegen unberechtigten Zugriff geschützt sind. Hierzu gehören insbesondere die Schaffung und Aufrechterhaltung von geeigneten und erforderlichen Zutritts- bzw. Zugriffsvorkehrungen für Räumlichkeiten, Behältnisse, IT-Systeme, Datenträger und sonstige Informationsträger in bzw. auf denen sich vertrauliche Informationen befinden. Diese Verpflichtung beinhaltet auch dem aktuellen Stand der Technik angepasste technische Sicherheitsmaßnahmen (Art. 32 DS-GVO) und die Verpflichtung der Mitarbeiter auf die Vertraulichkeit und die Beachtung des Datenschutzes (Art. 28 Abs. 3 lit. b DS-GVO).

4.4 Auf Aufforderung des GKM sowie ohne Aufforderung spätestens nach Erreichung des in dem Auftrag beschriebenen Zwecks ist der Auftragnehmer verpflichtet, sämtliche vertraulichen Informationen einschließlich der Kopien hiervon innerhalb von 10 Arbeitstagen nach Zugang der Aufforderung bzw. nach Beendigung des Auftrags zurückzugeben oder zu vernichten (einschließlich elektronisch gespeicherter vertraulicher Informationen), sofern nicht mit GKM vereinbarte oder gesetzliche Aufbewahrungspflichten dem entgegenstehen.

§ 5 Non Disclosure Agreement

5.1 Ist im Rahmen der Beauftragung ein weitergehender Austausch vertraulicher Informationen erforderlich, verpflichtet sich der Auftragnehmer bereits jetzt, mit GKM eine weitergehende Vertraulichkeitsvereinbarung in der Form eines Non Disclosure Agreement (NDA) abzuschließen. Dieses NDA enthält spezifische weitergehende Regelungen zum Schutz vertraulicher Informationen für das konkrete zwischen GKM und Auftragnehmer bestehende Auftragsverhältnis. Hierzu zählt eine Regelung zur Zahlung einer angemessenen Vertragsstrafe für den Fall der Verletzung der Vertraulichkeitspflicht, den Verlust von Informationen und Daten oder die Verletzung zur Löschung. Das NDA enthält zudem eine Regelung zur Beweislastverteilung für den Fall der Weitergabe vertraulicher Informationen an Dritte.

§ 6 Auftragserbringung

6.1 Der Auftragnehmer trägt die Verantwortung für den Schutz der ausgehändigten Zutrittsinformationen wie Schlüssel, Ausweise oder Token sowie die Verhinderung deren missbräuchlicher Nutzung durch die von ihm eingesetzten Personen oder Dritte.

6.2 Der Auftragnehmer haftet ausnahmslos für sämtliche Schäden, die aus dem unsachgemäßen Umgang mit Zutrittsinformationen resultieren.

6.3 Zutrittsinformationen sind bei Auftragsende an GKM auszuhändigen. Personenspezifische Zutrittsinformationen sind im Falle des Mitarbeiterwechsels auszuhändigen.

6.4 Der Auftragnehmer muss ein aktuelles Verzeichnis der Beschäftigten führen, die Zutritt zum Betriebsgelände oder Zugang zu Informationssystemen, Netzwerken und Anwendungen haben.

6.5 Darüber hat der Auftragnehmer beim Zutritt auf das Werksgelände die spezifischen Zutrittsregelungen des GKM und die Hausordnung einzuhalten. Der Auftragnehmer hat seine Mitarbeiter oder Erfüllungsgehilfen entsprechend auf die Einhaltung der Zutrittsregelungen zu verpflichten.

6.6 Der Auftragnehmer stellt durch eine entsprechende Unterweisung zu Beginn der Umsetzung des Auftrags sicher, dass er ausschließlich Personal einsetzt, das im Zusammenhang mit der Auftragsdurchführung zuverlässig und fachkundig ist. Zuverlässig sind die für die Auftragsdurchführung vorgesehenen Mitarbeiter, wenn zu erwarten ist, dass diese die bei der Auftragsdurchführung anfallenden Aufgaben mit der gebotenen Sorgfalt ausführen. Fachkundig sind die Mitarbeiter, die das für die Auftragsdurchführung einschlägige Fachwissen und die hierfür erforderliche praktische Erfahrung aufweisen, um die ihnen im Zusammenhang mit dem Auftrag gestellten Aufgaben fachgerecht auszuführen.

