[Name der Organisation]

ST7 Handbuch zur Sicherheit in Projekten, Entwicklung und beim Testen

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 in Projekten, in der Softwareentwicklung und während Testprozessen dient fü [Name der Organisation] als konsolidierter Rahmen, der unsere Strategie für die wirksame Verwaltung und Sicherung unserer Projektentwicklungs- und Testprozesse umreißt. Es dient als umfassender Leitfaden, in dem detailliert beschrieben wird, wie unsere Organisation verschiedene Sicherheitsherausforderungen im Zusammenhang mit den genannten Themen in unserem gesamten Betrieb angehen wird. Darüber hinaus dient es als übergeordnetes Dokument, das den Ansatz unserer Organisation in Bezug auf die Sicherheit in Projekten, sowie bei der Entwicklung und dem Testen umreißt.

1.1 Zweck und Umfang

Das Hauptziel dieser Sammlung von Richtlinien in einem Handbuch besteht darin, einen strukturierten Ansatz für die Sicherheit bei der Systementwicklung und dem Testen, sowie im Management von Projekten festzulegen, um sensible Informationen, Vermögenswerte und den Ruf unserer Organisation zu schützen. Durch die Einhaltung dieser Richtlinien wollen wir unsere Widerstandsfähigkeit gegen Sicherheitsverletzungen erhöhen und das Risiko von Unterbrechungen oder Kompromittierungen innerhalb unserer Projektentwicklungs- und Testprozesse minimieren. Die in unserer Organisation für Projekte verantwortlichen Personen haben die Aufgabe, in Zusammenarbeit mit den entsprechenden Abteilungen die Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung der in diesem Handbuch beschriebenen Verfahren zu überwachen.

1.2 Anwendbarkeit

Diese Richtlinien gelten für alle Mitarbeiter, Auftragnehmer, Drittanbieter und Interessengruppen, die in unserer Organisation an der Projektentwicklung oder am Testen beteiligt sind. Sie umfasst alle Aspekte der Projektentwicklung, der Testprozesse und der damit verbundenen Sicherheitsmaßnahmen, unabhängig von der Art oder dem Ort der Projektaktivitäten.

2. Prozessmanagement

2.1 Betriebsverfahren für Informationsverarbeitungsanlagen

2.1.1 Richtlinie

Die Organisation muss die Betriebsverfahren für Informationsverarbeitungsanlagen dokumentieren und relevanten Abteilungen bzw. Personen, die diese für ihre Arbeit benötigen zur Verfügung stellen.

2.1.2 Verfahren

Die in der Richtlinie genannten Betriebsverfahren für Informationsverarbeitende Anlagen müssen identifiziert werden und z.B. im Assetmanagement unter anderem zur Bewertung der Kritikalität in Bezug auf Schutzbedarf (Vertraulichkeit, Verfügbarkeit und Integrität) klassifiziert werden. Als kritisch sollten Betriebsverfahren klassifiziert und durch die Asset-Eigentümer (Fachabteilungen) dokumentiert werden,

1. Wenn die Tätigkeit von vielen Menschen auf dieselbe Weise ausgeführt werden soll.
2. Wenn die Tätigkeit selten ausgeführt wird und das Verfahren bei der nächsten Ausführung wahrscheinlich vergessen wurde.
3. Wenn die Tätigkeit neu ist und bei unsachgemäßer Durchführung ein Risiko darstellt.
4. Vor der Übergabe der Tätigkeit an neues Personal.

Spezifikationen in Betriebsabläufen

In Betriebsabläufen sollen die folgenden Aspekte festgelegt werden:

1. Die verantwortlichen Personen.

2. Sichere Installation und Konfiguration von Systemen.
3. Behandlung und Verarbeitung von Informationen, sowohl automatisiert als auch manuell.
4. Sicherung und Ausfallsicherheit.
5. Zeit- und Aufgabenplanung, einschließlich der Abhängigkeiten von anderen Bedingungen bzw. Systemen.
6. Anweisungen zur Behebung von Fehlern oder anderen außergewöhnlichen Bedingungen (z. B. Einschränkungen bei Versorgungsausfällen), die während der Auftragsausführung auftreten können.
7. Support- und Eskalationskontakte, einschließlich externer Supportkontakte für den Fall unerwarteter betrieblicher oder technischer Schwierigkeiten.
8. Hinweise zur Handhabung von Speichermedien.
9. Verfahren zum Neustart und zur Wiederherstellung des Systems im Falle eines Systemausfalls.
10. Management von Auditberichten und Systemprotokollinformationen und Videoüberwachungssystemen.
11. Überwachungsverfahren wie Kapazität, Leistung und Sicherheit
12. Anweisungen zur Wartung.

3. Projekt- und Änderungsmanagement

3.1 Informationssicherheit in Projekten

3.1.1 Richtlinie

Die Informationssicherheit muss in alle Phasen des Projektmanagements einbezogen werden, um sicherzustellen, dass alle potenziellen Risiken berücksichtigt werden.

3.1.2 Verfahren

Die Berücksichtigung von Informationssicherheit in Projekten ist ein wichtiges Instrument, um in Frühstadien von Entwicklungen, Veränderungen und Produktionsvorhaben Prozesse und Anwendungen sicherer zu gestalten und das Risiko von Sicherheitsvorfällen oder Datenverlusten zu minimieren. Informationssicherheit kann in Projekten durch die folgenden Maßnahmen berücksichtigt werden:

Identifikation von Projekten mit Bezug zur Informationssicherheit:
Die Organisation muss dem Informationssicherheits-(Security-)Team einen Überblick über Projekte mit relevantem Bezug zur Informationssicherheit ermöglichen. Als relevant ist ein Projekt einzustufen, wenn im Projekt sensible oder vertrauliche Informationen verarbeitet, gespeichert oder übertragen werden. Dies kann personenbezogene Daten, geistiges Eigentum, finanzielle Informationen oder andere geschäftskritische Daten umfassen. Zudem sind Projekte als relevant zu klassifizieren, wenn Prozesse oder Anwendungen betroffen sind, die für die Geschäftskontinuität erforderlich sind.

