[Name der Organisation]

ST6 Handbuch zur Sicherheit von Anbietern und Lieferketten

Version	1.0
Besitzer der Police	Name eingeben
Genehmigt durch	Ausschuss zur Genehmigung der Richtlinie
Datum der Genehmigung	Datum eingeben
Datum des Inkrafttretens	Datum eingeben
Nächster Überprüfungstermin	Datum eingeben
Vertraulichkeitsstufe	INTERN

Änderungsverlauf

Datum	Version	Erstellt von	Beschreibung der Änderung
26.09.24	0.91	DataGuard	Grundstruktur des Dokuments
XX.XX.24	1.00	XX	Genehmigte Version und minimale Änderungen

[Wie diese DataGuard Richtlinienvorlage zu verwenden ist:]

[DataGuard möchte Ihnen einige wichtige Hinweise zur Anwendung der bereitgestellten Richtlinienvorlage geben. Diese Vorlage soll Ihnen als Ausgangspunkt dienen, um eigene, auf Ihre Organisation zugeschnittene Richtlinien zu entwickeln. Bitte beachten Sie die folgenden Hinweise zur Verwendung der Vorlage sorgfältig.

Verwendung der Vorlage

- **Vorlage als Ausgangspunkt:** Diese Vorlage ist sorgfältig recherchiert und von Experten zusammengestellt worden. Sie ist als Ausgangspunkt für die Erstellung Ihrer eigenen Richtlinie gedacht und bietet eine Struktur sowie Beispiele für Ihre künftiges Dokument. Bei allen Bemühungen erhebt diese Vorlage jedoch keinen Anspruch auf Passgenauigkeit und Vollständigkeit, denn die individuellen Gegebenheiten in Ihrer Organisation können abweichen.
- **Grundsatz der Effektivität:** Eine Richtlinie soll erforderlich, angemessen, passend, aufklärend und unterstützend für Ihren individuellen Unternehmenszweck wirken. Sorgen Sie dafür, dass Ihre Richtlinien stets diesem Grundsatz entsprechen.
- **Überprüfung der Inhalte:** Gehen Sie die Inhalte der Vorlage sorgfältig durch und überprüfen Sie diese im Hinblick auf die spezifischen Bedürfnisse und Anforderungen.
- **Vollständiges Verständnis erforderlich:** Stellen Sie sicher, dass Sie als Ersteller dieses Dokuments alle beschriebenen Anweisungen und Verfahren vollständig verstehen und für Ihre Organisation als anwendbar halten. Nur so können Sie fundierte Entscheidungen über Anpassungen treffen.
- **Klärung von Unklarheiten:** Sollten Sie auf Inhalte stoßen, die Sie nicht vollständig verstehen, holen Sie unbedingt weitere Informationen ein. Dies kann durch Rücksprache mit unseren DataGuard-Experten, rechtlichen Beratern oder anderen Fachexperten außerhalb oder innerhalb Ihrer Organisation geschehen.
- **Individuelle Anpassung erforderlich:** Die in der Vorlage beschriebenen Anweisungen und Verfahren sind pauschale Beispiele oder Vorschläge ohne tiefere Berücksichtigung Ihres Unternehmenskontextes. Daher ist es erforderlich, dass Sie den Inhalt der Richtlinien an die tatsächlichen Gegebenheiten und Anforderungen Ihrer Organisation anpassen.*
- **Keine ungeprüfte Übernahme:** Übernehmen Sie keine Texte oder Anweisungen aus der Vorlage, wenn diese nicht den spezifischen Anforderungen und der tatsächlichen Situation in Ihrer Organisation entsprechen. Jede Organisation ist einzigartig, und pauschale Übernahmen können zu Fehlern oder Missverständnissen führen.

- **Verantwortung der Geschäftsführung:** Beachten Sie, dass die endgültige Verantwortung für die Gestaltung und Umsetzung von Richtlinien bei der obersten Leitung Ihrer Organisation liegt. Es ist entscheidend, dass diese alle Inhalte kritisch überprüft und eine Korrektur von unpassenden Inhalten veranlasst.]

[*) Die in dieser Vorlage gelb hinterlegten und in eckigen Klammern gesetzten Hilfstexte und Hinweise sollen nach Kennnisnahme eliminiert oder inhaltlich angepasst werden. Beispiel: Bitte eliminieren Sie diese Seite vor Veröffentlichung der Richtlinie.]

1 Einleitung

Dieses Handbuch zur Sicherheit von Anbietern und Lieferketten dient als konsolidierter Rahmen, der die Strategie von [Name der Organisation] für die effektive Verwaltung und Sicherung unserer Lieferantenbeziehungen und Lieferkettenaktivitäten umreißt. Es dient als umfassender Leitfaden, in dem detailliert beschrieben wird, wie unsere Organisation verschiedene Sicherheitsherausforderungen im Zusammenhang mit der Sicherheit von Lieferanten und der Lieferkette in unserem gesamten Betrieb angehen wird. Darüber hinaus dient es als übergeordnetes Dokument, das den Ansatz unserer Organisation in Bezug auf die Sicherheit von Lieferanten und Lieferketten umreißt.