6.7 Der Auftragnehmer stellt sicher, dass ein Mitarbeiter, bei dem eine Überprüfung durch den Auftragnehmer ergibt, dass er die erforderliche Zuverlässigkeit und / oder Fachkunde nicht aufweist, weder Zutritt auf das GKM-Gelände noch Zugang zu Informationen und Systemen des GKM erhält.

6.8 Auf Anfrage des GKM sind geeignete Unterlagen zur Überprüfung der Fachkunde und Zuverlässigkeit durch den Auftragnehmer vorzulegen.

6.9 Durch den Auftragnehmer eingesetztes Personal muss auch auf die Einhaltung datenschutzrechtlicher Anforderungen und auf sämtliche Vorgaben zur Wahrung der Informationssicherheit verpflichtet sein. Die Verpflichtung muss nach Beendigung der Tätigkeit entsprechend nachfolgendem § 15 dieser Richtlinie fortgelten.

§ 7 Anforderungen bei Zugang oder Zugriff auf IT-Systeme und Anwendungen

7.1 Allgemeine Zugangs- und Zugriffsrechte

Der Auftragnehmer ist verpflichtet, die von GKM eingeräumten Zugangs-/Zugriffsrechte auf IT-Systeme, Anwendungen Dienste, Daten ausschließlich im Rahmen seiner vertraglich zu erfüllenden Verpflichtungen zu nutzen.

7.2 Benutzerkennungen, Admin-Berechtigungen

Die für die Erfüllung des Auftrages erforderlichen Benutzerkennungen und Berechtigungen sind mit den jeweiligen Ansprechpartnern des GKM abzustimmen und mit einer Vorlaufzeit von mindestens drei Arbeitstagen über die GKM-Koordinatoren / -Ansprechpartner bei den jeweiligen System- und Anwendungsverantwortlichen zu beantragen.

Administrationsberechtigungen dürfen nur bei Bedarf und nur soweit genutzt werden, als es für die Erfüllung der Administrationsaufgaben erforderlich ist. Aufgaben, für die keine Administrationsrechte erforderlich sind, insbesondere die Nutzung des Internets, sind mit einem Account ohne Administrationsrechte durchzuführen. Ist für eine Administrationsaufgabe eine Genehmigung oder Freigabe erforderlich, darf die Aktion erst dann abgeschlossen werden, wenn dafür alle Genehmigungen oder Freigaben vorliegen.

Die Weitergabe und / oder die Übertragung von persönlich zugeordneten Berechtigungen sowie diesbezüglicher Benutzerkennungen und Passwörter ist untersagt.

Zugang und Zugriffe auf das GKM-Netz sowie Anwendungen und Systeme werden von GKM protokolliert.

Die Mitarbeiter des Auftragnehmers tragen die Verantwortung für den Schutz von Zugangsinformation wie Kennwörtern, Anmeldekennungen und Token sowie der Verhinderung der missbräuchlichen Nutzung und werden darauf vom Auftragnehmer auf der Grundlage einer vom GKM vorzulegenden Verpflichtungserklärung für Fremdfirmenmitarbeiter verpflichtet.

Werden Zugangsinformationen kompromittiert oder werden diese nicht mehr benötigt (z. B. bei Auftragsabschluss, Mitarbeiterwechsel, Kündigung oder sonstiger Beendigung des Auftrags), so ist umgehend das GKM zu informieren.

7.3 Stillschweigen über besondere Kenntnisse

Ein unberechtigter bzw. außerhalb der Administrationsaufgaben liegender Zugriff auf personenbezogene Daten oder eine Nutzung von im Einzelfall aus organisatorischen oder technischen Gründen weitergehenden Berechtigungen ist untersagt. Ist ein Zugriff auf persönlich zugeordnete Laufwerke oder Speicherbereiche erforderlich, darf dieser nur mit der Einwilligung des betroffenen GKM-Beschäftigten erfolgen. Ein heimliches Überwinden von Schutzmaßnahmen und Verschlüsselungsmechanismen ist untersagt.

