[Name der Organisation]

ST5 Handbuch zur Mitarbeitersicherheit, Schulung und Compliance

Version	**1.0**
Eigentümer der Richtlinie	Name eintragen
Geprüft von	Name oder Rolle eintragen
Prüfdatum	Datum eintragen
Gültig ab	Datum eintragen
Nächste Überprüfung	Datum eintragen
Vertraulichkeitsklasse	INTERN

Änderungsverlauf

Datum	Version	Erstellt von	Beschreibung der Änderung
27.05.25	0.93	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

Das Handbuch zur Mitarbeitersicherheit, Schulung und Compliance beschreibt die übergeordnete Strategie zur Steuerung der Informationssicherheit von [Name der Organisation] in der Mitarbeiterverwaltung, effektiven Schulung und Einhaltung der Vorschriften im ISMS durch unsere Mitarbeiter. Sie dient als umfassender Leitfaden, in dem beschrieben wird, wie wir die verschiedenen Herausforderungen im Zusammenhang mit der Kompetenzfeststellung und Schulung von Mitarbeitern und der Einhaltung von Vorschriften in unserer Organisation angehen.

1.1 Zweck und Umfang

Zweck dieser Richtliniensammlung ist es, einen strukturierten Ansatz für die Schulung von Mitarbeitern und die Einhaltung von Vorschriften festzulegen, sowie die erforderliche Kompetenz von Mitarbeitern festzustellen, um die sensiblen Daten unserer Organisation zu schützen, die Integrität der Infrastruktur aufrechtzuerhalten und unseren Ruf zu wahren. Durch die Einhaltung dieser Richtlinien wollen wir unsere Widerstandsfähigkeit gegenüber Compliance-Verstößen erhöhen und damit das Risiko der Nichteinhaltung von Vorschriften oder internen Richtlinien minimieren. Sie umfasst die Beschreibung der Anforderungen der Informationssicherheit an die Mitarbeiterverwaltung, Schulungsprogramme, Compliance-Anforderungen und Aktivitäten im Zusammenhang mit dem Verhalten der Mitarbeiter, unabhängig von deren Rolle oder Abteilung.

1.2 Anwendbarkeit

Diese Richtlinie gilt für alle Mitarbeiter sowie relevante Auftragnehmer, Drittanbieter von Dienstleistungen und Interessengruppen, die an Aktivitäten innerhalb unserer Organisation beteiligt sind oder unsere Interessen vertreten. [Die Personal- und Rechtsabteilungen haben in Zusammenarbeit mit den anderen Abteilungen] die Aufgabe, die Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung der hier beschriebenen Verfahren zu beaufsichtigen.

2 Mitarbeiter-Lebenszyklus-Prozesse

2.1 Sicherheits- und Kompetenzüberprüfung im Bewerbungsverfahren

2.1.1 Richtlinie

Die Überprüfung des Hintergrunds aller Bewerber für eine Stelle muss vor dem Eintritt in die Organisation und fortlaufend (je nach Sensibilität der Stelle) unter Berücksichtigung der geltenden Gesetze, Vorschriften und ethischen Grundsätze durchgeführt werden. Dieser Prozess steht in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Klassifizierung der Informationen, auf die zugegriffen werden soll, und den wahrgenommenen Aufgaben.

2.1.2 Verfahren

Unser Überprüfungsverfahren respektiert die Privatsphäre, schützt personenbezogene Daten und hält die arbeitsrechtlichen Vorschriften in Übereinstimmung mit lokalen und internationalen Gesetzen und Vorschriften ein.

I. Verifizierungsprozess:

- **Referenzen:**

  Prüfen Sie, ob angemessene Referenzen vorhanden sind. Dazu können geschäftliche Referenzen von früheren Arbeitgebern oder Kollegen sowie persönliche Referenzen von Nicht-Verwandten gehören, die für den Charakter und die Qualifikationen des Bewerbers bürgen können.

- **Überprüfung des Lebenslaufs:**

  Führen Sie eine umfassende Überprüfung des Lebenslaufs des Bewerbers durch, um dessen Vollständigkeit und Richtigkeit zu überprüfen. Dazu kann die Bestätigung der Beschäftigungsdaten, der ausgeübten Funktionen und der übernommenen Aufgaben gehören.

- **Bestätigung der Qualifizierung:**

  Bestätigen Sie die Echtheit der angegebenen akademischen und beruflichen Qualifikationen. Dies könnte bedeuten, dass Sie sich direkt an Bildungseinrichtungen oder Berufsverbände wenden oder einen externen Prüfdienst in Anspruch nehmen.

- **Identitätsüberprüfung:**

  Überprüfen Sie die Identität des Bewerbers z.B. durch Überprüfung eines Personalausweises, Reisepasses, Führerscheins oder eines anderen geeigneten Dokuments, das von anerkannten Behörden ausgestellt wurde.