1.1 Zweck und Umfang

Das Hauptziel dieses Richtlinienpakets besteht darin, einen strukturierten Ansatz für die Sicherheit von Lieferanten und Lieferketten zu entwickeln, um die sensiblen Informationen, Vermögenswerte und den Ruf unserer Organisation zu schützen. Durch die Einhaltung dieser Richtlinie wollen wir unsere Widerstandsfähigkeit gegen Sicherheitsverletzungen erhöhen und das Risiko von Unterbrechungen oder Kompromittierungen innerhalb unserer Lieferkette minimieren. Die in diesem Handbuch gebündelten Richtlinien gelten für alle Mitarbeiter, Auftragnehmer, Drittanbieter und Interessengruppen, die in das Lieferantenmanagement oder die Lieferkette innerhalb unserer Organisation eingebunden sind. Sie umfasst alle Aspekte der Lieferantenbeziehungen, der Lieferkettenprozesse und der damit verbundenen Sicherheitsmaßnahmen, unabhängig von der Art oder dem Ort der Lieferkettenaktivitäten.

1.2 Anwendbarkeit

Die folgenden Richtlinien gelten für alle Mitarbeiter und Beteiligten und stellt sicher, dass sie sich an die festgelegten Richtlinien für die Sicherheit von Lieferanten und Lieferketten halten. Die für die Beschaffung bzw. Beauftragung verantwortlichen Personen haben in Zusammenarbeit mit den zuständigen Abteilungen die Aufgabe, die Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung der in diesem Richtlinienpaket beschriebenen Verfahren zu überwachen.

2 Anforderungen an gekaufte Software-Anwendungen und Cloud-Services

2.1 Informationssicherheit bei der Nutzung von Cloud-Diensten

2.1.1 Richtlinie

Die in der Organisation für die Beschaffung und Einführung von Cloud-Diensten verantwortlichen Bereiche müssen für eine sichere und vorschriftsmäßige Nutzung von Cloud-Diensten sorgen, um sensible Informationen zu schützen und die betriebliche Ausfallsicherheit zu gewährleisten. In dieser Richtlinie werden die folgenden Grundregeln dargelegt:

1. Datenverschlüsselung: Alle Daten, die zu und von Cloud-Diensten übertragen werden, müssen verschlüsselt werden, um sie vor unbefugtem Zugriff zu schützen.

2. Zugangskontrolle: Der Zugang zu Cloud-Diensten muss auf befugtes Personal beschränkt werden, wobei zur Erhöhung der Sicherheit eine Multi-Faktor-Authentifizierung eingeführt werden muss.

3. Regelmäßige Audits: Die Anbieter von Cloud-Diensten müssen routinemäßig überprüft werden, um die Einhaltung von Sicherheits- und Compliance-Standards und -Bewertungen zu gewährleisten.

4. Datenaufenthalt: Die Einhaltung der Vorschriften zum Datenaufenthalt und zum Schutz der Privatsphäre muss überprüft werden, um sicherzustellen, dass die Daten in zugelassenen Ländern gespeichert werden.

5. Reaktion auf Vorfälle: Es müssen klare Verfahren für die Reaktion auf Sicherheitsvorfälle im Zusammenhang mit Cloud-Diensten festgelegt werden, um mögliche Auswirkungen zu minimieren.

2.1.2 Verfahren

[Bitte Überprüfen Sie dieses Verfahren und passen es ggf. an Ihre organisatorischen Bedingungen an]

Zu den Prozessen für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus einzelnen Cloud-Diensten gehören in Übereinstimmung mit den Informationssicherheitsanforderungen des Unternehmens folgende:

1. Überprüfung von Cloud-Service-Vereinbarungen:

Die Organisation überprüft die Cloud-Service-Vereinbarungen mit dem/den Cloud-Service-Anbieter(n). Diese Vereinbarungen müssen die Anforderungen des Unternehmens in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Informationsverarbeitung berücksichtigen.

[Bitte erstellen Sie einen Anforderungskatalog (z.B. einen Fragebogen) zur Beantwortung vom Cloud-Service Anbieter, in dem die Anforderungskriterien definiert und die Erfüllung abgefragt werden.]

2. Risikobewertungen:

Das Unternehmen führt einschlägige Risikobewertungen durch, um die mit der Nutzung des Cloud-Dienstes verbundenen Risiken zu ermitteln. Etwaige Restrisiken, die mit der Nutzung des Cloud-Dienstes verbunden sind, werden eindeutig ermittelt und wenn vorhanden von der zuständigen Unternehmensleitung akzeptiert.

[DataGuard empfiehlt Ihnen die Berücksichtigung bzw. die Bewertung und Dokumentation von Risiken im Zusammenhang mit Cloud-Services regelmäßig im Risikomanagement der DataGuard Plattform oder alternativ in einem separaten Lieferanten-Management vorzunehmen.]

3. Schutz der Daten und Verfügbarkeit der Dienste:

Eine Vereinbarung zwischen dem Cloud-Diensteanbieter und dem Unternehmen muss Bestimmungen über den Schutz der Daten des Unternehmens und die Verfügbarkeit der Dienste enthalten. Dazu gehören die Bereitstellung von Lösungen, die auf branchenweit anerkannten Standards für Architektur und Infrastruktur basieren, die Verwaltung der Zugangskontrollen des Cloud-Dienstes, die Implementierung von Lösungen zur Überwachung und zum Schutz vor Malware sowie die Verarbeitung und Speicherung sensibler Daten des Unternehmens an zugelassenen Standorten.