Sowohl das Erspähen von Kennwörtern anderer Benutzer als auch die Ausnutzung anderer Benutzerkonten sowie das Überwinden anderer Schutzmaßnahmen und Verschlüsselungsmechanismen ist strikt verboten.

Bei Abwesenheit vom Arbeitsplatz ist die Sitzung zu beenden oder ein kennwortgeschützter Bildschirmschoner zu aktivieren.

7.4 Fernmeldegeheimnis

Erbringt der Auftragnehmer betriebliche Telekommunikationsdienste, ist es ihm untersagt, sich oder anderen über das für die Erbringung der betrieblichen Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Kommunikation zu verschaffen. Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, darf der Auftragnehmer nur für die Erbringung der Kommunikationsdienste verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit das Telekommunikationsgesetz oder eine andere gesetzliche Vorschrift oder eine innerbetriebliche Regelung zur Nutzung elektronischer Medien und zum Umgang mit personenbezogenen Daten dies vorsehen oder zulassen und sich dabei ausdrücklich auf Telekommunikationsvorgänge beziehen.

Diese Verpflichtung gilt neben der Verpflichtung auf die Wahrung der Vertraulichkeit, nach der dem Auftragnehmer untersagt ist, personenbezogene Daten unbefugt zu erheben, zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen.

7.5 Der Auftragnehmer hat elektronisch vorliegende Informationen vor deren Versand an das GKM bzw. vor deren Verwendung innerhalb des GKM-Netzwerkes vom Auftragnehmer durch ein anerkannt wirksames und aktuelles Virenschutzprogramm auf mögliche Schadsoftware zu prüfen.

§ 8 Einsatz von Rechnersystemen und Komponenten des Auftragnehmers

8.1 Die Anbindung von Rechnersystemen und Komponenten des Auftragnehmers an Netze des GKM ist grundsätzlich untersagt.

8.2 Ist im Rahmen der Auftragserbringung die Nutzung und Integration von IT-Equipment des Auftragnehmers erforderlich, so ist dies vorab über den jeweiligen GKM-Koordinatoren / -Ansprechpartner mit den zuständigen Netzwerkverantwortlichen des GKM abzustimmen.

8.3 Ist im Rahmen der Auftragserbringung die Nutzung von Softwareprodukten des Auftragnehmers und / oder seiner Subunternehmer erforderlich, so ist dies ebenfalls vorab über den GKM-Koordinator / -Ansprechpartner mit den zuständigen Netzwerk- und Systemverantwortlichen des GKM abzustimmen.

8.4 Kommen Hard- oder Softwarekomponenten des Auftragsnehmers zum Einsatz, so müssen diese über einen definierten Patch-Management-Prozess sicherstellen, dass nur lizenzierte Software zum Einsatz kommt und alle Sicherheits-Patches für das Betriebssystem und alle Anwendungen installiert sind. Ebenso muss das eingesetzte Equipment über einen Schutz vor Schadsoftware (Virenschutz) verfügen.

8.5 Zur Gewährleistung der Betriebssicherheit muss das eingesetzte IT-Equipment allen elektrischen und mechanischen Standards und dem Stand der Technik entsprechen.

§ 9 Verbindung zu Systemen und Netzen von Extern

9.1 Erfolgt eine Kopplung von Netzen des Auftragnehmers mit Netzen des GKM, insbesondere auch für Zwecke der Fernwartung von Systemen, so ist vom Auftragnehmer sicherzustellen, dass von deren Netzwerken keine unkontrollierten Zugriffe durch Dritte beziehungsweise nicht autorisierte Personen auf das GKM-Netzwerk möglich sind. Jegliche Erstimplementierungen sowie sämtliche Änderungen mit Auswirkung auf die Sicherheit der Anbindung an das GKM-Netzwerk, müssen vorher mit GKM und dessen IT-Abteilung abgestimmt werden.

