[Name der Organisation]

ST8 Handbuch zur Steuerung von Gefahrenbewusstsein und Sicherheitsvorfällen

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

Change History

Datum	**Version**	**Erstellt von**	**Beschreibung der Änderung**
26.09.24	0.91	DataGuard	Grundstruktur des Dokuments
XX.XX.24	1.00	XX	Geprüfte Version mit geringen 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 Einführung

Dieses Handbuch mit Richtlinien zu den Themen Gefahrenbewusstsein (Threat Intelligence) und Vorfallsteuerung (Incident Response Management) für [Name der Organisation] stellt einen Rahmen dar, der unsere Strategie zur effektiven Verwaltung und Eindämmung von Sicherheitsbedrohungen und -vorfällen beschreibt. Dieses Dokument dient als umfassender Leitfaden, in dem detailliert beschrieben wird, wie unsere Organisation verschiedene Sicherheitsherausforderungen angeht und auf Vorfälle in unserem gesamten Betrieb reagiert. Darüber hinaus dient es als übergeordnetes Dokument, das den Ansatz vonGefahrenbewusstsein und Vorfallsteuerung umreißt.

1.1 Zweck und Umfang

Zweck dieser Richtlinie ist es, einen strukturierten Ansatz für die Sammlung von Bedrohungsdaten, die Analyse und das Management von Vorfällen zu entwickeln, um die sensiblen Informationen, die Infrastruktur und die Reputation der Organisation zu schützen. Durch die Einhaltung dieser Richtlinie wollen wir unsere Widerstandsfähigkeit gegenüber sich entwickelnden Cyber-Bedrohungen erhöhen und die Auswirkungen von Sicherheitsvorfällen auf unsere Geschäftsabläufe minimieren.

1.2 Anwendbarkeit

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Drittdienstleister und Interessengruppen, die Zugang zu den Informationsbeständen unserer Organisation haben oder an der Bewältigung von Sicherheitsvorfällen beteiligt sind. Sie umfasst alle Systeme, Netzwerke und Daten, die in den Zuständigkeitsbereich von der Organisation fallen, unabhängig von deren Standort oder Form.

2. Kontakt mit relevanten Parteien und Bedrohungsintelligenz

2.1 Kontakt mit Behörden

2.1.1 Richtlinie

Der Kontakt zu den zuständigen Behörden muss entsprechend den gesetzlichen und regulativen Bestimmungen hergestellt und aufrechterhalten werden.

Die Meldung von Vorfällen im Bereich der Informationssicherheit an Aufsichtsbehörden und Strafverfolgungsbehörden muss bei Bedarf eingerichtet bzw. durchgeführt werden.

2.1.2 Verfahren

Die Organisation führt ein Verzeichnis der lokalen und regionalen Strafverfolgungsbehörden und anderer relevanter Aufsichtsbehörden.
Referenz: [Fügen Sie bitte den Titel und den Ablageort des genannten Verzeichnisses ein].

In der Europäischen Union sind Unternehmen aufgrund von Gesetzen und Vorschriften dazu verpflichtet, bestimmte Sicherheitsvorfälle zu melden.

[Bitte legen Sie fest, wer in Ihrer Organisation befugt ist, Sicherheitsvorfälle intern und extern zu kommunizieren und wie die Kommunikation zu erfolgen hat.

Beispiel:

Vorfälle sind vom Leiter der Sicherheitsabteilung unter Verwendung des Melde-Dokuments [Dokument-Name] an den Leiter der Abteilung Recht und Compliance zu melden. Nur der Leiter der Abteilung Recht und Compliance ist befugt, die Vorfälle extern zu melden.]

2.2 Kontakt mit speziellen Interessengruppen

2.2.1 Richtlinie

Regelmäßig müssen Kontakte zu speziellen Interessengruppen oder anderen spezialisierten Sicherheitsforen geknüpft werden. Diese Gruppen tragen dazu bei, dass die Organisation über die neuesten bewährten Verfahren, Bedrohungen, Schwachstellen und Technologien im Bereich der Informationssicherheit informiert ist.

2.2.2 Verfahren

Die Organisation führt ein Verzeichnis der relevanten speziellen Interessengruppen.
Referenz: [Fügen Sie bitte den Titel und den Ablageort des genannten Verzeichnisses ein]

[Beschreiben Sie hier unter anderem die Quellen für Bedrohungsdaten – siehe auch Ihre speziellen Interessengruppen, einschließlich kommerzieller Bedrohungsdaten, Open-Source-Bedrohungsdaten, Branchengruppen oder interner Quellen wie Protokolle und Vorfallsberichte. Zum Beispiel: ENISA, BSI, das InfraGard-Programm des FBI oder die Cybersecurity & Infrastructure Security Agency (CISA), CrowdStrike, Recorded Future, FireEye, X (Twitter), usw.]

Die Teilnahme an Gruppen, Foren und Seminaren muss dokumentiert und jährlich überprüft werden.