[Bitte sammeln Sie entsprechende Vereinbarungen (z.B. SLA) für jeden Cloud-Service-Anbieter als dokumentierten Nachweis in Ihrer Lieferantenverwaltung.]

4. Unterstützung im Falle eines Zwischenfalls:

Die Vereinbarung muss Bestimmungen über die Information und Bereitstellung spezieller Unterstützung im Falle eines Informationssicherheitsvorfalls in der Cloud-Service-Umgebung enthalten.

5. Unterauftragsvergabe:

Die Vereinbarung soll sicherstellen, dass die Anforderungen unserer Organisation an die Informationssicherheit auch erfüllt werden, wenn vom Anbieter wiederum externe Dienstleistungen und Cloud-Dienste an einen weiteren externen Anbieter weitervergeben werden.

6. Digitale Beweise:

Die Vereinbarung soll regeln, wie unser Unternehmen bei der Sammlung digitaler Beweise unterstützt wird, wobei die Gesetze und Vorschriften für digitale Beweise in den verschiedenen Rechtsordnungen – insbesondere im Datenschutz - berücksichtigt werden.

7. Beenden des Cloud-Dienstes:

Die Vereinbarung muss eine angemessene Unterstützung und Verfügbarkeit der Dienste für einen angemessenen Zeitraum vorsehen, wenn das Unternehmen aus dem Cloud-Dienst aussteigen möchte.

8. Sicherung der Daten:

Der Vertrag muss die erforderliche Sicherung von Daten und Konfigurationsinformationen sowie gegebenenfalls die sichere Verwaltung von Sicherungskopien vorsehen.

9. Rückgabe von Informationen:

Die Vereinbarung muss vorsehen, dass Informationen wie Konfigurationsdateien, Quellcode und Daten, die Eigentum des Unternehmens sind, auf Anfrage während der Leistungserbringung oder bei Beendigung des Dienstes zur Verfügung gestellt und zurückgegeben werden.

10. Vorankündigung:

Unsere Organisation muss prüfen, ob in der Vereinbarung festgelegt wird, dass der Anbieter verpflichtet wird, vorab mitzuteilen, ob und wie wesentliche Änderungen an der Art und Weise, wie der Dienst für das Unternehmen erbracht wird, sich ändert.

11. Halten von engem Kontakt:

Unsere Organisation soll engen Kontakt zu seinen Cloud-Diensteanbietern halten. Diese Kontakte ermöglichen den gegenseitigen Austausch von Informationen über die Informationssicherheit bei der Nutzung von Cloud-Diensten.

12. Bewertung der Sicherheit von Daten und des Datenschutzes:

Eine Bewertung der Sicherheit von Daten, einschließlich der Verschlüsselung von Daten im Ruhezustand und bei der Übertragung, der Schlüsselspeicherung und des Schutzes muss gewährleistet sein. Die Verarbeitung von personenbezogenen Daten muss entsprechend den Anforderungen der DSGVO dokumentiert sein.

[Bitte schließen Sie erforderliche Verarbeitungsvereinbarungen ab und legen Sie diese als dokumentierten Nachweis in Ihrem Lieferantenmanagement ab.]

2.2 Anforderungen an die Anwendungssicherheit

2.2.1 Richtlinie

Die Anforderungen an die Informationssicherheit von Anwendungen müssen während der Entwicklung oder des Erwerbs von Anwendungen ermittelt, spezifiziert und genehmigt werden, um die Informationswerte der Organisation zu schützen.

2.2.2 Verfahren

1. Zuständigkeiten im Verfahren:

Zuständigkeit des Fachexperten für IT-Sicherheit (Risiko-Eigentümer):

- Durchführung von Risikobewertungen und Bereitstellung von Fachwissen bei der Ermittlung und Spezifizierung von Anwendungssicherheitsanforderungen.
- Zusammenarbeit mit Entwicklungsteams und Interessengruppen, um die Übereinstimmung mit den Sicherheitsrichtlinien und -standards des Unternehmens zu gewährleisten.

Zuständigkeit des Entwicklungsteams:

- Umsetzung der in diesem Verfahren spezifizierten Sicherheitsanforderungen bei der Entwicklung oder Beschaffung von Anwendungen.
- Mitteilung aller Probleme oder Unstimmigkeiten bei der Erfüllung der Sicherheitsanforderungen an den Spezialisten für Informationssicherheit.

2. Verfahren:

Risikobewertung und Bedarfsermittlung:

- Der Risiko-Eigentümer muss vorab eine Risikobewertung durchführen, um potenzielle Bedrohungen und Schwachstellen im Zusammenhang mit der Anwendung zu ermitteln.
- Es muss eine Zusammenarbeit des Risiko-Eigentümers mit dem Informationssicherheits-(Security-)Team frühzeitig bei der Festlegung spezifischer Sicherheitsanforderungen auf der Grundlage der Ergebnisse der Risikobewertung erfolgen. Eine Einbeziehung in einem frühen Prozessstadium ist erforderlich.