- **Bonitätsprüfung und Strafregisterauszug:**

  Bei Positionen mit besonderer Vertrauensstellung, das heißt z.B. bei Umgang mit Konten, Führungsaufgaben und kritischen Werten, kann es notwendig sein, die finanzielle Situation und die kriminelle Vergangenheit des Bewerbers im gesetzlich zulässigen Rahmen zu überprüfen. Dies kann z.B. durch eine Schufa-Auskunft mit Zustimmung der Bewerber erfolgen und durch Vorlage eines Führungszeugnisses.

[Bitte überprüfen Sie, ob dies der richtige Prozess ist, den Sie befolgen; wenn es Änderungen gibt, aktualisieren Sie sie direkt; Sie müssen den Nachweis erbringen, dass dieser Prozess wie angegeben durchgeführt wurde.]

II. Spezifische Maßnahmen für Informationssicherheitsrollen:

Bei der Einstellung für eine bestimmte Rolle im Bereich der Informationssicherheit sind zusätzliche Maßnahmen zu ergreifen, um sicherzustellen:

1. **Kompetenz:** Der Bewerber muss über die erforderlichen Fähigkeiten, Kenntnisse und Erfahrungen verfügen, um die Sicherheitsfunktion wirksam ausüben zu können. Dies kann durch Gespräche, praktische Tests oder Nachweise über frühere Leistungen in ähnlichen Funktionen festgestellt werden.
2. **Vertrauenswürdigkeit:**

   Der Bewerber muss seine Vertrauenswürdigkeit im Umgang mit potenziell sensiblen Informationen oder kritischen Aufgaben nachweisen. Dies kann durch die Überprüfung von Referenzen, Fragen zum Verhalten im Vorstellungsgespräch oder ggf. durch die Durchführung der Sicherheitsüberprüfung beurteilt werden.

[Bitte überprüfen Sie, ob dies der richtige Prozess ist, den Sie befolgen; wenn es Änderungen gibt, aktualisieren Sie sie direkt; Sie müssen den Nachweis erbringen, dass dieser Prozess wie angegeben durchgeführt wurde.]

III. Nachweise

Unsere Nachweise für die Durchführung der Sicherheits- und Kompetenzüberprüfung im Bewerbungsverfahren sind:

[Bitte beschreiben Sie die Art und Weise, wie die Organisation dokumentierte Nachweise für den beschriebenen Screening-Prozess sammeln wird. Beispiel:

- Ausgefüllte Checkliste in der Personalverwaltungssoftware

- Kopien von Zertfizierungen

- Kompetenz-Matrix...]

Diese Nachweise werden im [Speicherort] aufbewahrt.

2.2. Beschäftigung- und Vertragsbedingungen

2.2.1 Richtlinie

Die Richtlinie der Beschäftigungs- und Vertragsbedingungen soll sicherstellen, dass Mitarbeiter und relevante Dritte (Vertragspartner) ihre Verantwortung für die Informationssicherheit verstehen. Dazu gehören Vereinbarungen zu Vertraulichkeit, Geheimhaltung, Urheberrecht, Datenschutz, verantwortungsvoller Umgang mit Daten und einer Verpflichtung zur Einhaltung der Informationssicherheit.

2.2.2 Verfahren

I. Ausarbeitung des Vertrags

Identifizieren Sie die Anforderungen an Ihre Vertragspartner. Setzen Sie einen Vertrag auf, der spezielle Klauseln in Bezug auf die Verantwortlichkeiten im Bereich der Informationssicherheit enthält.

Stellen Sie dabei sicher, dass der Vertrag mindestens Folgendes vorsieht:

1. Die Anforderung an die Vertragspartner, Vertraulichkeits- oder Geheimhaltungsvereinbarungen zu unterzeichnen, bevor sie Zugang zu vertraulichen Informationen erhalten.
2. Gesetzliche Pflichten und Rechte des Personals, wie z. B. die Einhaltung von Urheberrechtsgesetzen oder Datenschutzvorschriften.
3. Personelle Zuständigkeiten für die Klassifizierung und Verwaltung der Informationen der Organisation und der damit verbundenen Vermögenswerte.
4. Maßnahmen, die zu ergreifen sind, wenn die Vertragspartner die Sicherheitsanforderungen der Organisation missachten.

II. Richtlinien einbeziehen

Beziehen Sie die Informationssicherheitsleitlinie der Organisation und alle relevanten themenspezifischen Richtlinien, in einer Verpflichtung auf die Informationssicherheit, durch Auflistung in den Vertrag ein.

III. Zuständigkeiten nach Beendigung der Beschäftigung

Nehmen Sie eine Klausel in den Vertrag auf, die besagt, welche Pflichten, wie z.B. die Verschwiegenheitspflicht, für einen bestimmten Zeitraum nach Beendigung des Arbeitsverhältnisses fortbestehen.