Die Pläne für die Teilnahme müssen dem Informationssicherheitsbeauftragten (ISB) zur Verfügung gestellt werden und können in die Jahrespläne der Mitarbeiter aufgenommen werden.

2.3 Bedrohungsintelligenz

2.3.1 Richtlinie

Die Sammlung und Analyse von Informationen über potenzielle oder bestehende Bedrohungen, die einer Organisation schaden könnten, muss dazu dienen, auf Bedrohungen der Cybersicherheit vorbereitet zu sein, zu erkennen und zu verhindern.

2.3.2 Verfahren

Ziele der Bedrohungsintelligenz:

Mit der Stärkung von Bedrohungsintelligenz verfolgt unsere Organisation folgende Ziele:

Früherkennung von Bedrohungen: Durch das Sammeln von Daten über potenzielle Bedrohungen kann die Organisation frühzeitig Warnzeichen erkennen und proaktiv Maßnahmen ergreifen, um Sicherheitsvorfälle zu verhindern oder zu mildern.

Risikobewertung: Die Analyse von Bedrohungsdaten ermöglicht es unserer Organisation, ihre spezifischen Risiken zu bewerten und zu verstehen, welche Bedrohungen am wahrscheinlichsten sind und welche potenzielle Auswirkungen sie haben könnten.

Identifikation von Sicherheitslücken aus internen und externen Informationsquellen: Durch das Sammeln von Bedrohungsdaten können Sicherheitslücken in Systemen, Anwendungen oder Netzwerken identifiziert werden, die von Angreifern ausgenutzt werden könnten. Dies ermöglicht es der Organisation, diese Schwachstellen zu beheben, bevor sie ausgenutzt werden.

[Ergänzen Sie ggf. was individuell noch mit der Verarbeitung von Bedrohungsdaten in Ihrer Organisation erreicht werden soll].

Sammeln und analysieren von Bedrohungsdaten:

Die Organisation sammelt und analysiert aus internen und externen Quellen Bedrohungsdaten. Als externe Quelle dient der Kontakt zu Behörden und speziellen Interessengruppen (siehe Verzeichnis) dienen. Die Sammlung interner Bedrohungsdaten erfolgt unter anderem durch die Verwendung von SIEM-Systemen (Security Information and Event Management), TIPs (Threat Intelligence Platforms) oder anderen Analysetools. Es ist die Aufgabe der Administratoren dieser Systeme, den ISB über relevante Erkenntnisse zu informieren [Bitte umschreiben, wenn nicht zutreffend].

Integration von Bedrohungsdaten in die Sicherheitsabläufe:

Die Aufgabe des ISB besteht darin, gesammelte Daten ggf. mit Hilfe von Experten zu analysieren, um potenzielle Bedrohungen und Schwachstellen zu ermitteln. Es sollen zudem die aus der Analyse gewonnenen Erkenntnisse genutzt werden, um die Sicherheitsmaßnahmen zu verbessern.

Effektive Kommunikation:

Relevante Stakeholder müssen die risikorelevanten Bedrohungsdaten verstehen und wissen, wie sich die Bedrohungen sich auf sie auswirken.

Evaluation und Anpassung:

Unsere Organisation überprüft regelmäßig die Maßnahmen zur Verarbeitung von Bedrohungsdaten, um ihre Wirksamkeit zu gewährleisten. Dazu gehören die Messung der wichtigsten Leistungsindikatoren (Key Performance Indicators, KPIs), die Einholung von Feedback von Beteiligten und die Durchführung regelmäßiger Audits.

3. Management von Informationssicherheitsvorfällen

3.1 Grundsätze bzw. Planung des Managements von Informationssicherheitsvorfällen

Diese Richtlinie beschreibt Grundsätze und Verfahren, wie unsere Organisation Informationssicherheitsvorfälle identifizieren und bewerten soll, um die Entscheidungsfindung beschleunigen und eine rasche Reaktion auf der Grundlage zuverlässiger Informationen ermöglichen zu können.

3.1.1 Richtlinie

Die folgenden Grundsätze tragen dazu bei, dass die Verwaltung und Bewältigung von Informationssicherheitsereignissen effektiv und effizient durchgeführt wird, um die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen in einer Organisation zu schützen. Sie müssen von den handelnden Personen in der Organisation umgesetzt werden:

- Prozesse zur automatischen oder persönlichen Meldung von auffälligen Ereignissen sind definiert bzw. bekanntgemacht worden
- Alle Mitarbeiter werden in die Verantwortung gezogen, vermutete oder bestätigte Sicherheitsvorfälle unverzüglich an die zuständige Stelle zu melden, damit diese ohne Verzögerung eskalieren und reagieren kann.
- Rollen und Verantwortlichkeiten bei der Behandlung von Vorfällen sind geklärt
- Erforderliche Ressourcen für das Notfallmanagement sind definiert und verfügbar
- Verfahren zur Klassifizierung von Ereignissen und Vorfällen sind definiert
- Es muss ein umfassender Plan für die Reaktion auf einen Vorfall vorliegen, in dem die im Falle eines Sicherheitsverstoßes zu ergreifenden Maßnahmen, einschließlich Eindämmung, Beseitigung, Wiederherstellung und Analyse nach dem Vorfall, im Einzelnen aufgeführt sind.
- Entscheidungsprozesse für die Reaktion auf Vorfälle sind beschrieben
- Kommunikation zu internen und externen interessierten Parteien wurde bestimmt
- Die erforderliche Dokumentation zur Sicherstellung der Nachweisbarkeit wurde festgelegt
- Verfahren zur Nachbehandlung von Informationssicherheitsvorfällen wurden festgelegt.
- Mitarbeiter müssen Regelungen zur Meldung von Informationssicherheitsereignissen erhalten.[Die Regeln für Mitarbeiter sind Bestandteil des Mitarbeiter-Sicherheitshandbuchs]
- Regelmäßige Schulungen und Sensibilisierungsprogramme müssen durchgeführt werden, um die Mitarbeiter darin zu schulen, wie sie potenzielle Sicherheitsvorfälle erkennen und darauf reagieren können.

3.1.2 Verfahren

Informationssicherheitsereignisse und -vorfälle

Die Organisation definiert Informationssicherheitsereignisse als alle beobachteten Abweichungen vom normalen Betrieb eines Informationssystems. Es handelt sich um potenziell sicherheitsrelevante Vorfälle, die genauer überwacht und analysiert werden müssen.

Beispiele für Informationssicherheitsereignisse sind:

- Anomalien bei Benutzeranmeldungen

- Malware-Erkennung
- Phishing-Versuche
- Unautorisierte Zugriffsversuche
- Datendiebstahl
- Systemfehler und -abstürze
- Abnormale Dateizugriffe
- Unerlaubter Zutritt zu Schutzzonen
- Extremwetterlagen
- Naturkatastrophen

Im Gegensatz dazu sind Informationssicherheitsvorfälle konkrete Ereignisse, bei denen die Sicherheitsrichtlinien einer Organisation verletzt wurden. Sie erfordern eine eingehende Untersuchung und eine gezielte Reaktion, um mögliche Schäden zu begrenzen und Sicherheitslücken zu schließen.

Rollen und Verantwortlichkeiten bei Informationssicherheitsvorfällen

Die Organisation benennt im Verzeichnis der ISMS-Rollen (siehe ISMS-Handbuch) und Verantwortlichkeiten Mitglieder des Vorfallmanagement-(Inciden Respond Management (IRM)-)Teams und zu dessen Führung einen Vorfallmanager.

Im IRM-Team sollen die folgenden Rollen aus der Organisation vertreten sein. Die spezifische Zusammensetzung des Teams kann jedoch je nach Art des Vorfalls variieren.

- [Bitte Liste an Ihre Organisation anpassen und in die Dokumentation der Rollen und Verantwortlichkeiten Ihres ISMS (ISMS-Handbuch) integrieren. Beispiele sind:
  - Mitglied der obersten Leitung
  - IRM-Manager (oder Stellvertreter)
  - SpezialistIn für IT-Sicherheit
  - Beauftragter für Öffentlichkeitsarbeit/Kommunikation
  - ExpertIn für Geschäftsprozesse/Operationen
  - SpezialistIn für IT-Infrastruktur
  - VertreterIn der Personalabteilung
  - RechtsberaterIn und Datenschutzbeauftragter
  - Zusätzliche Fachleute oder einschlägiges Fachpersonal nach Bedarf]

Erkennung und Meldung von Ereignissen und Vorfällen

Die Organisation kombiniert eine automatische Systemmeldung und die manuelle Meldung von Personen innerhalb und außerhalb der Organisation zur Erkennung von beachtenswerten Ereignissen.

Zur automatischen Erkennung und Verarbeitung von Ereignissen werden folgende Instrumente verwendet:

[Bitte listen Sie hier bestehende automatische Systeme und Datenbanken zur Erkennung von Angriffen oder Ereignissen, zum Beispiel SIEM (Security Information and Event Management Systeme), IDS (Intrusion Detection Systeme), AWS CloudWatch, MDM (Mobile Device Management) Systeme, Service Monitoring Systeme (Netz-, Dienst- und Hostsensoren) und andere Vulnerability Scanner oder physische Überwachungssensoren (z.B. Alarmmeldeanlagen) auf und beschreiben Sie grob die Servicetiefe der Systeme.]

In dem Bewusstsein, dass aus einer größeren Anzahl von Meldequellen ein immer schärferes Bild von möglichen Gefahren aus Ereignissen erkannt werden kann, strebt unsere Organisation eine Ausweitung und Vernetzung von Ereignisinformationen an, um eine kontinuierliche Verbesserung der Erkennung und Meldung von Ereignissen zu erreichen.