Spezifikation der Sicherheitsanforderungen:

- Sicherheitsanforderungen für die Anwendung müssen auf der Grundlage der ermittelten Risiken und der Unternehmensrichtlinien dokumentiert (Pflichtenheft) werden.
- Es muss sichergestellt werden, dass die Sicherheitsanforderungen alle relevanten Aspekte abdecken, einschließlich Authentifizierung, Datenvertraulichkeit, Integrität, Zugangskontrolle und Einhaltung rechtlicher und regulatorischer Anforderungen.

Genehmigung der Sicherheitsanforderungen:

- Es muss eine Vorlage der dokumentierten Sicherheitsanforderungen bei den entsprechenden Beteiligten erfolgen, einschließlich der Geschäftsleitung und der zuständigen Abteilungen.

- Vor der Entwicklung oder dem Erwerb neuer Anwendungen muss die Genehmigung für die Sicherheitsanforderungen eingeholt werden.

Integration von Sicherheitsanforderungen:

- Unsere Organisation muss sicherstellen, dass die genehmigten Sicherheitsanforderungen von Anfang an in den Entwicklungs- oder Beschaffungsprozess integriert werden.
- Die Zusammenarbeit von Entwicklern, Architekten und anderen Beteiligten muss durch die Organisation unterstützt werden, um Sicherheitsmaßnahmen in den Entwurf, die Architektur und die Funktionalität der Anwendung einzubinden (Prinzip von security by design).

Prüfung und Validierung:

- Durchführung gründlicher Tests der Anwendung, um zu überprüfen, ob die Sicherheitsanforderungen ordnungsgemäß umgesetzt wurden.
- Durchführung von Sicherheitstests, einschließlich Schwachstellenanalysen und Penetrationstests, zur Ermittlung und Behebung von Sicherheitslücken.

3 Externe Entwicklung und IKT-Dienstleistungen

3.1 Management der Informationssicherheit in der IKT-Lieferkette.

3.1.1 Richtlinie

Um die mit der Lieferkette von Informations- und Kommunikationstechnik (IKT)-Produkten und -Dienstleistungen verbundenen Risiken für die Informationssicherheit wirksam zu mindern, muss die Organisation einen soliden Rahmen für die Sicherheit der IT-Lieferkette schaffen, der gewährleistet, dass beteiligte Parteien die einschlägigen Anforderungen an die Informationssicherheit erfüllen.

3.1.2 Verfahren

[Das folgende Verfahren erläutert, wie Sie Ihre IKT-Lieferkette verwalten. Bitte Überprüfen Sie dieses Verfahren und passen es ggf. an Ihre organisatorischen Bedingungen an.]

Sicherheitsanforderungen: Die Anforderungen an die Informationssicherheit bei der Beschaffung von IT-Produkten oder -Dienstleistungen sind wie folgt definiert und werden bei der Beschaffung berücksichtigt:

[Bitte beschreiben Sie hier Ihre Sicherheitsanforderungen an die Beschaffenheit von neuen IT- und Kommunikationssystemen, (z.B. Biometrische Erkennung, Fernlöschung, …) oder verweisen Sie auf bestehende Beschaffungsrichtlinien hierfür hin. Für die Anforderungen von Software haben Sie in Kapitel 2. Bereits Anforderungen definiert, auf die verwiesen werden kann. Beschreiben Sie zudem, wie Sie organisatorisch sicherstellen, dass die Anforderungen angewendet werden.]

Weitergabe der Anforderungen in der Lieferkette:

Die Anbieter von IT-Dienstleistungen müssen die festgelegten Sicherheitsanforderungen in der gesamten Lieferkette weitergeben, wenn sie Teile der für das Unternehmen erbrachten IT-Dienstleistung an Unterauftragnehmer vergeben. Die konkrete Umsetzung ist in Kap. 2 dieser Richtlinie beschrieben.

Sicherheitspraktiken:

Die Lieferanten von IT-Produkten müssen für angemessene Sicherheitspraktiken in der gesamten Lieferkette sorgen, wenn diese Produkte Komponenten enthalten, die von anderen Lieferanten oder anderen Stellen gekauft oder erworben wurden. Entsprechende Verpflichtungen müssen in Vereinbarungen mit Lieferanten integriert werden.

Informationen über Softwarekomponenten:

Die Lieferanten von IT-Produkten müssen Informationen über die in den Produkten verwendeten Softwarekomponenten bereitstellen.

Informationen über Sicherheitsfunktionen:

Lieferanten von IT-Produkten müssen Informationen zur Verfügung stellen, die die implementierten Sicherheitsfunktionen ihres Produkts und die für den sicheren Betrieb erforderliche Konfiguration beschreiben. [Der dokumentierte Nachweis hierfür kann durch ein Lieferanten- bzw. Produkt-Assessment erfolgen]

Überwachungsprozess:

Es sind ein Überwachungsprozess und annehmbare Methoden zur Validierung der Übereinstimmung der gelieferten IT-Produkte und -Dienste mit den angegebenen Sicherheitsanforderungen zu implementieren.

[Bitte planen Sie entsprechende Lieferantenüberprüfungen in regelmäßigen Abständen in Ihrem ISMS Aufgabenmanagement ein.]