IV. Kommunikation vor Vertragsbeginn

Vermitteln Sie den Vertragspartnern klar die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit. Stellen Sie vor Vertragsabschluss sicher, dass die Bedingungen für die Informationssicherheit und die Konsequenzen ihrer Nichteinhaltung verstanden werden.

V. Vertragsunterzeichnung

Wenn alle Vertragsbedingungen stimmen, lassen Sie den Vertrag von unserem Vertragspartnern und durch Verantwortliche unserer Organisation unterzeichnen.

VI. Überprüfung und Aktualisierung

Überprüfen und aktualisieren Sie regelmäßig die Bedingungen für die Informationssicherheit, insbesondere wenn sich Gesetze, Vorschriften, die Informationssicherheitsrichtlinie oder themenspezifische Richtlinien ändern.

VII. Nachweise

Unterzeichnete Verträge, Entwürfe und dazugehörige Dokumente werden sicher und vertraulich im [Speicherort] aufbewahrt.

2.3 Verantwortlichkeiten nach Beendigung oder Wechsel des Beschäftigungsverhältnisses.

2.3.1 Richtlinie

Die Verwaltung von Informationssicherheitsaufgaben bei Beendigung oder Wechsel des Beschäftigungsverhältnisses ist von entscheidender Bedeutung für den Schutz der Informationswerte der Organisation und die Gewährleistung der Kontinuität von Rollen und Verantwortlichkeiten. Dies umfasst die Identifizierung von Zuständigkeiten, die Fortführung von Zuständigkeiten, die Übertragung von Zuständigkeiten, die Kommunikation von Änderungen, die Entfernung von externem Personal und den IT-Zugang sowie Änderungen.

2.3.2 Verfahren

[Bitte prüfen und bestätigen Sie, dass der folgende Prozess auf Ihren organisatorischen Prozess zutrifft; allerdings sollten alle unten genannten Bereiche eine Prozessbeschreibung erhalten, wenn nicht bereits vorhanden].

I. Identifizierung der Verantwortlichkeiten:

Identifizieren Sie die Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die eine Person innehat, die die Organisation verlässt oder ihre Rolle wechselt. Dies könnte unter anderem die Vertraulichkeit von Informationen, Rechte an geistigem Eigentum und andere Verantwortlichkeiten umfassen, die in einer Vertraulichkeitsvereinbarung festgelegt sind.

II. Definieren Sie gültige Zuständigkeiten:

Legen Sie fest, welche Aufgaben und Pflichten nach Beendigung oder Wechsel des Beschäftigungsverhältnisses bestehen bleiben. Diese müssen in den Beschäftigungsbedingungen der betreffenden Person enthalten sein.

III. Übertragung von Zuständigkeiten:

Sobald sie identifiziert sind, werden diese Rollen und Verantwortlichkeiten auf eine andere Person übertragen. Dies gewährleistet einen kontinuierlichen Schutz der Informationsbestände der Organisation.

IV. Mitteilung von Änderungen:

Einführung eines Verfahrens zur Mitteilung von Änderungen und aktualisierten Betriebsverfahren an das Personal, andere relevante Parteien und Kontaktpersonen (z. B. Kunden und Lieferanten).

V. Anwendung auf externes Personal:

Dasselbe Verfahren ist auf externes Personal (z. B. Lieferanten) anzuwenden, wenn eine Kündigung erfolgt oder ein Arbeitsplatzwechsel innerhalb der Organisation stattfindet.

VI. IT-Zugangsverwaltung:

Im Rahmen dieses Prozesses muss sichergestellt werden, dass Zugangsdaten wie Passwörter und Multi-Faktor-Authentifizierung deaktiviert oder geändert werden und die Person aus allen Systemen oder Datenbanken entfernt wird, auf die sie Zugriff hatte.

VII. Überprüfung und Wartung:

Überprüfen und aktualisieren Sie diese Verfahren regelmäßig, um sicherzustellen, dass sie wirksam bleiben und mit allen Änderungen der geltenden Gesetze, Vorschriften oder Industriestandards übereinstimmen.

2.4.1 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

2.4.1 Richtlinie

Alle Mitarbeiter und interessierten Parteien müssen eine Vertraulichkeits- oder Geheimhaltungsvereinbarung (Non-disclosure-agreement = NDA) unterzeichnen, um sensible Informationen zu schützen. Diese Vereinbarungen müssen festgelegt, dokumentiert und regelmäßig überprüft werden, um den Bedürfnissen der Organisation gerecht zu werden.

[Wenn dieser Prozess nicht durchgeführt wird, wird in der Regel empfohlen, während der Beschäftigung von Personen, die mit geschäftskritischen Informationen umgehen, ein NDA zu erstellen].