Für die manuelle Meldung von Ereignissen bestehen folgende Kanäle:

[Bitte listen Sie hier bestehende Meldekanäle für Informationssicherheitsereignisse in Ihrer Organisation auf. Dies können sein: Allgemein genutztes Ticketsystem, spezifische E-Mail-Adresse, Telefonnummer, Teams-/Slack-/WhatsApp-/ oder sonstiger Kanal mit entsprechendem Empfängerkreis. Grundsätzlich gilt: Je leichter und intuitiver die Meldung abgegeben

werden kann, desto wahrscheinlicher wird eine Meldung abgegeben. Sofern aktuell noch keine Kanäle für Informationssicherheitsmeldungen eingerichtet sind, sollte das jetzt erfolgen.]

Alle Mitarbeiter müssen zur Mithilfe bei der Meldung von Ereignissen und Vorfällen verpflichtet werden. Um eine unmittelbare und hilfreiche manuelle Meldung von Ereignissen zu erhalten, wird das Thema zum einen in die Richtlinien im Mitarbeiter-Sicherheitshandbuch integriert, zum anderen zu einem Bestandteil des ISMS Schulungs- und Trainingsplans. Zweifel von Personen darüber, ob ein Vorfall im Bereich der Informationssicherheit gemeldet werden sollte oder nicht, müssen über Schulungen und Trainings identifiziert und Klarheit geschaffen werden.

3.2 Bewertung und Entscheidung über Ereignisse im Bereich der Informationssicherheit

3.2.1 Richtlinie

Um Vorfälle im Bereich der Informationssicherheit beurteilen und entscheiden zu können, muss das Incident Management Team über die erforderliche Kompetenz verfügen, um auf Vorfälle reagieren zu können. Durch regelmäßige Schulungen und Übungen muss sichergestellt werden, dass das Team auf den Umgang mit realen Vorfällen vorbereitet ist, wenn diese eintreten.

Zur Bewältigung von Vorfällen im Bereich der Informationssicherheit sind die folgenden Schritte erforderlich, um eine schnelle, wirksame, einheitliche und ordnungsgemäße Reaktion zu gewährleisten

1. Kategorisierung und Prioritätensetzung:

Erstellung eines Schemas zur Kategorisierung und Priorisierung von Informationssicherheitsvorfällen auf der Grundlage ihrer Folgen und ihrer Priorität.

2. Bewertung:

Die benannte Kontaktstelle bewertet jedes Informationssicherheitsereignis anhand des vereinbarten Schemas.

3. Entscheidungsfindung:

Das für die Koordinierung von und Reaktion auf Informationssicherheitsvorfälle zuständige Personal trifft Entscheidungen über Informationssicherheitsvorfälle.

4. Führung von Aufzeichnungen:

Die Ergebnisse der Bewertung und der Entscheidung werden zur späteren Bezugnahme und Überprüfung detailliert aufgezeichnet.

3.2.2 Verfahren

Die Beurteilung, ob es ich bei einem Ereignis um eine reguläre Aktivität oder um ein außergewöhnliches Ereignis handelt, beruht auf einer Vielzahl von Aspekten, die individuell zu betrachten und abzuwägen sind. In der Organisation im Einsatz befindliche automatische Meldesysteme müssen vom IRM-Manager entsprechend den technischen Vorgaben und Konventionen so konfiguriert bzw. so verantwortet werden, dass die gemeldeten Ereignisse der Verwaltung der Informationssicherheit dienen und ggf. automatische Maßnahmen zur Eindämmung einer Störung ergreifen kann. Bei fragwürdigen Ereignissen müssen die Systeme so konfiguriert sein, dass die verantwortliche Person für das IRM unmittelbar in Kenntnis von dem Ereignis gesetzt wird.

Der IRM-Manager hat die Ereignisse nach folgendem Klassifizierungsschema zu bewerten:

- **Informative Ereignisse:** Es sind keine Maßnahmen erforderlich
- **Warnende Ereignisse:** Es muss möglicherweise bald oder jetzt gehandelt werden, um eine Ausnahme zu verhindern
- **Ausnahme Ereignisse:** Es muss etwas unternommen werden, um eine Situation zu beheben, die nicht der Norm entspricht

Informative Ereignisse:
Informationsereignisse werden automatisch geschlossen (auch wenn dies keine explizite Aktion erfordert) und für einen Zeitraum aufbewahrt, der der Richtlinie zur Aufbewahrung von Unterlagen entspricht. Auch wenn sie nicht weitergeleitet werden, können Informationsereignisse für betriebliche Zwecke erforderlich sein, um einen Prüfpfad für spätere Untersuchungen zu erstellen.

Warnende Ereignisse:
Ereignisse, die als Warnungen eingestuft werden, werden einer zusätzlichen Überprüfung unterzogen. Wenn festgestellt

wird, dass zu diesem Zeitpunkt keine weiteren Maßnahmen erforderlich sind, wird das Ereignis geschlossen. Bei Ereignissen, die eine Aktion erfordern, entscheidet Der IRM-Lead oder in Vertretung ein Mitglied des ISMS-Teams mit Hilfe der in der Ereignismeldung enthaltenen Informationen und ggf. nach Rücksprache mit Experten über die geeignete Vorgehensweise. Dieser Eskalationsprozess soll so erfolgen, dass rechtzeitige Reaktionen und eine effektive Handhabung potenzieller Sicherheitsvorfälle gewährleistet wird.