[Bitte erstellen Sie – wenn nicht bereits vorhanden – ein Verzeichnis der relevanten Projekte in Ihrer Organisation. Hierbei sind sowohl Projekte mit Absatz- bzw. Kundenbezug zu berücksichtigen als auch Gestaltungs- und Infrastrukturprojekte Ihrer Organisation bzw. Projekte mit Lieferantenbezug.]

Eindeutigkeit der Projektverantwortung:
Innerhalb von Projekten müssen eindeutige persönliche Verantwortlichkeiten festgelegt sein, damit sichergestellt werden kann, dass die Interessen der Informationssicherheit in Projekten adressiert werden können und Berücksichtigung finden. Im Falle einer Nicht-Berücksichtigung müssen diese Projektverantwortlichen zur Rechenschaft gezogen werden können.

Risikoanalyse und -bewertung:
Das Informationssicherheitsteam hat die Aufgabe, mit dem Projekt-Team eine umfassende Risikoanalyse durchzuführen, um potenzielle Sicherheitsrisiken im Zusammenhang mit dem Projekt zu identifizieren. Dabei müssen unter anderem alle Aspekte von der Datenspeicherung und -übertragung bis hin zur Systemintegration berücksichtigt werden.

Einbeziehung von Sicherheitsanforderungen: In Anlehnung an die Anforderung an die Informationssicherheit in Systemanwendungen und Lieferantenbeziehungen müssen klare Sicherheitsanforderungen für das Projekt definiert und diese in die Projektziele, Spezifikationen und Anforderungen einbezogen werden. Dies kann die Anforderungen an den Datenschutz, Zugriffskontrollen, Verschlüsselung und andere Sicherheitsaspekte umfassen. Das Informationssicherheitsteam bzw. der ISB muss in die Festlegung von Sicherheitsanforderungen involviert werden.

Mandantentrennung in Kundenprojekten: Eine Mandantentrennung in Kundenprojekten bezieht sich auf die Isolierung von Daten, Ressourcen und Funktionen, um sicherzustellen, dass Informationen verschiedener Kunden sicher voneinander getrennt sind. Das umfasst Maßnahmen zur Isolation von Daten auf Datenbankebene, eine grundsätzliche physische und/oder logische mandantenfähige Architektur, Authentifizierung und Autorisierung, Verschlüsselung und Mitarbeitersensibilisierung.

Sicherheitsbewusstsein schaffen: Projektmitarbeiter müssen in Bezug auf bewährte Verfahren zur Informationssicherheit geschult und für die Bedeutung der Sicherheit in ihren jeweiligen Aufgabenbereichen sensibilisiert werden. Hierzu gehört auch die Registrierung und Meldung von Anomalien und Informationssicherheitsereignissen im Projektgeschehen.

Sicherheitskontrollen implementieren: Es müssen geeignete Sicherheitskontrollen und -maßnahmen gemäß den identifizierten Risiken und Sicherheitsanforderungen implementiert werden. Dies kann die Implementierung von Zugriffskontrollen, Verschlüsselung, Firewalls, Intrusion Detection Systems (IDS) und anderen Sicherheitsmaßnahmen umfassen.

Regelmäßige Sicherheitsprüfungen: Während relevanten Projekten müssen regelmäßige Sicherheitsprüfungen und -tests durchgeführt werden, um sicherzustellen, dass die implementierten Sicherheitsmaßnahmen wirksam sind und den Anforderungen entsprechen.

Sicherheitsdokumentation: Alle Sicherheitsaspekte des Projekts, einschließlich der identifizierten Risiken, implementierten Sicherheitsmaßnahmen und durchgeführten Sicherheitsprüfungen sollen dokumentiert werden. Dies ermöglicht eine lückenlose Nachverfolgbarkeit und Transparenz bezüglich der Informationssicherheit im Projekt.

3.2 Änderungsmanagement

3.2.1 Richtlinie

Ein Änderungsmanagement muss an Informationsverarbeitungsanlagen durchgeführt werden, um die Informationssicherheit und Integrität während der Durchführung von Änderungen und Modifikationen zu wahren.

3.2.2 Verfahren

[Bitte ändern Sie diesen Abschnitt, wenn Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für einen exemplarischen Änderungprozess in einem Audit vorzuzeigen]

Rollen und Zuständigkeiten: [ändern Sie diese, wenn Sie andere Rollen oder Zuständigkeiten haben]

1. **Antragsteller einer Änderung:** Jede Person oder jedes Team, die/der eine Änderung an Einrichtungen oder Systemen zur Informationsverarbeitung vorschlägt.
2. **Eigentümer der Änderung:** Verantwortlich für die Beaufsichtigung des Änderungsprozesses, die Einholung von Genehmigungen und die Sicherstellung der Einhaltung der Vorschriften.
3. **Änderungsprüfungsausschuss (Change Advisory Board = CAB):** Eine benannte Gruppe, die für die Überprüfung und Genehmigung von Änderungsvorschlägen zuständig ist. [Dies kann z.B. auch das Informationssicherheits-(Security-)Team in Zusammenarbeit mit der Gruppe der betroffenen Asset- & Risikoeigentümern sein]
4. **Umsetzungsteam:** Verantwortlich für die kontrollierte Durchführung der genehmigten Änderungen.
5. **Koordinator der Änderung:** Erleichtert die Kommunikation und Koordination zwischen den Beteiligten während des gesamten Veränderungsprozesses.

Einreichung von Änderungsanträgen:

- Der Antragsteller reicht ein formelles Änderungsantragsformular ein, in dem er die vorgeschlagene Änderung, die Gründe und die möglichen Auswirkungen darlegt.
- Das Änderungs-Anfrageformular wird vom Eigentümer der Änderung auf Vollständigkeit und Richtigkeit geprüft.