2.4.2 Verfahren

[Spezifizieren Sie den in Ihrer Organisation gelebten Prozess und aktualisieren Sie den folgenden entsprechend]

I. Identifizieren Sie die Informationen:

Bestimmen Sie die Art der zu schützenden Informationen. Dazu können Geschäftsgeheimnisse, geistiges Eigentum, Kundendaten, Geschäftsstrategien usw. gehören.

II. Entwerfen Sie die Vereinbarung:

Entwerfen Sie eine Vertraulichkeits- oder Geheimhaltungsvereinbarung (NDA), die die Bedingungen für den Umgang mit diesen vertraulichen Informationen festlegt. In der Vereinbarung müssen alle in den Richtlinien genannten Punkte behandelt werden.

III. Überprüfen Sie die Vereinbarung:

Lassen Sie die Vereinbarung von einem Rechtsbeistand überprüfen, um sicherzustellen, dass sie durchsetzbar ist und allen geltenden Gesetzen und Vorschriften entspricht.

IV. Übermitteln Sie die Vereinbarung:

Geben Sie die NDA an alle relevanten Mitarbeiter und interessierten Parteien weiter. Dazu können Mitarbeiter, Auftragnehmer, Lieferanten, Partner usw. gehören.

V. Unterschreiben Sie die Vereinbarung:

Holen Sie die Unterschriften aller beteiligten Parteien ein. Vergewissern Sie sich, dass sie die Bedingungen der Vereinbarung und die Konsequenzen bei Nichteinhaltung verstehen.

VI. Umsetzung der Vereinbarung:

Umsetzung der in der Vereinbarung vorgesehenen Maßnahmen, z. B. Beschränkung des Zugangs zu vertraulichen Informationen, Überwachung von Aktivitäten usw.

VII. Überwachung der Einhaltung:

Regelmäßige Überwachung der Einhaltung der NDA. Dies könnte durch Audits, Überprüfungen oder andere geeignete Maßnahmen geschehen.

3. Sensibilisierung und Schulung

3.1 Bewusstsein für Informationssicherheit, Ausbildung und Schulung

3.1.1 Richtlinie

Das gesamte Personal innerhalb unserer Organisation und relevante interessierte Parteien müssen ein angemessenes Bewusstsein für die Informationssicherheit sowie entsprechende Schulungen und Trainings erhalten. Regelmäßige Aktualisierungen der Informationssicherheitsrichtlinie der Organisation, themenspezifischer Richtlinien und Verfahren müssen je nach Aufgabenbereich zur Verfügung gestellt werden, unter Berücksichtigung der schützenswerten Informationen der Organisation und der zu deren Schutz implementierten Informationssicherheitskontrollen.

3.1.2 Verfahren

[Ein Großteil dieses Prozesses kann über die DataGuard-Plattform durchgeführt werden; wenn Sie unsere Akademie für diesen Schritt nutzen, aktualisieren Sie die Angaben unten entsprechend.]

I. Einrichtung des Programms:

Entwicklung eines Programms zur Sensibilisierung, Ausbildung und Schulung im Bereich der Informationssicherheit im Einklang mit der Informationssicherheitsleitlinie der Organisation, themenspezifischen Richtlinien und einschlägigen Verfahren.

II. Erstausbildung:

Durchführung von zeitnahen Sensibilisierungs-, Ausbildungs- und Schulungsveranstaltungen für neue Mitarbeiter oder solche, die in neue Positionen mit anderen Anforderungen an die Informationssicherheit versetzt werden.

III. Bewertung:

Bewerten Sie am Ende einer Schulungsmaßnahme das Verständnis des Personals, um den Wissenstransfer und die Wirksamkeit des Programms zu messen.

IV. Entwicklung von Sensibilisierungsprogrammen:

Entwickeln Sie ein Programm zur Sensibilisierung für die Informationssicherheit, um das Personal auf seine Verantwortung für die Informationssicherheit aufmerksam zu machen. Planen Sie dieses Programm unter Berücksichtigung der Rollen der internen und externen Mitarbeiter. Planen Sie regelmäßig Aktivitäten ein, um neue Mitarbeiter und die aus Vorfällen gewonnenen Erkenntnisse zu berücksichtigen.

V. Aktivitäten zur Sensibilisierung:

Durchführung verschiedener Sensibilisierungsmaßnahmen über geeignete physische oder virtuelle Kanäle. Dazu könnten Kampagnen, Broschüren, Poster, Newsletter, Websites, Informationsveranstaltungen, Briefings, E-Learning-Module und E-Mails gehören.

VI. Allgemeine zu berücksichtigende Aspekte:

Stellen Sie sicher, dass das Sensibilisierungsprogramm Folgendes umfasst:

1. Das Engagement des Managements für die Informationssicherheit.
2. Vertrautheit mit den geltenden Vorschriften und Verpflichtungen im Bereich der Informationssicherheit und deren Einhaltung.
3. Persönliche Verantwortlichkeit für Handlungen und Unterlassungen sowie allgemeine Verantwortung für die Sicherung

von Informationen.