Außergewöhnliche Ereignisse:
Bei Ereignissen, die als Ausnahmen betrachtet werden, hat eine Folgenabschätzung zu erfolgen und wird ein Vorfall ausgelöst, der dann über das Verfahren zur Verwaltung von Vorfällen im Bereich der Informationssicherheit mit entsprechender Diagnose, Untersuchung und Eskalation behandelt wird.

Zu den wichtigsten Überlegungen bei der Entscheidung, ob ein Ereignis einen Vorfall darstellt, gehören Situationen mit folgendem Charakter:

- Es gibt Beweise für vorsätzliche menschliche Interaktion zu böswilligen Zwecken
- Es handelt sich um Informationen mit hohem Geheimhaltungsgrad
- Die Umstände sind auf irgendeine Weise ungewöhnlich
- Es liegt ein klarer Verstoß gegen die Richtlinien zur Informationssicherheit vor
- Es ist offensichtlich, dass sich die Situation verschlimmern kann, wenn nicht gehandelt wird
- Die tatsächlichen oder potenziellen Auswirkungen auf die Organisation sind erheblich
- Es gibt Hinweise darauf, dass eine Maßnahme nicht effektiv funktioniert
- Es wird eine Reihe von Verhaltensweisen angezeigt, die als bösartig bekannt sind
- Es gibt noch einen anderen Grund, verdächtig zu sein

Die Verantwortung für die Bewertung von Ereignissen und Einstufung als Vorfall überträgt [Name der Organisation] auf das IRM-Team unter Führung des IRM-Managers. Als Vertretung für den IRM-Manager bei Nicht-Erreichung wird ein anderes Mitglied des IRM-Teams benannt. Die verantwortliche Person muss seine Entscheidung auf Basis einer Folgenabschätzung vornehmen, um eine angemessene Reaktion zu bestimmen und eine entsprechende Priorisierung bei mehreren gleichzeitigen Vorfällen vornehmen zu können.

Die Folgenabschätzung soll auf folgenden Einschätzungen basieren:

- Die Auswirkungen auf die IT-Infrastruktur, einschließlich Computern, Netzwerken, Geräten und Einrichtungen.
- Die gefährdeten oder kompromittierten Informationswerte und -trägerbestände.
- Die voraussichtliche Dauer des Vorfalls, einschließlich der geschätzten Anfangszeit.
- Die betroffenen Geschäftsbereiche und das Ausmaß ihrer Auswirkungen.
- Vorläufiger Hinweis auf die wahrscheinliche Ursache des Vorfalls.

Entscheidungen zur Eindämmung:

Wenn sich die Folgen des Vorfalls ausbreiten können, müssen Entscheidungen darüber getroffen werden, wie die vom Vorfall betroffenen Systeme eingegrenzt werden.

Priorisierung von Informationssicherheitsvorfällen

Auf der Grundlage einer Folgenabschätzung wird einem Vorfall eine hohe, mittlere oder niedrige Priorität zugewiesen. Bei der Entscheidung über die Priorität werden folgende Aspekte zugrunde gelegt:

PRIORITÄT	BESCHREIBUNG
Hoch	Erhebliche tatsächliche oder potenzielle Unterbrechung des Geschäftsbetriebs Beispiele: • Malware wurde entdeckt und verbreitet sich über das Netzwerk • Es wurde festgestellt, dass Unbefugte Zugang zu erheblichen Mengen vertraulicher Daten hatten. • Die E-Commerce-Website ist aufgrund eines möglichen Denial-of-Service-Angriffs für Kunden nicht verfügbar

Mittel	Lokalisierte Störungen, die mehrere Geschäftsbereiche betreffen Beispiele: • Einzelnes System nicht verfügbar • Netzwerk läuft langsam • Verlust einer verschlüsselten Festplatte
Niedrig	Örtlich begrenzte Unannehmlichkeiten, die einen einzelnen Nutzer betreffen Beispiele: • Geringfügiger Verstoß gegen Informationssicherheitsichtlinien • Virenalarm auf einem einzelnen Computer • Weitergabe des Passworts an ein System mit geringerer Empfindlichkeit

Tabelle 1: Prioritäten der Vorfälle

Protokollierung

Die Ergebnisse der Bewertung und der Entscheidung werden zur späteren Bezugnahme und Überprüfung detailliert aufgezeichnet.

3.3. Behandlung von Informationssicherheitsvorfällen

3.3.1 Richtlinie

Einstufung von Vorfällen: Vorfälle müssen von der Informationssicherheit auf der Grundlage ihres Schweregrads, ihrer Art und ihrer möglichen Auswirkungen klassifiziert werden.

Rollen und Zuständigkeiten: Die Mitarbeiter der Informationssicherheit sind für die Leitung der Reaktion auf einen Vorfall verantwortlich.

Reaktion: Die Reaktion auf einen Vorfall umfasst Benachrichtigung, Sichtung, Analyse, Eindämmung, Entfernung und Wiederherstellung.