Identifizierung von kritischen Komponenten:

Es ist ein Verfahren zur Identifizierung und Dokumentation von Produkt- oder Dienstkomponenten einzuführen, die für die Aufrechterhaltung der Funktionalität kritisch sind.

[Das Asset-Verzeichnis ist z.B. ein geeigneter Ort, um die Kritikalität von Komponenten zu klassifizieren. Das Klassifizierungsschema muss ebenfalls festgelegt werden. Eine vertiefende Business-Impact-Analyse kann hierzu Transparenz in Fragen der Kritikalität von Komponenten in Ihrer Organisation verschaffen.]

Sicherstellung der Rückverfolgbarkeit:

Es muss sichergestellt werden, dass kritische Komponenten und ihre Herkunft über die gesamte Lieferkette hinweg zurückverfolgt werden können.

Sicherstellung der Funktionalität:

Es soll sichergestellt werden, dass die gelieferten IT-Produkte wie erwartet funktionieren und keine unerwarteten oder unerwünschten Merkmale aufweisen. [Nachweise hierzu erbringen entsprechende Systemtests.]

Echtheit der Bestandteile:

Es müssen Verfahren eingeführt werden, die sicherstellen, dass die von den Lieferanten gelieferten Komponenten echt sind und nicht von ihrer Spezifikation abweichen.

Zusicherung von Sicherheitsstufen:

Die Gewissheit, dass IT-Produkte die geforderten Sicherheitsniveaus erreichen, ist z. B. durch eine formale Zertifizierung oder ein Evaluierungssystem wie das Common Criteria Recognition Arrangement zu erlangen.

Regeln für den Informationsaustausch:

Es sind Regeln für den Austausch von Informationen über die Lieferkette und mögliche Probleme und Kompromisse zwischen dem Unternehmen und den Lieferanten festzulegen.

Verwaltung des Lebenszyklus von IT-Komponenten:

Es sind spezifische Verfahren für die Verwaltung des Lebenszyklus und der Verfügbarkeit von IT-Komponenten und der damit verbundenen Sicherheitsrisiken einzuführen.

3.2 Ausgelagerte Systementwicklung

3.2.1 Richtlinie

Die ausgelagerte Systementwicklung muss die Anforderungen des Unternehmens an die Informationssicherheit, die Überwachung und die Überprüfung der effektiven Umsetzung der Informationssicherheitsmaßnahmen erfüllen.

3.2.2 Verfahren

[Stellen Sie sicher, dass das nachstehende Verfahren immer dann durchgeführt wird, wenn eine neue ausgelagerte Tätigkeit hinzukommt oder wenn sich eine bestehende Tätigkeit ändert - eine ausgelagerte Tätigkeit könnte ein Drittunternehmen sein, das Software für Ihre Organisation erstellt]

Vorbereitungen zur Auslagerung:

1. Anforderungen ermitteln:

Definition on klaren Anforderungen und Erwartungen an das ausgelagerte Systementwicklungsprojekt, einschließlich der Anforderungen an Sicherheit und Datenschutz.

2. Auswahl der Zulieferer:

Auswahl der Lieferanten auf der Grundlage ihrer Fähigkeit, die Anforderungen der Organisation zu erfüllen, einschließlich ihrer Erfahrung, ihres Fachwissens und der Einhaltung von Sicherheitsstandards.

3. Vertragliche Vereinbarungen:

Entwerfen von umfassenden Verträgen, die Klauseln zu sicherem Design, Coding, Testverfahren, Rechten an geistigem Eigentum, Eigentum am Code und Einhaltung der geltenden Gesetze und Vorschriften enthalten.

4. Festlegen von Sicherheitsprotokollen:

Definition von Sicherheitsprotokollen für die Entwicklungsumgebung und Festlegung von Sicherheitswerkzeugen oder -maßnahmen, die während des Entwicklungsprozesses eingesetzt werden sollen.

Überwachung und Überprüfung von ausgelagerten Aktivitäten:

1. Regelmäßige Kommunikation:

Regelmäßige Kommunikation mit dem externen Lieferanten, um die Übereinstimmung mit den Projektzielen und die Einhaltung der Sicherheitsanforderungen zu gewährleisten.

2. Überprüfung der Evaluationsberichte:

Überprüfung der Evaluationsberichte an wichtigen Meilensteinen, um sicherzustellen, dass sie den spezifizierten Anforderungen und Sicherheitsstandards entsprechen.

3. Durchführung von Audits:

Machen Sie von Ihrem vertraglichen Recht Gebrauch, die Entwicklungsprozesse und -maßnahmen des Lieferanten regelmäßig zu überprüfen, um die Einhaltung der Sicherheitsanforderungen zu kontrollieren.

4. Prüfung und Validierung:

Gründliche Prüfung und Validierung der Entwicklungsergebnisse, um sicherzustellen, dass sie frei von Sicherheitslücken und bösartigen Inhalten sind und den Qualitätsstandards entsprechen.

5. Escrow-Vereinbarungen:

Stellen Sie sicher, dass Treuhandvereinbarungen für den Software-Quellcode bestehen, um Risiken im Zusammenhang mit dem Ausfall oder der Kündigung von Lieferanten zu mindern.