4. Grundlegende Verfahren der Informationssicherheit und Basiskontrollen.
5. Kontaktstellen und Ressourcen für zusätzliche Informationen und Beratung zu Fragen der Informationssicherheit.

VII. Bildungs- und Ausbildungsplan:

Identifizierung, Vorbereitung und Durchführung eines geeigneten Schulungsplans für technische Teams, die bestimmte Fähigkeiten und Fachkenntnisse benötigen. Ergreifen Sie bei fehlenden Fähigkeiten Maßnahmen, um diese zu erwerben.

VIII. Methoden zur Durchführung von Schulungen:

Erwägen Sie verschiedene Formen und Mittel zur Durchführung des Aus- und Weiterbildungsprogramms. Dazu könnten Vorträge, Selbststudium, Ausbildung am Arbeitsplatz, Personalrotation, Einstellung von Fachkräften, Beauftragung von Beratern, Ausbildung im Klassenzimmer, Fernunterricht, webbasierte Ausbildung oder Lernen im eigenen Tempo gehören.

[Update hier über DataGuard academy]

IX. Regelmäßige Fortbildung:

Führen Sie in regelmäßigen Abständen Sensibilisierungs-, Ausbildungs- und Schulungsmaßnahmen zur Informationssicherheit durch, um sicherzustellen, dass alle Mitarbeiter auf dem neuesten Stand der Informationssicherheitsstandards, -richtlinien und -verfahren sind.

[Bitte planen Sie in Ihrem ISMS-Aufgabenmanagement die Sensibilisierung für die Sicherheit sowie die Aus- und Weiterbildung mindestens für das kommende Jahr].

X. Überprüfung und Aktualisierung:

Regelmäßige Überprüfung und Aktualisierung des Programms, um es an Änderungen von Gesetzen, Vorschriften, Richtlinien oder der Informationssicherheitslandschaft anzupassen.

[Bitte planen Sie die regelmäßige Überprüfung des Programms in Ihrem ISMS-Aufgabenmanagement ein].

4. Einhaltung der Vorschriften durch die Mitarbeiter

4.1 Maßregelungsprozess

4.1.1 Richtlinie

Verstöße gegen die Informationssicherheitsrichtlinie der Organisation durch Mitarbeiter oder relevante interessierte Parteien werden durch einen formalisierten und kommunizierten Maßregelungsprozess geahndet. Dies gilt für unbeabsichtigte, erstmalige, wiederholte, betrügerische oder bedrohliche Verstöße, unabhängig davon, ob der Täter geschult ist oder nicht.

4.1.2 Verfahren

[Überprüfen Sie, ob der nachstehende Prozess für Sie passt und aktualisieren Sie ihn ggf. entsprechend]

I. Identifizierung des Verstoßes:

Der erste Schritt besteht darin, den Verstoß gegen die Informationssicherheitsrichtlinie festzustellen. Dies kann durch Routineüberwachung, Audits oder Berichte von anderen Mitarbeitern oder Systemen geschehen.

II. Untersuchung und Bestätigung:

Sobald ein möglicher Verstoß festgestellt wird, wird eine Untersuchung eingeleitet, um den Verstoß zu bestätigen. Dies kann die Überprüfung von Systemprotokollen, die Befragung von Beteiligten oder die Untersuchung physischer oder digitaler Beweise beinhalten.

III. Einstufung des Verstoßes:

Nach der Bestätigung wird der Verstoß nach seiner Schwere und der dahinterstehenden Absicht eingestuft. Dies kann von unbeabsichtigten, erstmaligen Verstößen bis hin zu wiederholten, vorsätzlichen Verstößen mit Betrug oder Drohungen reichen.

IV. Einleitung eines Disziplinarverfahrens:

Je nach Einstufung wird der entsprechende Maßregelungsprozess eingeleitet. Orientieren Sie sich an dieser Einstufung:

Stufe 1 - Mündliche Ermahnung: Bei geringfügigen Verstößen erfolgt zunächst ein vertrauliches Gespräch zwischen dem Mitarbeiter und dem Vorgesetzten, um das Fehlverhalten zu besprechen und Lösungsmöglichkeiten zu finden.

Stufe 2 - Formelle Maßnahmen:

- Schriftliche Verwarnung: Bei wiederholtem oder schwerwiegendem Fehlverhalten wird eine schriftliche Verwarnung ausgesprochen. Diese enthält eine Beschreibung des Fehlverhaltens, die erforderlichen Korrekturmaßnahmen und die Konsequenzen bei weiteren Verstößen.
- Abmahnung: Eine oder mehrere schriftliche Abmahnungen erfolgen bei fortgesetztem Fehlverhalten. Eine Abmahnung dokumentiert das Fehlverhalten, gibt konkrete Anweisungen zur Verhaltensänderung und weist auf mögliche weitere disziplinarische Schritte hin.
- Letzte Abmahnung: Vor einer möglichen Kündigung wird eine letzte Abmahnung ausgesprochen, die dem Mitarbeiter eine letzte Chance zur Verhaltensänderung gibt.