9.2 GKM übernimmt keine Verantwortung für etwaige Schäden an angrenzenden Systemen des Auftragnehmers, die auftreten können, während der Auftragnehmer mit dem GKM-Netzwerk verbunden ist.

9.3 Die Anbindung von IT-Equipment des Auftragnehmers in das GKM-Netzwerk (Remote oder Vorort) wird grundsätzlich nur über die von GKM-IT präferierten Technologien gestattet. Vor der Anbindung hat der Auftragnehmer die präferierten Technologien schriftlich bei GKM-IT abzufragen und mögliche Ausnahmen hiervon mit GKM-IT abzustimmen.

§ 10 Entwicklung und Integration von Software

10.1 Im GKM-Netz und auf allen Geräten des Unternehmens dürfen nur Softwareprodukte genutzt werden, die rechtmäßig lizenziert und durch GKM genehmigt wurden.

10.2 Jegliche Installation von Software ist vorab durch GKM zu genehmigen.

10.3 Sämtliche Schwachstellen und Sicherheitslücken innerhalb der für das GKM entwickelten oder für das GKM bereitgestellten Software hat der Auftragnehmer umgehend an GKM-IT zu melden.

10.4 Alle Schwachstellen und Sicherheitslücken sind im Rahmen von Gewährleistungs- bzw. Wartungsvereinbarung durch den Auftragnehmer zu schließen. Ist der Auftragnehmer nicht der Entwickler der Software, hat er seine Gewährleistungsansprüche gegen den Entwickler / Hersteller der Software an GKM auf schriftliche Aufforderung abzutreten.

10.5 Erbringt der Auftragnehmer Leistungen der Softwareentwicklung und / oder -integration, sind gegebenenfalls weitere projektspezifische Sicherheitsanforderungen umzusetzen.

§ 11 Betrieb von Systemen- und Anwendungen für das GKM

11.1 Werden IT-Systeme, -Anwendungen und IT-Infrastrukturen vom Auftragnehmer betrieben und / oder administriert, so sind Mindestanforderungen an den Datenschutz und die Informationssicherheit zu erfüllen, um als vertrauenswürdig anerkannt zu werden. Hierzu hat der Auftragnehmer insbesondere

11.1.1. die gesetzlichen Anforderungen einzuhalten,

11.1.2. die allgemeingültigen Sicherheitsstandards nach BSI und / oder ISO 27001 zu beachten,

11.1.3. den Stand der Technik zur sicheren Erhebung, Verarbeitung, Speicherung und Aufbewahrung, Weitergabe sowie Löschung / Entsorgung schutzwürdiger Informationen und

11.1.4. die Anforderungen an Kommunikations- und Eskalationsprozesse bezogen auf informationsschutzrelevante Ereignisse zu beachten.

11.2 Der Auftragnehmer muss angemessene Vorsichtsmaßnahmen treffen, um die Hardware-Komponenten vor physischen Schäden zu schützen und die Verwendung durch unbefugte Benutzer zu verhindern.

11.3 Der Auftragnehmer muss die Sicherheit der Betriebsumgebung gewährleisten sowie logische Zugangs- und Zugriffskontrollen implementieren, um eine effektive Trennung von Subnetzen zu gewährleisten.

11.4 Beinhaltet der Auftrag die Erhebung, Nutzung oder Verarbeitung personenbezogener Daten im Sinne der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes, muss der Auftragnehmer alle aufgrund der Gesetze erforderlichen Maßnahmen (Art. 32 DS-GVO) zum Schutz der Daten treffen.

§ 12 Meldepflicht von sicherheitsrelevanten Ereignissen

12.1 Der Auftragnehmer verpflichtet sich, ein dokumentiertes Verfahren zur Meldung und Behandlung von sicherheitsrelevanten Ereignissen zu etablieren.

12.2 Sicherheitsrelevante Ereignisse mit Bezug oder möglichem Einfluss auf die Informationssicherheit des GKM sind unverzüglich zu melden. Dazu gehören z. B. Schadsoftwarebefall, Diebstahl von Daten, Verlust oder Zerstörung von IT-Equipment.