Kommunikation: Der Vorfall muss den betroffenen Parteien intern und/oder extern mitgeteilt werden.

Überprüfung nach einem Zwischenfall: Nachdem ein Vorfall geklärt ist, muss eine Überprüfung durchgeführt werden, um Erkenntnisse und Möglichkeiten zur kontinuierlichen Verbesserung zu ermitteln.

3.3.2 Verfahren

Bei Ereignissen, die aufgrund ihrer größeren Auswirkungen auf die Wertschöpfung der Organisation, als bedeutsam eingestuft und als Informationssicherheitsvorfall behandelt werden, ist es die Aufgabe des IRM-Managers entsprechende hilfreiche Aktivitäten zu initiieren:

- Aktivierung des Notfall-Teams
- Maßnahmen aus dem Notfallplan der Organisation zu initiieren
- Einleitung einer forensischen Analyse, um die Ursachen des Vorfalls zu verstehen
- Wenn erforderlich - alternative Maßnahmen zu erarbeiten und zu initiieren
- Isolation betroffener Bereiche, um eine Ausbreitung des Vorfalls zu beschränken
- Kommunikation mit Betroffenen oder internen bzw. externen interessierten Parteien
- Dokumentation des Vorfall-Geschehens und der Maßnahmen

Da die konkreten Maßnahmen stark von der Art des Vorfalls abhängen, stellt unsere Organisation den Akteuren bei der Behandlung von Vorfällen einen Notfallplan mit konkreten Vorfall-Szenarien und den empfohlenen Maßnahmen zur Verfügung.
[Bitte erstellen Sie als Ergänzung zu dieser Richtlinie unter Berücksichtigung der genannten Anforderungen einen individuellen Notfallplan – am besten mit Flussdiagramm des Melde- & Bearbeitungsprozesses - für Ihre Organisation].

3.4 Protokollierung von Vorfällen & Sammlung von Beweismitteln:

3.4.1 Richtlinie

Es müssen Verfahren existieren, um Beweismittel von Informationssicherheitsvorfällen z.B. für eine datenforensische Untersuchung zu sammeln.

Gesammelte Beweismittel müssen gerichtsverwertbar gesichert werden und können Strafverfolgungsbehörden bzw. Dritten zugänglich gemacht werden.

Die Organisation muss sicherstellen, dass Beweismittel nicht beabsichtigt oder unbeabsichtigt unbrauchbar gemacht werden können.

3.4.2 Verfahren

Alle als Vorfall eingestuften Ereignisse müssen dokumentiert werden, um ein klares und zeitbezogenes Verständnis der entstehenden Situation für sofortige Maßnahmen und zukünftige Überprüfungen zu schaffen. Es sollte ein umfassendes Protokoll erstellt werden, in der die Informationswerte und -träger, Geschäftsaktivitäten, Produkte, Dienstleistungen, Teams und unterstützenden Prozesse aufgeführt sind, die von dem Vorfall betroffen sein könnten. Außerdem sollte diese Liste eine Bewertung des Ausmaßes der Auswirkungen enthalten.

Identifizierung, Erfassung, Beschaffung und Sicherung von Beweismaterial im Zusammenhang mit Informationssicherheitsvorfällen:

1. Verfahren einführen:

Die Organisation muss interne Verfahren für den Umgang mit Beweisen im Zusammenhang mit Informationssicherheitsvorfällen für die Zwecke von Disziplinar- und Gerichtsverfahren festlegen. Diese Verfahren sind zu entwickeln und zu befolgen.

- **Berücksichtigen Sie die Anforderungen der Gerichtsbarkeit**

  Die Anforderungen der verschiedenen Gerichtsbarkeiten sind zu berücksichtigen, um die Chancen auf eine Zulassung in den relevanten Gerichtsbarkeiten zu maximieren.

- **Anweisungen für das Evidenzmanagement**:

  Diese Verfahren enthalten Anweisungen für die Identifizierung, Erfassung, Beschaffung und Sicherung von Beweismitteln in Übereinstimmung mit verschiedenen Arten von Speichermedien, Geräten und dem Status der Geräte (d. h. ein- oder ausgeschaltet).

- **Zulässigkeit von Beweisen**:

  Die Beweise müssen in der Regel in einer Weise erhoben werden, die vor den zuständigen nationalen Gerichten oder einem anderen Disziplinarorgan zulässig ist. Es muss nachgewiesen werden können, dass die Aufzeichnungen vollständig sind und in keiner Weise manipuliert wurden, dass die Kopien elektronischer Beweismittel mit den Originalen identisch sind und dass jedes Informationssystem, aus dem Beweismittel erhoben wurden, zum Zeitpunkt der Aufzeichnung der Beweismittel ordnungsgemäß funktionierte.

- **Zertifizierung oder Qualifizierung**:

  Sofern verfügbar, werden Zertifizierungen oder andere einschlägige Qualifikationsnachweise für Personal und Werkzeuge angestrebt, um den Wert der gesicherten Beweismittel zu erhöhen.