Stufe 3 - Disziplinarische Anhörungen:

- Vorladung zur Anhörung: Vor der Umsetzung schwerwiegender Maßnahmen, wie einer letzten Abmahnung oder Kündigung, wird der Mitarbeiter zu einer formellen Anhörung geladen. Der Mitarbeiter hat das Recht, eine Vertrauensperson hinzuzuziehen.
- Durchführung der Anhörung: In der Anhörung werden die Vorwürfe erläutert und der Mitarbeiter erhält die Möglichkeit, seine Sichtweise darzulegen. Die Anhörung wird protokolliert.

Stufe 4 -Kündigung:

- Ordentliche Kündigung: Bei fortgesetztem Fehlverhalten trotz vorheriger Maßnahmen kann eine ordentliche Kündigung ausgesprochen werden. Die Kündigungsfrist wird eingehalten.
- Außerordentliche Kündigung: Bei schwerwiegenden Verstößen, die eine weitere Zusammenarbeit unzumutbar machen, kann eine außerordentliche Kündigung ohne Einhaltung der Kündigungsfrist erfolgen.

Sonderfälle:

- Mobbing und Diskriminierung: Bei Vorwürfen von Mobbing, Diskriminierung oder Belästigung wird eine sofortige Untersuchung eingeleitet. Betroffene Mitarbeiter werden bis zur Klärung des Sachverhalts geschützt.
- Verstöße gegen Sicherheitsvorschriften: Bei Verstößen gegen Sicherheitsvorschriften, die die Gesundheit oder Sicherheit gefährden, erfolgen sofortige Maßnahmen, einschließlich möglicher Freistellung des Mitarbeiters.

[Das Thema "Disziplinarische Maßnahme" ist ebenfalls Bestandteil des Mitarbeiterhandbuchs. Sofern Sie die zuvor dargestellten Stufen disziplinarischer Maßnahmen an Ihre individuellen Bedürfnisse angepasst haben, bitten wir Sie diese Anpassungen in diesem Dokument und im Mitarbeiterhandbuch synchron zu halten].

V. Dokumentation:

Alle Schritte des Maßregelungsprozesses sind sorgfältig zu dokumentieren. Dazu gehören die Art des Verstoßes, die Ergebnisse der Untersuchung, die Einstufung des Verstoßes und die ergriffenen Disziplinarmaßnahmen.

[Bitte beschreiben Sie die Art und Weise, wie die Organisation dokumentierte Nachweise für den durchgeführten Maßregelungsprozess sammeln wird. Beispiel: Ausgefüllte Berichtsvorlage ...]

VI. Kommunikation:

Die Ergebnisse des Maßregelungsprozesses sind dem Zuwiderhandelnden, seinem Vorgesetzten und allen anderen Beteiligten mitzuteilen. Diese Mitteilung muss klar, prägnant und respektvoll sein und gleichzeitig sicherstellen, dass der Zuwiderhandelnde die Schwere seines Handelns und die Konsequenzen versteht.

VII. Nachbereitung:

Nach dem Maßregelungsprozesses sind Folgemaßnahmen zu ergreifen, um künftige Verstöße zu verhindern. Dazu könnten zusätzliche Schulungen, Änderungen der Strategien oder Verfahren oder Verbesserungen der Sicherheitssysteme und -kontrollen gehören.

VIII. Rückblick:

Überprüfen und aktualisieren Sie den Maßregelungsprozess regelmäßig, um sicherzustellen, dass es wirksam bleibt und allen Änderungen von Gesetzen, Vorschriften oder Branchenstandards entspricht.

5. Arbeiten außerhalb der Geschäftsräume

5.1 Arbeiten außerhalb der Geschäftsräume

5.1.1 Richtlinie

Mitarbeiter, die an anderen Orten arbeiten, müssen geeignete Sicherheitsmaßnahmen ergreifen, um Informationen zu schützen, auf die sie außerhalb der Räumlichkeiten der Organisation zugreifen, sie verarbeiten oder speichern.

5.1.2 Verfahren

[Prüfen Sie, dass alle nachstehenden Punkte für Ihre Organisation zutreffend sind. Die folgenden Punkte dienen als Orientierung.]

I. Bewertung von Arbeiten außerhalb der Geschäftsräume:

Durchführung einer Bewertung der physischen Sicherheit von Remote-Arbeitsplätzen unter Berücksichtigung des Standorts, des lokalen Umfelds und der verschiedenen gesetzlichen Anforderungen, die auf das Personal anzuwenden ist.