6. Dokumentation:

Bewahren Sie die Dokumentation aller Mitteilungen, Überprüfungen, Audits und Testergebnisse für zukünftige Referenz- und Konformitätszwecke auf.

[In der Praxis geht dieses Verfahren einher mit dem Prozess des „Request for Information“ (RFI). Das ist ein Vorgehen innerhalb des Einkaufs, das dem Gesamtprozess der Beschaffung vorangeht. Es kann sowohl im Rahmen der strategischen als auch der operativen Beschaffung zur Anwendung kommen. Beschreiben Sie bitte ggf. den RFI-Prozess Ihrer Organisation]

4 Lieferantenmanagement

4.1 Informationssicherheit in Lieferantenbeziehungen

[In Organisationen mit starker digitaler Wertschöpfung ist es normal, dass die Kapitel 2-4 dieser Richtlinie starke Überscheidungen haben. In solchen Fällen kann es sinnvoll sein, diese Kapitel zusammen zu ziehen. Bitte Überprüfen Sie daher die folgenden Verfahren und passen sie ggf. an Ihre organisatorischen Bedingungen an.]

4.1.1 Richtlinie

Bei Lieferantenbeziehungen und der gemeinsamen Nutzung von Daten durch Dritte ist die Informationssicherheit von größter Bedeutung. Alle Parteien müssen sich an strenge Vertraulichkeitsmaßnahmen, Datenverschlüsselungsprotokolle und Zugangskontrollverfahren halten, um sensible Informationen zu schützen. Regelmäßige Sicherheitsbeurteilungen und die Einhaltung von Vorschriften müssen durchgeführt werden, um die Integrität der Datenverarbeitungspraktiken zu gewährleisten.

Für kritische Lieferanten müssen Notfallpläne vorhanden sein, um die Kontinuität der Informationsverarbeitung zu gewährleisten, falls ein Lieferant seine Produkte oder Dienstleistungen nicht liefern kann.

4.1.2 Verfahren

Bewertung der Informationssicherheit in Lieferantenbeziehungen/Drittparteien - die wichtigsten Schritte:

[Bitte Überprüfen Sie dieses Verfahren und passen es ggf. an Ihre organisatorischen Bedingungen an. - Ihr Auditor wird nach Nachweisen für dieses Verfahren fragen und um Einsicht in Dokumente bitten, die zeigen, wie Sie diese Lieferantenbeziehungen verwalten]

1. Definieren Sie Lieferantenebenen auf der Grundlage der Klassifizierung gemeinsam genutzter Daten und der Kritikalität von Prozessen, um Informationssicherheitsrisiken zu bestimmen. [Im Folgenden finden Sie ein Beispiel für einige der Lieferantenbeziehungen. Legen Sie fest, welche Struktur Sie wünschen, hier ein Beispiel für eine mögliche Vorgehensweise: *Beispiel: Stufe 1 - Kritische Lieferanten (GDPR, PCI, Gesundheitsdaten, Finanztransfers), Stufe 2 - Wichtig (begrenzte PIII, Kundendienst, Betrieb), Stufe 3 - Alle anderen]*

2. Identifizierung der Informationssicherheitsmaßnahmen der Lieferanten für jede Stufe. Dazu kann es erforderlich sein, Kopien der relevanten Informationssicherheitsrichtlinien von den Lieferanten anzufordern.

3. Führen Sie Sicherheitsfragebögen ein, um Informationen über den aktuellen Stand der Sicherheit bei einem Lieferanten zu sammeln.

4. Integrieren Sie die Lieferantenbewertung in das Risikomanagement.

5. Überwachung, Überprüfung und Durchführung von Audits bei Lieferanten, um sicherzustellen, dass sie die festgelegten Anforderungen an die Informationssicherheit einhalten.

4.2 Berücksichtigung der Informationssicherheit in Lieferantenvereinbarungen.

4.2.1 Richtlinie

Informationssicherheitsanforderungen in Lieferantenvereinbarungen müssen umgesetzt werden, um ein vereinbartes Niveau an Informationssicherheit in den Lieferantenbeziehungen aufrechtzuerhalten.

Diese Punkte bilden die Grundlage für eine solide Lieferantenvereinbarung, die sicherstellt, dass beide Parteien die relevanten Anforderungen an die Informationssicherheit erfüllen.

4.2.2 Verfahren

Zur Aufrechterhaltung eines mit einem Lieferanten vereinbarten Niveaus der Informationssicherheit sind die folgenden Punkte zu berücksichtigen:

1. **Beschreibung der Informationen:**
   Die bereitzustellenden oder abzurufenden Informationen und die Methoden der Bereitstellung oder des Zugriffs auf die Informationen sind klar zu beschreiben.

2. **Klassifizierung von Informationen:**
   Informationen sind gemäß dem Klassifizierungsschema des Unternehmens zu klassifizieren.

3. **Zuordnung von Klassifizierungsschemata:**
   Es muss ein Mapping zwischen dem unternehmenseigenen Klassifizierungsschema und dem Klassifizierungsschema des Lieferanten geben.