- **Digitale Beweise**:

  Digitale Beweismittel können über Organisations- oder Zuständigkeitsgrenzen hinausgehen. In solchen Fällen muss sichergestellt werden, dass die Organisation berechtigt ist, die erforderlichen Informationen als digitale Beweismittel zu sammeln.

Diese Punkte bilden die Grundlage für ein solides Verfahren zur Verwaltung von Beweismitteln im Zusammenhang mit Vorfällen im Bereich der Informationssicherheit, das eine einheitliche und wirksame Verwaltung von Beweismitteln gewährleistet.

2. Vollständigkeit und Unverfälschtheit der Aufzeichnungen

- Alle Aufzeichnungen im Zusammenhang mit digitalen Beweismitteln müssen systematisch dokumentiert und in

sicheren, manipulationssicheren Behältern aufbewahrt werden.

- Es werden regelmäßige Audits durchgeführt, um die Vollständigkeit der Aufzeichnungen zu überprüfen und Anzeichen von Manipulationen festzustellen.
- Es werden Zugangskontrollen und Prüfverfahren eingeführt, um jegliche Änderungen an den Aufzeichnungen zu überwachen.

3. Überprüfung von identischen Kopien

- Bei der Beschaffung elektronischer Beweismittel werden diese sofort mit einem Hash-Verfahren unter Verwendung von Industriestandard-Algorithmen zur Erstellung digitaler Fingerabdrücke versehen.
- Alle späteren Kopien oder Repliken des Beweismittels werden mit einem Hashwert versehen und mit dem ursprünglichen digitalen Fingerabdruck verglichen, um sicherzustellen, dass der Inhalt identisch ist.
- Zur Wahrung der Integrität des Beweismaterials sind sichere und überprüfte Vervielfältigungsmethoden anzuwenden.

4. Funktionale Verifikation von Informationssystemen

- Vor der Erfassung digitaler Beweismittel ist die Funktionsfähigkeit und Integrität der beteiligten Informationssysteme zu validieren.
- Systemprotokolle, Netzverkehr und Systemkonfigurationen werden überprüft, um den ordnungsgemäßen Betrieb der Informationssysteme während der Beweiserhebung zu bestätigen.
- Alle Anomalien oder Unregelmäßigkeiten im Systemverhalten sind zu dokumentieren und zu beheben, um die Zuverlässigkeit der gewonnenen Erkenntnisse zu gewährleisten.

3.5 Nachbereitung von Ereignissen im Bereich der Informationssicherheit

3.5.1 Richtlinie

Aus Informationssicherheitsvorfällen gewonnene Erkenntnisse müssen zur Verstärkung und Verbesserung der Informationssicherheitsmaßnahmen genutzt werden.

3.5.2 Verfahren

1. Aktionen überprüfen:
Bei Ereignissen, die aufgrund ihrer größeren Auswirkungen auf die Wertschöpfung der Organisation als bedeutsam eingestuft werden, wird eine gründliche Überprüfung durchgeführt, um die Wirksamkeit der durchgeführten Prozesse und den Abschluss aller erforderlichen Maßnahmen sicherzustellen. Wenn bei dieser Überprüfung Mängel festgestellt werden, ist eine Neubewertung früherer Schritte des Verfahrens erforderlich, um die Probleme zu beheben und geeignete Korrekturmaßnahmen zu ergreifen. Dieser iterative Ansatz stellt sicher, dass alle wichtigen Ereignisse angemessen behandelt und gemildert werden, um die Informationssicherheit und die betriebliche Kontinuität des Unternehmens zu gewährleisten.

2. Ereignis schließen:
Wenn das als Vorfall eingestufte Ereignis zufriedenstellend bearbeitet wurde, wird es geschlossen.

3. Aus Vorfällen lernen:
Um nach einem Informationssicherheitsvorfall dem allgemeinen Prinzip der kontinuierlichen Verbesserung zu folgen, sollen alle Vorfälle im Report für das Managementreview auf Verbesserungsansätze überprüft und entsprechend dokumentiert werden. Identifizierte Verbesserungsansätze müssen über eine entsprechende Behandlung im Managementreview Einzug in die kontinuierliche Verbesserung des ISMS finden.

3.6 Aus Vorfällen in der Informationssicherheit lernen & Reaktionen üben

3.6.1 Richtlinie

Das Lernen aus Vorfällen im Bereich der Informationssicherheit muss die Dokumentation und Berichterstattung über Vorfälle, die Analyse der Ursachen, die Pflege eines Speichers für gelernte Lektionen, die Förderung kontinuierlicher Verbesserungen und die Bereitstellung von Schulungs- und Sensibilisierungsprogrammen umfassen. Dies gilt für alle

Mitarbeiter, Auftragnehmer und Einrichtungen, die mit der Organisation in Verbindung stehen, und wird regelmäßig überprüft, um die Anpassung an die sich entwickelnden Anforderungen und die Bedrohungslage sicherzustellen.