II. Regeln für eine Remote Umgebung aufstellen:

Entwickeln Sie Regeln für physische Remote-Umgebungen, um die sichere Datenübertragung zwischen den Standorten, eine klare Arbeitsplatzrichtlinie, die sichere Entsorgung von Informationen und die Meldung von Ereignissen zu gewährleisten.

[DataGuard sieht vor, dass die Regeln Teil der Richtlinien im Mitarbeiterhandbuch sind.]

III. Sicherheitsmaßnahmen für die Kommunikation:

Implementieren Sie Kommunikationssicherheitsmaßnahmen wie sichere VPNs, verschlüsselte E-Mails und sichere Datenübertragungsprotokolle.

IV. Schutz vor Bedrohungen durch unbefugten Zugriff:

Verwenden Sie strenge Passwortrichtlinien, Zwei-Faktor-Authentifizierung und automatische Sperrung nach Zeiten der Inaktivität, um unbefugten Zugriff zu verhindern.

V. Richtlinien für die Netznutzung:

Festlegung von Richtlinien für die Nutzung privater und öffentlicher Netzwerke, einschließlich der Konfiguration drahtloser Netzwerkdienste. Z.B. sind alle Außendienstmitarbeiter anzuweisen, sichere Netzwerke zu nutzen und öffentliches WLAN für arbeitsbezogene Aufgaben zu vermeiden. Weisen Sie die Benutzer auf Risiken in öffentlichen WLAN-Netzwerken hin. [Sie können nicht vorschreiben, dass die Mitarbeiter die Konfiguration des Heimnetzwerks befolgen, es liegt also in Ihrem Ermessen, ob Sie dies hinzufügen möchten.]

VI. Implementierung von Sicherheitssoftware:

Installieren Sie Firewalls, Antivirensoftware und anderen Schutz vor Malware auf allen mobilen Geräten, die für die Arbeiten außerhalb der Geschäftsräume verwendet werden.

VII. Authentifizierungsmechanismen:

Einrichtung sicherer Mechanismen für die Authentifizierung und Freigabe von Zugriffsrechten, insbesondere beim Fernzugriff auf das Netz der Organisation.

VIII. Sorgen Sie für eine geeignete Ausrüstung und Schulung:

Stellen Sie für Arbeiten außerhalb der Geschäftsräume geeignete Ausrüstung zur Verfügung, legen Sie die zulässigen Arbeiten klar fest und bieten Sie Schulungen zur sicheren Arbeit außerhalb der Geschäftsräume an.

IX. Legen Sie Regeln für den Zugang von Familienangehörigen und Besuchern fest:

Legen Sie Regeln fest, wer auf die für die Arbeiten außerhalb der Geschäftsräume verwendeten Geräte und Informationen zugreifen darf.

X. Hardware- und Software-Unterstützung:

Stellen Sie technischen Support für Remote-Mitarbeiter zur Verfügung, um sicherzustellen, dass ihre Hardware und

Software korrekt und sicher funktioniert.

XI. Sicherungs- und Geschäftskontinuitätsverfahren:

Stellen Sie sicher, dass Verfahren für die Datensicherung und die Aufrechterhaltung des Geschäftsbetriebs auch für Geräte außerhalb der Geschäftsräume verfügbar sind.

XII. Audit und Sicherheitsüberwachung:

Führen Sie eine regelmäßige Überwachung und Prüfung von Arbeiten außerhalb der Geschäftsräume durch, um die Einhaltung der Sicherheitsmaßnahmen zu gewährleisten.

XIII. Entzug der Befugnis und Rückgabe der Ausrüstung:

Nach Beendigung der Arbeiten außerhalb der Geschäftsräume sind spezielle – für diesen Zweck genutzte Zugangsrechte zu entziehen und alle entsprechenden Geräte zurückzuholen.

6. Schutz personenbezogener Daten

6.1 Privatsphäre und Schutz von personenbezogenen Daten (PII)

6.1.1 Richtlinie

Zu den persönlich identifizierbaren Informationen (PII) gehören unter anderem Daten wie Namen, Adressen, E-Mail-Adressen, Telefonnummern, Sozialversicherungsnummern, Führerscheinnummern, Reisepassnummern und Finanzkontodaten.

Wir erheben und verarbeiten PII nur für festgelegte und rechtmäßige Zwecke. PII müssen als solche eingestuft werden und es müssen entsprechende Sicherheitskontrollen zu ihrem Schutz vorgesehen werden, einschließlich Verschlüsselung im Ruhezustand und bei der Übertragung, sichere Datensicherung, strenge Zugangskontrollen auf der Grundlage des Grundsatzes "Kenntnis nur, wenn nötig". Regelmäßige Bewertungen müssen durchgeführt werden, um potenzielle Risiken zu ermitteln.