4. **Rechtliche Anforderungen:**
   Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen müssen erfüllt werden, einschließlich des Datenschutzes, des Umgangs mit persönlich identifizierbaren Informationen (PII), der Rechte an geistigem Eigentum und des Urheberrechts.

5. **Durchführung von Kontrollen:**
   Jede Vertragspartei ist verpflichtet, eine vereinbarte Reihe von Kontrollen durchzuführen, einschließlich Zugangskontrolle, Leistungsüberprüfung, Überwachung, Berichterstattung und Rechnungsprüfung.

6. **Regeln für die Nutzung:**
   Es werden Regeln für die zulässige Nutzung von Informationen und anderen zugehörigen Ressourcen aufgestellt.

7. **Genehmigungsverfahren:**
   Es müssen Verfahren oder Bedingungen für die Genehmigung und den Entzug der Genehmigung für die Nutzung der Informationen des Unternehmens und anderer zugehöriger Vermögenswerte durch das Personal des Lieferanten

vorhanden sein.

8. **IT-Infrastruktur:**
   Es sind Anforderungen an die Informationssicherheit der IT-Infrastruktur des Lieferanten festzulegen.

9. **Entschädigungen und Abhilfemaßnahmen:**
   Entschädigungen und Abhilfemaßnahmen für die Nichterfüllung der Anforderungen durch den Auftragnehmer sind zu berücksichtigen.

10. **Management von Zwischenfällen:**

Es werden Anforderungen und Verfahren für das Management von Zwischenfällen festgelegt.

1. **Schulung und Sensibilisierung:**
   Es müssen Schulungs- und Sensibilisierungsmaßnahmen für spezifische Verfahren und Informationssicherheitsanforderungen vorhanden sein.

2. **Bestimmungen für die Vergabe von Unteraufträgen:**
   Einschlägige Bestimmungen für die Vergabe von Unteraufträgen sind zu berücksichtigen.

3. **Kontaktinformationen:**
   Es sind einschlägige Kontakte, einschließlich einer Kontaktperson für Fragen der Informationssicherheit, anzugeben.

4. **Überprüfungsanforderungen:**
   Die Anforderungen an die Überprüfung des Personals des Lieferanten müssen festgelegt werden.

[Prüfen Sie, ob die folgenden Punkte zutreffen, und fügen Sie sie gegebenenfalls der Liste hinzu: Zusätzliche Punkte:

1. Identifizieren Sie alternative Lieferanten:

Die Unternehmen müssen im Voraus alternative Lieferanten ermitteln. Dies kann dazu beitragen, Verzögerungen bei der Beschaffung von Ersatzprodukten oder -dienstleistungen zu vermeiden.

2. Diversifizierung der Lieferantenbasis:

Anstatt sich auf einen einzigen Lieferanten zu verlassen, können Unternehmen ihre Lieferantenbasis diversifizieren. Dies kann dazu beitragen, das Risiko zu mindern, das mit dem Ausfall eines einzelnen Lieferanten verbunden ist.

3. Aufrechterhaltung einer engen Beziehung zu den Lieferanten:

Die Unternehmen sollen eine enge Beziehung zu ihren Lieferanten pflegen. Dies kann zu einer besseren Kommunikation und einer schnelleren Lösung bei Problemen beitragen.

4. Regelmäßige Überprüfung und Aktualisierung von Notfallplänen:

Die Notfallpläne werden regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie weiterhin relevant und wirksam sind.

5. In Technologie investieren:

Unternehmen können in Technologie investieren, um ihre Lieferkette besser zu verwalten. Dies kann dazu beitragen, potenzielle Probleme schnell zu erkennen und Abhilfemaßnahmen zu ergreifen.

6. Versicherung:

Unternehmen können den Abschluss einer Versicherung in Erwägung ziehen, um etwaige finanzielle Verluste im Zusammenhang mit dem Ausfall eines Lieferanten zu decken].

4.3 Überwachung, Überprüfung und Änderungsmanagement von Lieferanten-Dienstleistungen.

4.3.1 Richtlinie

Zu den Grundsätzen für die Überwachung, Überprüfung und das Änderungsmanagement von Lieferanten-Dienstleistungen müssen gehören:

1. Kontinuierliche Überwachung:

Durchführung regelmäßiger Bewertungen und Überwachung der Dienste von kritischen Zulieferern, um potenzielle

Probleme, Leistungslücken oder Sicherheitsbedenken proaktiv zu ermitteln.

2. Gründliche Überprüfungen:

Regelmäßige Überprüfungen der Dienstleistungsvereinbarungen und der Leistung der kritischen Lieferanten müssen durchgeführt werden, um die Übereinstimmung mit den Unternehmenszielen und Qualitätsstandards zu gewährleisten.

3. Protokolle zum Änderungsmanagement:

Robuste Verfahren für das Änderungsmanagement wurden eingeführt, um nahtlose Übergänge zu erleichtern und Unterbrechungen zu minimieren, wenn Änderungen bei den Dienstleistungen von Zulieferern erforderlich sind.

4. Kommunikation und Kollaboration:

Mit den Zulieferern werden klare Kommunikationskanäle unterhalten, um ein effektives Änderungsmanagement zu gewährleisten und etwaige Herausforderungen, die während des Prozesses auftreten können, anzugehen.