Überprüfung und Genehmigung von Änderungen

- Der Änderungseigentümer legt den Änderungsantrag dem Änderungsprüfungsausschuss zur Bewertung vor.
- Der Änderungsprüfungsausschuss bewertet die vorgeschlagene Änderung und berücksichtigt dabei Faktoren wie potenzielle Risiken, Abhängigkeiten und die Übereinstimmung mit den Organisationszielen.

- Falls erforderlich, kann der Änderungsprüfungsausschuss zusätzliche Informationen oder Klarstellungen vom Initiator der Änderung verlangen.
- Auf der Grundlage der Überprüfung genehmigt der Änderungsprüfungsausschuss den Änderungsantrag entweder, lehnt ihn ab oder verschiebt ihn.
- Genehmigte Änderungen werden mit einer Änderungs-ID versehen und durchlaufen die nächste Stufe des Änderungsmanagementprozesses.

Planung und Bewertung von Änderungen:

- Der Eigentümer der Änderung entwickelt einen detaillierten Plan für die Implementierung der genehmigten Änderung, einschließlich Zeitplan, Ressourcenbedarf und Testverfahren.
- Potenzielle Auswirkungen der Änderung werden unter Berücksichtigung von Abhängigkeiten, Systemzusammenhängen und Bedürfnissen der Beteiligten bewertet.

Prüfung und Validierung:

- Änderungen werden in einer kontrollierten Umgebung gründlich getestet, um die Funktionalität, Leistung und Sicherheit zu überprüfen.
- Die Auditergebnisse werden dokumentiert und überprüft, um die Einhaltung der Abnahmekriterien sicherzustellen.

Durchführung:

- Das Umsetzungsteam führt die genehmigten Änderungen gemäß dem festgelegten Plan und Zeitplan durch.
- Die Umsetzungsaktivitäten werden genau überwacht, um etwaige Probleme oder Abweichungen vom Plan zu erkennen und zu beheben.

Kommunikation und Einbeziehung von Interessengruppen:

- Während des gesamten Veränderungsprozesses werden die Beteiligten über Fortschritte, mögliche Auswirkungen und notwendige Maßnahmen informiert.
- Es werden klare Kommunikationskanäle eingerichtet, um die Zusammenarbeit zu erleichtern und Bedenken auszuräumen.

Dokumentation und Aufzeichnungen:

- Umfassende Aufzeichnungen über alle änderungsbezogenen Aktivitäten, einschließlich Genehmigungen, Testergebnissen und Implementierungsdetails, werden in einem zentralen Repository aufbewahrt.
- Die Dokumentation wird bei Bedarf aktualisiert, um Änderungen an den Informationsverarbeitungseinrichtungen und -systemen zu berücksichtigen.

4. Sichere Entwicklung & Programmierung

4.1 Der Lebenszyklus einer sicheren Entwicklung

[Bitte ändern Sie diesen Abschnitt, wenn Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für einen exemplarischen durchgeführten Prozess in einem Audit vorzuzeigen.]

4.1.1 Richtlinie

Der sichere Entwicklungszyklus (Software Development Lifecycle = SDLC) von Software und Systemen muss so gestaltet werden, dass die Informationssicherheit in den Lebenszyklus der Entwicklung integriert wird.

4.1.2 Verfahren

Rollen & Zuständigkeiten: [ändern Sie diese, wenn Sie andere Rollen oder Zuständigkeiten haben]

1. Abteilung für IT-Sicherheit:

- Verantwortlich für die Beaufsichtigung der Umsetzung sicherer Entwicklungspraktiken.

- Durchführung regelmäßiger IT-Sicherheitsaudits und Bewertungen, um die Einhaltung der Richtlinie zu gewährleisten.
- Beratung und Unterstützung der Entwicklungsteams bei bewährten Sicherheitsverfahren.

2. Entwicklungsteams:

- Verantwortlich für die Einhaltung der in diesem Verfahren dargelegten sicheren Entwicklungspraktiken.
- Zusammenarbeit mit der IT-Sicherheitsabteilung, um etwaige Sicherheitsbedenken während des Entwicklungslebenszyklus zu beseitigen.

Verfahren:

[Dies ist ein Standardverfahren für einen SDLC. Passen Sie ihn ggf. an ihre Organisation an]

a) Trennung der Umgebungen:

- Betrieb von getrennten Entwicklungs-, Test- und Produktionsumgebungen, um unbefugten Zugriff zu verhindern und die Integrität der Produktionssysteme zu gewährleisten.
- Implementierung von Zugangskontrollen und Aufgabentrennung, um den Zugang zu Produktionsumgebungen zu beschränken.

b) Integration der Sicherheit in den SDLC:

- Integration der Sicherheit in jede Phase des Softwareentwicklungszyklus (SDLC), einschließlich Anforderungserfassung, Entwurf, Kodierung, Tests, Bereitstellung und Wartung.
- Einbeziehung von Richtlinien zur sicheren Kodierung und bewährten Verfahren für jede bei der Entwicklung verwendete Programmiersprache.

c) Sicherheitsanforderungen und Kontrollpunkte:

- Definition von Sicherheitsanforderungen während der Spezifikations- und Entwurfsphase der Software- und Systementwicklung.
- Einrichtung von Sicherheitskontrollpunkten (z.B. in Form von Milestones) während der Projekte, um die Einhaltung der Sicherheitsstandards und -richtlinien zu überprüfen und zu bestätigen.

d) System- und Sicherheitstests:

- Durchführung umfassender System- und Sicherheitstests, einschließlich Regressionstests, Code-Scans und Penetrationstests, um Schwachstellen zu erkennen und zu beseitigen.
- Dokumentation und Priorisierung der festgestellten Sicherheitsprobleme zur Behebung.

e) Sichere Quellcode- und Konfigurationsrepositories:

- Nutzung von sicheren Repositories für die Speicherung von Quellcode und Konfigurationsdateien und implementierung von Zugriffskontrollen, Verschlüsselung und Versionskontrolle.
- Regelmäßige Überprüfung von Zugriffsberechtigungen und Repository-Aktivitäten, um unbefugte Zugriffe oder Änderungen zu erkennen.

f) Sicherheit der Versionierung:

- Implementierung von Sicherheitsmaßnahmen in Versionierungssystemen, um Änderungen zu verfolgen, Zugriffsregelungen durchzusetzen und die Integrität von Code-Repositories zu gewährleisten.
- Durchsetzung von Code-Review-Prozessen zur Validierung von Änderungen vor dem Zusammenführen in den Hauptcode.

g) Kenntnisse und Schulungen zur Anwendungssicherheit:

- Schulung von Entwicklern zu den Grundsätzen der Anwendungssicherheit, zu sicheren Codierungsverfahren und zu neuen Bedrohungen.
- Förderung der kontinuierlichen Weiterbildung und des Ausbaus von Fähigkeiten, um über Sicherheitstrends und bewährte Verfahren auf dem Laufenden zu bleiben.

g) Entwicklerfähigkeiten für das Schwachstellenmanagement:

- Ausstattung von Entwicklern mit Tools und Ressourcen für das Schwachstellenmanagement, einschließlich

Codeanalysetools, Sicherheitsbibliotheken und Verfahren zur Reaktion auf Vorfälle.

- Förderung einer Kultur des proaktiven Schwachstellenmanagements, die Entwickler dazu ermutigt, Sicherheitsprobleme umgehend zu melden und zu beheben.

h) Lizensierungsanforderungen und Alternativen:

- Bewertung von Software- und Systemkomponenten im Hinblick auf Lizenzanforderungen und Prüfung kostengünstiger Alternativen, um die Einhaltung der Vorschriften zu gewährleisten.
- Dokumentieren Sie Lizenzvereinbarungen und stellen Sie sicher, dass alle in der Entwicklung verwendeten Softwarekomponenten ordnungsgemäß lizenziert sind. Das betrifft bezahlte, sowie open-source Lizenzen.

l) Ausgelagerte Entwicklung:

[Bitte verweisen Sie hier auf Ihr entsprechendes Kapitel in der Richtlinie zum Lieferantenmanagement]

Wenn die Entwicklung ausgelagert wird, muss sichergestellt werden, dass der Drittanbieter die Anforderungen der Organisation an eine sichere Entwicklung erfüllt, und es muss bei Bedarf eine Überwachung stattfinden.

j) Dokumentation und Berichterstattung:

- Pflege der Dokumentation von sicheren Entwicklungsaktivitäten, einschließlich Sicherheitsanforderungen, Testergebnissen und Abhilfemaßnahmen.
- Erstellung regelmäßiger Berichte über die Sicherheitslage, Schwachstellen und den Stand der Einhaltung der Vorschriften zur Überprüfung durch das Management.

4.2 Sichere Systemarchitektur und technische Grundsätze

[Bitte ändern Sie diesen Abschnitt, wenn Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für einen exemplarischen durchgeführten Prozess in einem Audit vorzuzeigen.]

4.2.1 Richtlinie

Eine sichere Systemarchitektur muss während des Lebenszyklus der Entwicklung eines Informationssystems erstellt, dokumentiert, gepflegt und angewendet werden.

4.2.2 Verfahren

Rollen & Zuständigkeiten: [ändern Sie diese, wenn Sie andere Rollen oder Zuständigkeiten haben]

1. Spezialist für Informationssicherheit:

- Durchführung von Risikobewertungen und Bereitstellung von Fachwissen zur Festlegung von Grundsätzen der Sicherheitstechnik.
- Zusammenarbeit mit den Entwicklungsteams, um die Einhaltung der Sicherheitsgrundsätze während des gesamten Entwicklungszyklus zu gewährleisten.

2. Entwicklungsteams:

- Anwendung von Grundsätzen der IT-Sicherheit beim Entwurf, der Entwicklung und dem Einsatz von Informationssystemen.
- Mitteilung aller Herausforderungen oder Abweichungen von den Sicherheitsgrundsätzen an den Spezialisten für Informationssicherheit.

Verfahren:
[Im Folgenden werden alle verschiedenen Systemarchitektur- und Konstruktionsprinzipien in der Organisation aufgelistet; überprüfen Sie, ob alles richtig ist und ändern Sie es entsprechend]

a) Einrichtung einer Sicherheitssystemarchitektur:

- Definition und Dokumentation von Prinzipien der Sicherheitstechnik auf der Grundlage von Industriestandards, organisatorischen Anforderungen und bewährten Verfahren.

- Sicherstellen, dass die Sicherheitsgrundsätze alle Architekturebenen abdecken, einschließlich Unternehmen, Daten, Anwendungen und Technologien.

b) Risikoanalyse und Bedrohungsmodellierung:

- Durchführung von Risikobewertungen zur Ermittlung potenzieller Sicherheitsbedrohungen und Schwachstellen im Zusammenhang mit der Entwicklung von Informationssystemen.
- Durchführung von Bedrohungsmodellierungsübungen, um Angriffsmuster und potenzielle Sicherheitsschwächen zu verstehen.

c) Integration von "Security by Design":

- Umsetzung von Grundsätzen der "Security by Design", einschließlich "Defense in Depth", "Security by Default" und "Least Privilege", in der Architektur- und Entwurfsphase.
- Sicherstellen, dass die Sicherheitskontrollen auf jeder Ebene des Informationssystems integriert sind.

d) Anwendung der Zero-Trust-Prinzipien:

- Anwendung von Zero-Trust-Prinzipien wie "Vertrauen, aber überprüfen" und dynamische Zugangskontrolle, um den Zugang zu Informationssystemen zu authentifizieren und zu autorisieren.
- Implementieren Sie Verschlüsselungs- und starke Authentifizierungsmechanismen, um die Sicherheit zu erhöhen.