6.1.2 Verfahren

I. Identifizierung von PII:

[Definieren Sie, was in Ihrem Unternehmen als PII gilt, einschließlich spezifischer Datenelemente. Das Datenschutz-Team von DataGuard oder ihr Datenschutzbeauftragter helfen Ihnen bei Bedarf bei der exakten Bearbeitung dieser Richtlinien]

II. Einschränkung der Datenerhebung und des Zwecks:

Dokumentieren Sie, dass die Erhebung von PII auf das beschränkt ist, was für die angegebenen Zwecke im Rahmen des Projekts und/oder der Systemnutzung erforderlich ist.

III. Zustimmung und Mitteilung:

- Festlegung von Verfahren zur Einholung der Zustimmung von Einzelpersonen vor der Erhebung ihrer personenbezogenen Daten.
- Klare und transparente Mitteilungen an Einzelpersonen über die Erhebung und Verwendung ihrer personenbezogenen Daten.

IV. Maßnahmen zur Datensicherheit:

- Umsetzung von Sicherheitsmaßnahmen zum Schutz von PII vor unbefugtem Zugriff, Offenlegung, Änderung und Zerstörung.
- Verwenden Sie Verschlüsselung, Zugangskontrollen und regelmäßige Sicherheitsbewertungen, um personenbezogene Daten zu schützen.

V. Aufbewahrung und Vernichtung von Daten:

- Definieren Sie Aufbewahrungsfristen für verschiedene Arten von personenbezogenen Daten auf der Grundlage rechtlicher Anforderungen und geschäftlicher Bedürfnisse.
- Festlegung von Verfahren für die sichere Entsorgung von PII am Ende der Aufbewahrungsfrist.

VI. Gemeinsame Nutzung und Übermittlung von Daten:

- Implementierung von Protokollen für den sicheren Austausch von personenbezogenen Daten mit autorisierten Dritten.
- Sicherstellen, dass alle internationalen Übertragungen von personenbezogenen Daten den einschlägigen Datenschutzbestimmungen und Nutzervereinbarungen entsprechen.

VII. Individuelle Rechte und Anträge:

- Festlegung von Verfahren, mit denen Einzelpersonen ihre Rechte in Bezug auf ihre PII ausüben können, z. B. Zugang, Berichtigung und Löschung.
- Einrichtung von Mechanismen für die Bearbeitung und Beantwortung von Anfragen von Einzelpersonen zu personenbezogenen Daten.

VIII. Schulung und Sensibilisierung:

- Regelmäßige Schulung der Mitarbeiter über bewährte Datenschutzpraktiken und die Verfahren der Organisation zum Schutz personenbezogener Daten.
- Förderung einer Kultur des Datenschutzbewusstseins und der Verantwortlichkeit in der gesamten Organisation.

IX. Überwachung und Überprüfung der Einhaltung der Vorschriften:

- Überprüfen und aktualisieren Sie das Verfahren regelmäßig, um sicherzustellen, dass es mit den sich entwickelnden Datenschutzgesetzen und -vorschriften übereinstimmt.
- Durchführung interner Audits und Bewertungen zur Überwachung der Einhaltung des Verfahrens.

X. Reaktion auf Vorfälle und Berichterstattung:

Erstellung von Protokollen für die Reaktion auf Verletzungen oder Vorfälle von personenbezogenen Daten und deren Meldung an die zuständigen Behörden und die betroffenen Personen.

XI. Dokumentation und Aufbewahrung von Aufzeichnungen:

Führen Sie eine Dokumentation der PII-Verarbeitungstätigkeiten, einschließlich Aufzeichnungen über die Zustimmung, Datenübertragungen, Sicherheitsmaßnahmen und Reaktionen auf Vorfälle.

XII. Rechenschaftspflicht und Durchsetzung:

- Festlegung von Maßnahmen zur Gewährleistung der Einhaltung des Verfahrens und zur Behandlung von Verstößen.
- Die Folgen eines Verstoßes gegen das Verfahren zum Schutz personenbezogener Daten müssen klar dargelegt werden.

7. Norm-Referenzen

7.1 Norm-Referenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. Einleitung	
2. Mitarbeiter-Lebenszyklus-Prozesse	A 6.1; A6.5; A 6.2; A 6.6
3. Sensibilisierung und Schulung	Klausel 7.3; A 6.3
4. Einhaltung der Vorschriften durch die Mitarbeiter	A 6.4
5. Arbeiten außerhalb der Geschäftsräume	A 6.7

6. Schutz personenbezogener Daten	A 5.34

7.2 Norm-Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	Normkapitel (TISAX-ISA 6.0)
1. Einleitung	
2. Mitarbeiter-Lebenszyklus-Prozesse	2.1.1; 2.1.2
3. Sensibilisierung und Schulung	2.1.3; 3.1.1; 5.2.3
4. Einhaltung der Vorschriften durch die Mitarbeiter	1.1.1; 2.1.2
5. Arbeiten außerhalb der Geschäftsräume	2.1.4; 3.1.4
6. Schutz personenbezogener Daten	3.1.4; 7.1.2