4.3.2 Verfahren

Überwachung der Einhaltung der Vereinbarung, einschließlich der Erfüllung der Anforderungen an die Informationssicherheit. Eskalation von Mängeln an das Risikomanagement.

Regelmäßige Überwachung, Überprüfung, Bewertung und Steuerung von Änderungen in den Informationssicherheitspraktiken und der Leistungserbringung der Lieferanten:

[Dies sollte eine Liste von Prüfkriterien oder Kennzahlen sein, die Sie überwachen, überprüfen und pflegen können. Daher müssen Sie sicherstellen, dass alle Punkte in der Liste unten ihrer Organisation entsprechen - ein Auditor wird bestätigen wollen, dass die Angaben in jedem Punkt eingehalten werden.]

1. Serviceleistung überwachen:

Überprüfung der Einhaltung der Vereinbarungen, indem das Leistungsniveau der Dienste überwacht wird.

2. Überwachen Sie die von den Lieferanten vorgenommenen Änderungen:

Verfolgung von Erweiterungen des aktuellen Dienstleistungsangebots, Entwicklung neuer Anwendungen und Systeme, Änderungen oder Aktualisierungen der Richtlinien und Verfahren des Anbieters sowie neue oder geänderte Kontrollen zur Behebung von Informationssicherheitsvorfällen und zur Verbesserung der Informationssicherheit.

3. Überwachen Sie Änderungen bei den Dienstleistungen von Lieferanten:

Überwachung von Änderungen und Erweiterungen von Netzen, den Einsatz neuer Technologien, die Einführung neuer Produkte oder neuerer Versionen oder Releases, neuer Entwicklungswerkzeuge und -umgebungen, Änderungen des Standorts von Serviceeinrichtungen, den Wechsel von Unterlieferanten und die Vergabe von Unteraufträgen an andere Lieferanten.

4. Überprüfung der Serviceberichte:

Überprüfung der von den Lieferanten erstellten Leistungsberichte und Organisation regelmäßiger Fortschrittsbesprechungen, wie in den Vereinbarungen vorgesehen.

5. Durchführung von Audits:

Durchführung von Audits bei Lieferanten und Unterlieferanten in Verbindung mit der Überprüfung von Berichten unabhängiger Prüfer, falls vorhanden, und Weiterverfolgung der festgestellten Probleme.

6. Informationen über Vorfälle bereitstellen:

Bereitstellung von Informationen über Vorfälle im Bereich der Informationssicherheit und Überprüfung dieser Informationen, wie in den Vereinbarungen und den dazugehörigen Leitlinien und Verfahren vorgesehen.

7. Überprüfung von Auditaktivitäten und deren Aufzeichnungen:

Überprüfung der Auditpläne und Aufzeichnungen des Anbieters über Ereignisse im Bereich der Informationssicherheit, betriebliche Probleme, Ausfälle, Rückverfolgung von Fehlern und Unterbrechungen im Zusammenhang mit dem erbrachten Dienst.

8. Reaktion auf Vorfälle und deren Verwaltung:

Reaktion auf festgestellte Ereignisse oder Vorfälle im Bereich der Informationssicherheit und Betreuung.

9. Erkennen und Verwalten von Schwachstellen:

Erkennen von Schwachstellen in der Informationssicherheit und deren Behebung.

10. Überprüfung der Lieferantenbeziehungen:

Überprüfung der Informationssicherheitsaspekte in den Beziehungen des Lieferanten zu seinen eigenen Lieferanten.

11. Sicherstellung der Diensttauglichkeit:

Sicherstellen, dass der Anbieter über ausreichende Servicekapazitäten und praktikable Pläne verfügt, die sicherstellen, dass die vereinbarten Servicekontinuitätsniveaus nach größeren Serviceausfällen oder Katastrophen aufrechterhalten werden.

12. Sicherstellung der Einhaltung:

Sicherstellung, dass die Lieferanten Verantwortlichkeiten für die Überprüfung der Einhaltung und Durchsetzung der Anforderungen der Vereinbarungen zuweisen.

13. Bewertung der Sicherheitsstufen:

Regelmäßige Bewertung der Lieferanten zur Aufrechterhaltung eines angemessenen Niveaus der Informationssicherheit.

[Bitte planen Sie entsprechende Lieferantenüberprüfungen in regelmäßigen Abständen in Ihrem ISMS Aufgabenmanagement ein.]

5. Norm-Referenzen

5.1 Normreferenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. Einleitung	
2. Anforderungen an gekaufte Software-Anwendungen und Cloud-Services	A 5.23; A 8.26
3. Externe Entwicklung und IKT-Dienstleistungen	A 5.21; A 8.30
4. Lieferantenmanagement	A 5.19; A 5.20; A5.21; A 5.22

5.2 Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	Normkapitel (ISA-TISAX 6.0)
1. Einleitung	
2. Anforderungen an gekaufte Software-Anwendungen und Cloud-Services	1.3.3; 5.3.1; 5.3.3; 5.3.4
3. Externe Entwicklung und IKT-Dienstleistungen	1.2.4; 6.1.1
4. Lieferantenmanagement	1.2.4; 1.3.4; 6.1.1; 6.1.2