e) Sicherheitsüberprüfung und Dokumentation:

- Durchführung sicherheitsorientierter Entwurfsprüfungen zur Ermittlung und Behebung von Sicherheitsschwachstellen und zur Gewährleistung der Einhaltung von Sicherheitsgrundsätzen.
- Dokumentieren Sie die Sicherheitskontrollen, einschließlich aller Abweichungen oder Ausnahmen, und holen Sie die formale Bestätigung der relevanten Beteiligten ein.

f) Ausgelagerte Überwachung der Entwicklung:

- Sicherstellung, dass ausgelagerte Entwicklungstätigkeiten durch vertragliche Vereinbarungen die festgelegten Grundsätze der Sicherheitstechnik einhalten.
- Überprüfung und Überwachung der Sicherheitspraktiken der Lieferanten, um die Übereinstimmung mit den Unternehmensstandards zu gewährleisten.

g) Regelmäßige Überprüfung und Aktualisierung:

- Regelmäßige Überprüfung der sicherheitstechnischen Grundsätze, um Aktualisierungen auf der Grundlage neuer Bedrohungen, technologischer Fortschritte und organisatorischer Erfordernisse einzubeziehen.
- Aktualisierung der Sicherheitsverfahren und -leitlinien zur Berücksichtigung von Änderungen in der Sicherheitstechnik.

4.3 Sichere Programmierung

4.3.1 Richtlinie

Bei der Softwareentwicklung müssen die Grundsätze der sicheren Kodierung eingehalten werden, um die Zahl der potenziellen Sicherheitslücken in der Software zu verringern.

4.3.2 Verfahren

Rollen & Zuständigkeiten: [ändern Sie diese, wenn Sie andere Rollen oder Zuständigkeiten haben]

1. Entwicklungsteam:

- Verantwortlich für die Umsetzung sicherer Programmierungspraktiken bei der Entwicklung von Software.
- Zusammenarbeit mit dem Informationssicherheits-(Security-)Team, um die Einhaltung der Grundsätze der sicheren Programmierung zu gewährleisten.

2. Spezialist für IT-Sicherheit:

- Beratung und Unterstützung von Entwicklungsteams in Bezug auf sichere Programmierverfahren.

- Durchführung regelmäßiger Überprüfungen, um die Einhaltung der Standards für sichere Programmierung zu gewährleisten.

Verfahren:

a) Sichere Programmierungsprozesse einrichten:

- Definition von organisationsweiten Prozessen für die Steuerung der sicheren Programmierung, einschließlich der Festlegung eines Mindestmaßes an Sicherheit.
- Vermittlung von Standards für sichere Programmierung und Erwartungen an alle Entwicklungsteams.

b) Schulung und Sensibilisierung:

- Durchführung von Schulungen für Entwickler zu den Grundsätzen der sicheren Programmierung, bewährten Verfahren und Techniken.
- Sicherstellen, dass die Entwickler mit den organisationsspezifischen Standards für sichere Programmierung vertraut sind.

c) Planung und Voraussetzungen:

- Bevor mit der Programmierung begonnen wird, sollen Sie die unternehmensspezifischen Grundsätze der sicheren Programmierung und die anerkannten Standards prüfen und verstehen.
- Konfigurieren der Entwicklungswerkzeuge wie IDEs so, dass sichere Programmierungspraktiken durchgesetzt werden.
- Sicherstellen, dass die Entwickler für das Schreiben von sicherem Code qualifiziert sind und Zugang zu den erforderlichen Ressourcen und Tools haben.

d) Während der Programmierung:

- Implementierung sicherer Programmierungspraktiken, die für die verwendeten Programmiersprachen und -techniken spezifisch sind.
- Sichere Programmiertechniken wie Pair Programming, Peer Review und testgetriebene Entwicklung anwenden.
- Sorgfältige Dokumentation des Codes und umgehende Behebung von festgestellten Programmierfehlern.

e) Prüfung und Bewertung:

- Durchführung von Tests während des gesamten Entwicklungsprozesses, einschließlich statischer Anwendungssicherheitstests (SAST), um Sicherheitsschwachstellen zu ermitteln und zu beseitigen.
- Bewertung von Angriffspotenzial und Sicherstellung, dass das Prinzip der geringsten Privilegien (least privilidge) angewendet wird, bevor die Software bereitgestellt wird.

f) Überprüfung und Wartung:

- Sicheres „Containern“ und Verteilen von Software-Updates, um sicherzustellen, dass alle gemeldeten Sicherheitslücken umgehend behoben werden.
- Protokollierung von Fehlern und vermuteten Angriffen, regelmäßige Überprüfung der Protokolle, um notwendige Anpassungen des Codes vorzunehmen.
- Schutz des Quellcodes vor unbefugtem Zugriff und Manipulation durch Versionskontrolle und Zugriffskontrollmechanismen.

g) Verwendung von externen Tools und Bibliotheken:

- Effiziente Verwaltung externer Bibliotheken, Gewährleistung regelmäßiger Aktualisierungen und Führung eines Inventars der verwendeten Bibliotheken und Versionen.
- Sorgfältige Prüfung externer Komponenten und Berücksichtigung von Faktoren wie Lizenz, Sicherheit und Historie, bevor diese in Software integriert werden.

h) Modifizierung von Softwarepaketen:

- Bewertung des Risikos und der Auswirkungen von Änderungen an Softwarepaketen, ggf. Einholung der erforderlichen Genehmigungen und Zustimmung der Anbieter.
- Sicherstellung der Kompatibilität mit bestehenden Systemen und Berücksichtigung auch von langfristigen Auswirkungen auf die Wartung, bevor Änderungen vorgenommen werden.

5. Testen der Entwicklung

5.1 Sicherheitstests in Entwicklung und Abnahme

[Bitte ändern Sie diesen Abschnitt, wenn Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für einen exemplarischen durchgeführten Prozess in einem Audit vorzuzeigen.]