3.6.2 Verfahren

Das Verfahren zur Bewältigung von Informationssicherheitsvorfällen, das eine schnelle, wirksame, einheitliche und ordnungsgemäße Reaktion gewährleistet, umfasst

1. Dokumentation und Berichterstattung über Vorfälle

- Alle Sicherheitsvorfälle, unabhängig von ihrem Ausmaß oder ihren Auswirkungen, müssen gründlich dokumentiert werden, einschließlich der ersten Entdeckung, der Reaktionsmaßnahmen und der Analyse nach dem Vorfall.
- Die Vorfallsberichte müssen umfassend sein und die Art des Vorfalls, die betroffenen Systeme oder Daten, die Reaktionsmaßnahmen und die Ergebnisse im Einzelnen aufführen.

2. Analyse der Grundursache

- Nach Beendigung eines Vorfalls wird eine formelle Ursachenanalyse durchgeführt, um die Faktoren zu ermitteln, die zu dem Vorfall beigetragen haben.
- Die Analyse zielt darauf ab, systemische Schwächen, Prozessmängel oder menschliche Fehler aufzudecken, die behoben werden müssen, um ähnliche Vorfälle in Zukunft zu verhindern.

3. Verzeichnis für gelernte Lektionen

- Die Erkenntnisse und Ergebnisse von Vorfallanalysen, einschließlich der Ermittlung der Grundursache und der Abhilfemaßnahmen, werden in einem zentralen Speicher für künftige Referenzen gespeichert.
- Das Repository dient als Wissensbasis für die Organisation und ermöglicht es ihr, bei der Reaktion auf neue Vorfälle oder bei der proaktiven Verbesserung von Sicherheitsmaßnahmen auf frühere Erfahrungen zurückzugreifen.

4. Kontinuierliche Verbesserung

- Die Organisation ist bestrebt, die aus Sicherheitsvorfällen gezogenen Lehren zu nutzen, um ihre Sicherheitskontrollen, Prozesse und das Bewusstsein der Mitarbeiter kontinuierlich zu verbessern.
- Korrektur- und Präventivmaßnahmen, die sich aus der Analyse von Vorfällen ergeben, werden nach Prioritäten geordnet und in die Initiativen der Organisation zur Verbesserung der Sicherheit integriert.

5. Schulung und Sensibilisierung

- Mitarbeiter, die an der Reaktion auf Vorfälle beteiligt sind, sowie relevante Interessengruppen erhalten Schulungen zu den aus der Analyse von Vorfällen gewonnenen Erkenntnissen und bewährten Verfahren.
- Regelmäßige Programme zur Förderung des Sicherheitsbewusstseins sollen die Bedeutung des Lernens aus Vorfällen unterstreichen und die Rolle jedes Einzelnen bei der Gewährleistung einer widerstandsfähigen Sicherheitsumgebung hervorheben.

4. Norm-Referenzen

4.1 Normreferenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. **Einführung**	
2. **Kontakt mit relevanten Parteien und Bedrohungsintelligenz**	
• 2.1 Kontakt mit Behörden	A 5.5
• 2.2 Kontakt mit speziellen Interessengruppen	A 5.6

• 2.3 Bedrohungsintelligenz	A 5.7
3. **Management von Informationssicherheitsvorfällen**	
• 3.1 Grundsätze bzw. Planung des Managements von Informationssicherheitsvorfällen	A 5.24; A 6.8
• 3.2 Bewertung und Entscheidung über Ereignisse im Bereich der Informationssicherheit	A 5.25
• 3.3 Behandlung von Informationssicherheitsvorfällen	A 5.26
• 3.4 Protokollierung von Vorfällen & Sammlung von Beweismitteln	A 5.28
• 3.5 Nachbereitung von Ereignissen im Bereich der Informationssicherheit	A 5.28
• 3.6 Aus Vorfällen in der Informationssicherheit lernen und Reaktionen üben	A 5.27

4.2 Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	**Normkapitel (ISA-TISAX 6.0)**
1. **Einführung**	
2. **Kontakt mit relevanten Parteien und Bedrohungsintelligenz**	
• 2.1 Kontakt mit Behörden	1.2.2
• 2.2 Kontakt mit speziellen Interessengruppen	1.2.2
• 2.3 Bedrohungsintelligenz	1.6.1; 1.6.3; 5.2.5
3. **Management von Informationssicherheitsvorfällen**	
• 3.1 Grundsätze bzw. Planung des Managements von Informationssicherheitsvorfällen	1.6.1; 1.6.2; 2.1.3
• 3.2 Bewertung und Entscheidung über Ereignisse im Bereich der Informationssicherheit	1.6.2; 5.2.4
• 3.3 Behandlung von Informationssicherheitsvorfällen	5.2.5; 5.2.6

• 3.4 Protokollierung von Vorfällen & Sammlung von Beweismitteln	5.3.1
• 3.5 Nachbereitung von Ereignissen im Bereich der Informationssicherheit	5.3.1
• 3.6 Aus Vorfällen in der Informationssicherheit lernen und Reaktionen üben	5.3.1