12.3 Sicherheitsrelevante Ereignisse können dabei auch potenzielle Schwachstellen umfassen, die Einfluss auf die Informationssicherheitsziele (Authentizität, Integrität, Verfügbarkeit, Vertraulichkeit) der materiellen oder immateriellen Werte und Prozesse oder auf eine bei der GKM operierende Dienstleistung des Auftragnehmers nehmen können. Auch diese Schwachstellen hat der Auftragnehmer zu melden.

12.4 Die Verfahren müssen die Berichterstattung an GKM, Analyse, Überwachung und Lösung der Sicherheitsvorfälle beinhalten.

12.5 Der Auftragnehmer verpflichtet sich, die an das GKM gelieferten Produkte / Dienstleistungen kontinuierlich auf vorhandene Schwachstellen zu untersuchen und Informationssicherheitsvorfälle unverzüglich an GKM zu melden.

§ 13 Kontrolle der Einhaltung der Vorgaben

13.1 Der Auftragnehmer sorgt innerhalb seines Unternehmens und der von ihm eingesetzten Subunternehmen für die Beachtung und Einhaltung der Anforderungen und Regelungen dieser Richtlinie.

13.2 Der Auftragnehmer verpflichtet sich, GKM unverzüglich darüber zu informieren, wenn die in dieser Richtlinie festgelegten Anforderungen und Regelungen nicht eingehalten werden können.

13.3 Der Auftragnehmer verpflichtet sich, Informationen seiner Sicherheitsorganisation auf Anfrage offenzulegen, damit das GKM eine Möglichkeit zur Bewertung der Reife der Sicherheitsorganisation wahrnehmen kann.

13.4 Der Auftragnehmer verpflichtet sich, zur Herausgabe jeglicher auftragsbezogener Dokumentation zur Kontrolle dieser Anforderungen.

13.5 GKM ist berechtigt, eine regelmäßige Überprüfung der Einhaltung der Informationssicherheitsvorgaben im erforderlichen Umfang durchzuführen. Das Audit-Recht schließt das Recht ein, jede Einrichtung, die Informationen des GKM verarbeitet, zu besichtigen und gilt ebenfalls für Unterauftragnehmer. Diese hat der Auftragnehmer vertraglich auf das Audit-Recht des GKM zu verpflichten. Die Prüfung findet in Absprache mit dem Auftragnehmer statt und wird mit einer angemessenen Vorankündigungsfrist angemeldet. Aufwände hierfür sind nicht gesondert zu vergüten, sofern keine anderweitigen vertraglichen Vereinbarungen getroffen wurden.

§ 14 Ausnahmen

14.1 Ausnahmeregelungen zu einzelnen Punkten dieses Dokumentes sind in Einzelfällen möglich, dann aber mit dem GKM-Informationssicherheitsbeauftragten abzustimmen und vertraglich festzuhalten.

14.2 Sollten diese Sicherheitsrichtlinien nicht eingehalten werden, behält sich GKM das Recht vor, den Zugriff des Auftragnehmers auf das GKM-Netzwerk sowie bestehende Anbindungen an das GKM-Netzwerk ohne vorherige Ankündigung ganz oder teilweise zu sperren.

§ 15 Geltungsdauer

15.1 Diese Informationssicherheitsrichtlinie tritt mit ihrer Einbeziehung in den Auftrag in Kraft und gilt bis 3 Jahre nach Beendigung des Auftrages.

15.2 In Fällen nachvertraglich unangemessener beruflicher oder wirtschaftlicher Behinderung des Auftragnehmers kann GKM einseitig auf die nachvertragliche Fortgeltung dieser Vereinbarung ganz oder teilweise verzichten oder dem Auftragnehmer auf entsprechenden Antrag hin von den Verpflichtungen dieser Vereinbarung ganz oder teilweise freistellen.

§ 16 Gerichtsstand

16.1 Ausschließlicher Gerichtsstand für alle sich aus oder im Zusammenhang mit dieser Richtlinie ergebenden Streitigkeiten ist Mannheim.