5.1.1 Richtlinie

Sicherheitstests müssen während des gesamten Entwicklungszyklus von Softwareanwendungen durchgeführt werden, um die Einhaltung der IT-Sicherheitsanforderungen zu überprüfen und potenziell ausnutzbare Anwendungsschwachstellen zu reduzieren.

5.1.2 Verfahren

[Dies ist ein Standardverfahren für die Sicherheitsprüfung von Systemen. Bitte vergewissern Sie sich, dass dieses Ihrem tatsächlichen Prozess entspricht und passen sie es ggf. an Ihre Organisation an.]

1. Integration von Sicherheitstests:

Sicherstellen, dass Sicherheitstests in den gesamten Testprozess für alle Softwaresysteme, Upgrades und neue Versionen während des Entwicklungslebenszyklus und des Projektmanagements integriert werden.

2. Umfang der Sicherheitstests:

a) Prüfung von Sicherheitsfunktionen wie Benutzerauthentifizierung, Zugangsbeschränkung und Kryptographie.

b) Prüfung sicherer Programmierverfahren.

c) Prüfung der Konfigurationen von Betriebssystemen, Firewalls und anderen Sicherheitskomponenten.

3. Testen:

a) Faktoren, die die Bedeutung des Systems, die Art der Änderungen und die möglichen Auswirkungen betreffen.

b) Jeder Test soll Folgendes umfassen:

- Zeitplan für Aktivitäten und Tests.
- Erwartete Inputs und Outputs unter verschiedenen Bedingungen.
- Kriterien für die Bewertung der Testergebnisse.
- Maßnahmen zur Abhilfe.

3.a Während der Entwicklung: [Bitte beschreiben Sie ihre anzuwendenden Verfahren]

1. **Statische Prüfung der Anwendungssicherheit (SAST)**: Hierbei wird der Quellcode einer Anwendung auf Sicherheitsschwachstellen untersucht. Sie werden in der Regel zu Beginn des Entwicklungsprozesses durchgeführt.
2. **Dynamische Prüfung der Anwendungssicherheit (DAST)**: Hierbei handelt es sich um eine Art von Black-Box-Sicherheitstests, bei denen die Anwendung von außen nach innen auf Schwachstellen geprüft wird, die ein Angreifer ausnutzen könnte.
3. **Interaktives Prüfen der Anwendungssicherheit (IAST)**: Hierbei werden Elemente von SAST und DAST kombiniert, um Schwachstellen in einer Anwendung zu ermitteln.
4. **Software Composition Analyse (SCA)**: Hierbei werden Open-Source-Komponenten in Ihrer Codebasis identifiziert und auf bekannte Schwachstellen überprüft.

3.b Akzeptanzprüfung:
[Umzusetzen sobald das System erstellt wurde, aber bevor es für die Benutzer in den Produktionsbetrieb überführt wird (dies soll auch in bestimmten Abständen nach der Überführung in den Produktionsbetrieb geschehen)]:

1. **Penetrationstests**: Hierbei wird ein realer Angriff auf ein System simuliert, um Schwachstellen zu ermitteln, die von Angreifern ausgenutzt werden könnten. Er wird normalerweise gegen Ende des Entwicklungszyklus durchgeführt.

2. **Sicherheitsprüfung**: Hierbei handelt es sich um eine gründliche Prüfung des Systems, um sicherzustellen, dass es den Sicherheitsstandards und -vorschriften entspricht.
3. **Risikobewertung**: Dabei werden die Risiken für das System identifiziert, bewertet und nach Prioritäten geordnet.

3.c Sicherheitsakzeptanz:

- Integration der Sicherheitsakzeptanz in die Phasen des Projektmanagements.
- Einbeziehung in das Genehmigungsverfahren für die Projektphase.

[Nachfolgend finden Sie eine Liste von Testmethoden. Bitte überprüfen Sie, ob diese Methoden in Ihrer Organisation für das Testen der Systementwicklung verwendet werden und passen Sie diese ggf. entsprechend an. Es gilt als „Best Practice“ für Organisationen, diese Schritte als Minimum zu befolgen.]

3.d Automatisierte Werkzeuge:

- Einsatz automatisierter Tools wie Code-Analyse-Tools und Schwachstellen-Scanner zur Unterstützung der Sicherheitstests.
- Sicherstellung, dass festgestellte sicherheitsrelevante Mängel behoben und überprüft werden.

3.e Durchführung von internen Entwicklungstests:

- Die ersten Sicherheitstests sollen vom Entwicklungsteam durchgeführt werden.
- Durchführung von Code-Review-Aktivitäten, Schwachstellen-Scans und Penetrationstests als Teil der internen Tests.
- Durchführung unabhängiger Abnahmetests, um zu bestätigen, dass das System wie erwartet funktioniert und die Sicherheitsanforderungen erfüllt.

3.f Verwaltung der ausgelagerten Entwicklung und Beschaffung:

- Befolgung der Prozesse für die ausgelagerte Entwicklung und Beschaffung von Komponenten.
- Sicherstellung, dass die Verträge mit den Zulieferern die ermittelten Sicherheitsanforderungen berücksichtigen.
- Bewertung von Produkten/Dienstleistungen anhand von Sicherheitskriterien vor dem Erwerb.

3.g Anpassen der Testumgebung:

- Führen Sie die Tests in einer Testumgebung durch, die der Produktionsumgebung sehr ähnlich ist, um Zuverlässigkeit zu gewährleisten und die Einführung von Schwachstellen zu verhindern.
- Einrichtung mehrerer Testumgebungen für verschiedene Arten von Tests, einschließlich Funktions- und Leistungstests.

3.h Sicherstellung von Tests und Überwachung:

- Implementierung effektiver Tests und Überwachung von Testumgebungen, Tools und Technologien.
- Überwachung der Überwachungssysteme, die in Entwicklungs-, Test- und Produktionsumgebungen eingesetzt werden, um deren Wirksamkeit sicherzustellen.

3.i Dokumentation und Berichterstattung:

- Dokumentation aller Sicherheitstests, einschließlich Testplänen, Ergebnissen und Abhilfemaßnahmen.
- Meldung aller festgestellten Sicherheitsschwachstellen und des Stands ihrer Behebung an die zuständigen Stellen.

5.2 Trennung von Entwicklungs-, Test- und Produktionsumgebung

5.2.1 Richtlinie

Die Trennung und Sicherheit von Entwicklungs-, Test- und Produktionsumgebungen muss umgesetzt werden, um die Produktionsumgebung und -daten vor Kompromissen und Datenverschmutzung durch Entwicklungs- und Testaktivitäten zu schützen.

5.2.2 Verfahren

[Bei diesem Verfahren geht es darum, wie Sie Ihre verschiedenen Entwicklungsumgebungen aufteilen. Dieses Verfahren ist ein Standardverfahren. Bitte vergewissern Sie sich, dass dieses Ihrem tatsächlichen Prozess entspricht und passen sie es ggf. an Ihre Organisation an.]

Umgebungstrennung:

- Trennung von Entwicklungs-, Test- und Produktionsumgebungen je nach den Bedürfnissen des Unternehmens.
- Einrichtung von separaten physischen oder virtuellen Umgebungen für Entwicklungs-, Test- und Produktionssysteme und Sicherstellung, dass diese voneinander isoliert sind.

Regeln für die Bereitstellung:

- Definition und Dokumentation von Regeln und Genehmigungsverfahren für die Bereitstellung von Software aus der Entwicklungsumgebung in der Produktionsumgebung.
- Implementierung eines Änderungsmanagementprozesses zur Überprüfung und Genehmigung von Softwareeinführungen in der Produktionsumgebung.

Prüfung und Inszenierung:

- Durchführung von gründlichen Tests von Softwareänderungen in einer Test- oder Staging-Umgebung, bevor diese in der Produktionsumgebung eingesetzt werden.
- Sicherstellung, dass alle Änderungen strengen Tests unterzogen werden, um mögliche Probleme oder Schwachstellen zu ermitteln und zu beheben.

Zugangskontrolle:

- Beschränkung des Zugangs zu Entwicklungs- und Testumgebungen auf befugtes Personal.
- Sicherstellung, dass Entwicklungstools und Dienstprogramme nicht von Produktionssystemen aus zugänglich sind, um unbefugten Zugriff oder Änderungen zu verhindern.
- Implementierung von Zugangskontrollen und Authentifizierungsmechanismen, um sicherzustellen, dass nur autorisierte Personen Änderungen an den Produktionssystemen vornehmen können.

Schutz der Umgebungen:

- Regelmäßige Patches und Updates für Entwicklungs-, Test- und Produktionssysteme, um Sicherheitslücken zu schließen und sicherzustellen, dass sie auf dem neuesten Stand sind.
- Implementierung sicherer Konfigurationen für alle Systeme und Softwarekomponenten, um das Risiko eines Missbrauchs zu minimieren.
- Überwachung von Änderungen an der Umgebung und dem darin gespeicherten Code, um unbefugte Änderungen oder Zugriffe zu erkennen.
- Durchführung regelmäßiger Backups von Entwicklungs-, Test- und Produktionsumgebungen, um die Integrität und Verfügbarkeit der Daten zu gewährleisten.

Trennung der Zuständigkeiten:

- Einführung von Kontrollen, die sicherstellen, dass die für die Entwicklungstätigkeiten zuständigen Personen nicht in der Lage sind, ohne entsprechende Genehmigung Änderungen an den Produktionssystemen vorzunehmen.
- Überwachung und Überprüfung von Zugriffsprotokollen und Prüfpfaden, um unbefugte Änderungen oder unbefugten Zugriff auf Produktionssysteme zu erkennen und zu verhindern.

5.3 Testinformationen

5.3.1 Richtlinie

Sensible betriebliche Informationen (einschließlich personenbezogener Daten) müssen geschützt werden und dürfen daher nicht zu Testzwecken verwendet werden.

5.3.2 Verfahren

[Testinformationen sind alle Daten, die zum Testen der von Ihnen entwickelten Systeme verwendet werden; das nachstehende Verfahren gibt Ihnen ein Verfahren für die Verwaltung solcher Daten. Bitte vergewissern Sie sich, dass dieses Ihrem tatsächlichen Prozess entspricht und passen sie es ggf. an Ihre Organisation an.]

Auswahl der Testinformationen:

- Die Auswahl der Testinformationen erfolgt auf der Grundlage ihrer Relevanz für die Testziele und ihrer Fähigkeit, betriebliche Szenarien genau darzustellen.
- Bevor betriebliche Informationen in Testumgebungen kopiert werden, muss eine gründliche Bewertung durchgeführt werden, um die Notwendigkeit und Eignung der Daten für Testzwecke festzustellen.
- Sensible Informationen, einschließlich personenbezogener Daten (PII), dürfen nicht in Testumgebungen verwendet werden. Wenn sie für den Test unerlässlich sind, müssen sie anonymisiert werden, um unbefugten Zugang oder Offenlegung zu verhindern.

Schutz von Testumgebungen:

- Es müssen Zugangskontrollen implementiert werden, um den Zugang zu Testumgebungen zu beschränken und sicherzustellen, dass nur befugtes Personal die Erlaubnis hat, Testinformationen einzusehen oder zu manipulieren.
- Jedes Kopieren betrieblicher Informationen in eine Testumgebung bedarf der ausdrücklichen Genehmigung durch die Asset-Eigentümer. Es sind Aufzeichnungen über solche Aktivitäten zu Prüfzwecken zu führen.
- Sensible Informationen, die für Tests verwendet werden, müssen in geeigneter Weise maskiert oder anonymisiert werden, um eine unbefugte Offenlegung zu verhindern und gleichzeitig die Integrität des Testprozesses zu wahren.

Einhaltung und Überwachung:

- Es werden regelmäßige Audits und Bewertungen durchgeführt, um die Einhaltung der Verfahren zur Verwaltung von Testinformationen zu überprüfen und etwaige Verstöße zu ermitteln.
- Es sollen Überwachungsinstrumente und -techniken eingesetzt werden, um den Zugang zu Testumgebungen zu verfolgen und unbefugte Aktivitäten oder Sicherheitsverstöße aufzudecken.
- Alle Abweichungen von den festgelegten Verfahren oder bewusste Verstöße müssen unverzüglich untersucht, dokumentiert und erforderlichenfalls behoben werden.

5.4 Schutz der Informationssysteme während eines Audits

5.4.1 Richtlinie

Audit-Tests und andere Überprüfungstätigkeiten, die eine Bewertung der operativen Systeme beinhalten, sollen konzeptionell geplant und zwischen dem Auditor und der zuständigen Geschäftsleitung abgestimmt werden.

5.4.2 Verfahren

[In diesem Verfahren geht es um die Auditierung Ihrer Systeme; die nachstehenden Schritte erläutern, wie Sie diese Audits planen und durchführen sollen; diese Schritte sind eine gute Praxis und sollen als Minimum für diese Maßnahme verstanden werden.]

Planung und Vereinbarung:

- Vor der Einleitung von Audit-Tests oder Überprüfungsaktivitäten muss der der Auditor mit der zuständigen Geschäftsleitung den Umfang, die Ziele und die möglichen Auswirkungen der vorgeschlagenen Aktivitäten abstimmen.
- Zwischen dem Auditor und der Geschäftsleitung ist eine förmliche Vereinbarung über den Zeitplan, die Ressourcen und die Zugangsberechtigungen für die Durchführung der Audit-Tests zu treffen.

Umfang und Grenzen:

- Der Auditor muss den Umfang der technischen Audits festlegen und dabei sicherstellen, dass sie sich auf Bereiche konzentrieren, die für die Sicherheitslage der Organisation und die Einhaltung der Anforderungen relevant sind.
- Beschränkungen und Einschränkungen im Zusammenhang mit den Audit-Tests, wie z. B. Zugriffsbeschränkungen und Systemabhängigkeiten, sind zu ermitteln und zu dokumentieren, um unbeabsichtigte Folgen zu vermeiden.

Zugangskontrolle und Sicherheitsanforderungen:

- Anträge auf Zugang für Prüfungszwecke sind unter Angabe des Zwecks und der Dauer des gewünschten Zugangs der zuständigen Leitung zur Genehmigung vorzulegen.
- Vor der Gewährung des Zugangs prüft das IT-Sicherheitsteam die Sicherheitslage der für den Zugang zu den operativen Systemen verwendeten Geräte und stellt sicher, dass die festgelegten Sicherheitsanforderungen eingehalten werden.

Testdurchführung und -überwachung:

Die Audit-Tests müssen gemäß dem vereinbarten Plan durchgeführt werden, wobei sorgfältig darauf geachtet werden muss, dass die betrieblichen Systeme und Geschäftsprozesse so wenig wie möglich gestört werden.

- Während der Durchführung von Audit-Tests müssen die Zugriffsaktivitäten und Systeminteraktionen kontinuierlich überwacht und protokolliert werden, um die Transparenz und Rechenschaftspflicht aufrechtzuerhalten.

Zeitplan und Koordinierung:

- Audit-Tests, die sich auf die Systemverfügbarkeit oder -leistung auswirken können, sind so zu planen und mit den Beteiligten abzustimmen, dass der normale Betrieb möglichst wenig gestört wird.
- Die Koordinierung umfasst auch die Unterrichtung der Systemadministratoren und anderer zuständiger Mitarbeiter über den Zeitplan und die Art der Audit-Aktivitäten, um die Zusammenarbeit und Unterstützung sicherzustellen.

6. Norm-Referenzen

6.1 Normreferenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. **Einleitung**	
2. **Prozessmanagement**	
• 2.1 Betriebsverfahren für Informationsverarbeitungsanlagen	A 5.37
3. **Projekt- und Änderungsmanagement**	
• 3.1 Informationssicherheit in Projekten	A 5.8
• 3.2 Änderungsmanagement	A 8.32
4. **Sichere Entwicklung und Programmierung**	
• 4.1 Der Lebenszyklus einer sicheren Entwicklung	A 8.25
• 4.2 Sichere Systemarchitektur und technische Grundsätze	A 8.27
• 4.3 Sichere Programmierung	A 8.28
5. **Testen der Entwicklung**	
• 5.1 Sicherheitstests in Entwicklung und Abnahme	A 8.29

• 5.2 Trennung von Entwicklungs-, Test- und Produktumgebung	A 8.31
• 5.3 Testinformationen	A 8.33
• 5.4 Schutz der Informationssysteme während eines Audits	A 8.34

6.2 Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	Normkapitel (ISA-TISAX 6.0)
1. **Einleitung**	
2. Prozessmanagement	
• 2.1 Betriebsverfahren für Informationsverarbeitungsanlagen	1.5.1
3. **Projekt- und Änderungsmanagement**	
• 3.1 Informationssicherheit in Projekten	1.2.3; 1.4.1; 5.3.1
• 3.2 Änderungsmanagement	5.2.1; 5.3.1
4. **Sichere Entwicklung und Programmierung**	
• 4.1 Der Lebenszyklus einer sicheren Entwicklung	5.3.1
• 4.2 Sichere Systemarchitektur und technische Grundsätze	5.3.1
• 4.3 Sichere Programmierung	5.3.1
5. **Testen der Entwicklung**	
• 5.1 Sicherheitstests in Entwicklung und Abnahme	5.3.1
• 5.2 Trennung von Entwicklungs-, Test- und Produktumgebung	5.2.2
• 5.3 Testinformationen	5.3.1
• 5.4 Schutz der Informationssysteme während eines Audits	5.2.6