B to B - Praxistools für Unternehmen und Freiberufler

knowNOW
TOOLS FOR BUSINESS SUCCESS

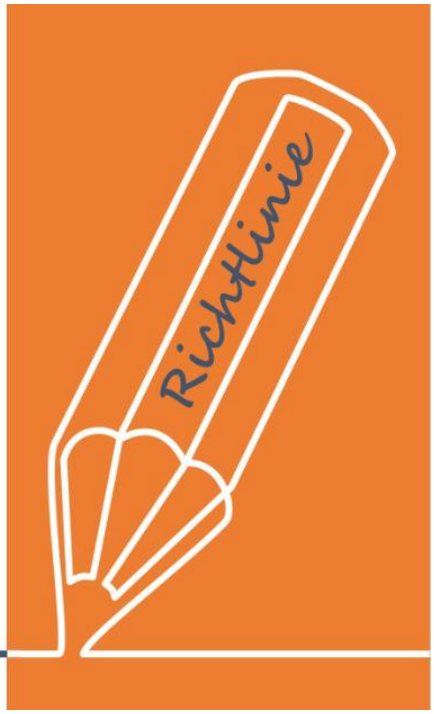
Richtlinie Informationssicherheitsvorfall

UseNOW - TeachNOW - LearnNOW - FindNOW

- Sofort nutzbar: Auswählen - Anpassen - Anwenden
- In der Praxis erprobt und bewährt
- Im Tagesgeschäft sofort anwendbare Hilfsmittel
- Aktuell durch regelmäßige Updates

Richtlinie Informations-sicherheitsvorfall

des Unternehmens



Inhaltsverzeichnis

1. Zweck und Zielsetzung

Diese Richtlinie legt Verfahren zur Erkennung, Meldung, Untersuchung und Behebung von potenziellen Informationssicherheitsvorfällen fest. Das Ziel ist es, die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen zu schützen und sicherzustellen, dass auf Sicherheitsvorfälle angemessen reagiert wird.

2. Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigten, Dienstleister und alle anderen relevanten Parteien, die auf Informationswerte des Unternehmens oder Systeme zugreifen, die diese Informationen schützen.

3. Definitionen

- **Informationssicherheitsereignis:**
  Gelegenheit, bei der es ohne entsprechende Reaktion zu einem Sicherheitsvorfall kommen könnte. Ereignisse machen uns darauf aufmerksam, dass Sicherheitsrisiken in der Organisation bestehen.

- **Sicherheitsvorfall:**
  Einzelnes ungewolltes oder unerwartetes Informationssicherheitsereignis oder eine Reihe solcher Ereignisse, die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die Informationssicherheit zu bedrohen.

Das Ereignis wird basierend auf dessen Risikopotenzial bewertet und ggf. als Vorfall eingestuft. Die Person, die das Ereignis entdeckt, kann vorschlagen, dies als Vorfall zu behandeln. Verantwortlich, ob ein Ereignis als Informationssicherheitsvorfall eingestuft wird, ist jedoch der/die Informationssicherheitsbeauftragte.

4. Verantwortlichkeiten

- **Informationssicherheitsbeauftragter:**
  Verantwortlich für die Koordination von Maßnahmen im Falle von Informationssicherheitsereignissen und Leitung des Reaktionsprozesses bei Sicherheitsvorfällen.

- **IT-Abteilung/IT-Dienstleister:**
  Zuständig für die technische Untersuchung und Behebung von Sicherheitsvorfällen.

- **Beschäftigte:**
  Verantwortlich für die sofortige Meldung aller beobachteten oder vermuteten Informationssicherheitsereignisse.

5. Erfassung von Ereignissen und Vorfällen

Informationssicherheitsereignisse bzw. Sicherheitsvorfälle können auf die folgenden beiden Arten erfasst bzw. erkannt werden:

- **Überwachung**:
  Mittels Implementierung geeigneter technischer Detektivmaßnahmen wird kontinuierlich nach Anzeichen von Informationssicherheitsereignissen bzw. Abweichungen von Sicherheitsvorfällen gesucht.
- **Meldung** durch Mitarbeiter:
  Mitarbeiter melden Informationssicherheitsereignisse bzw. Sicherheitsvorfälle sofort an die IT-Abteilung bzw. dem IT-Dienstleister oder den Informationssicherheitsbeauftragten zu melden:
  Formular Meldung Sicherheitsereignis

6. Kommunikation von Ereignissen und Vorfällen

Zur Vermeidung zeitverzögerter Kommunikation muss im Vorfeld ein Verteiler festgelegt werden, um alle relevanten internen Verantwortlichen zeitnah über das Ereignis oder den Vorfall und ggf. bereits getroffene Maßnahmen zu informieren. Eine Kommunikation außerhalb des Unternehmens hat ausschließlich über die oberste Leitung zu erfolgen.

Die Kontaktaufnahme mit Behörden und Meldung von Sicherheitsvorfällen erfolgt bei Vorliegen einer Meldepflicht. Der/die Informationssicherheitsbeauftragte führt eine Liste, inwieweit gesetzliche Meldepflichten bestehen.

7. Untersuchung und Klassifizierung von Vorfällen

Nach Eingang einer Meldung führt die IT-Abteilung bzw. der IT-Dienstleister zusammen mit dem/der Informationssicherheitsbeauftragten eine Erstbewertung des Ereignisses durch, ob dies als Vorfall eingestuft werden muss. Sicherheitsvorfälle sind zu dokumentieren (*siehe Formular Klassifizierung Informationssicherheitsvorfall*).

Erfolgt die Einstufung als Vorfall, ist die Klassifizierung von Sicherheitsvorfällen nach ihrer Schwere in Kategorien ein wichtiger Schritt, um die richtige Reaktion und Ressourcenallokation sicherzustellen.

Die Schwere eines Sicherheitsvorfalls wird durch verschiedene Faktoren bestimmt, darunter die Art des Vorfalls, die betroffenen Systeme und Daten, die Auswirkungen auf Geschäftsabläufe sowie die Dringlichkeit der Reaktion. Hier sind einige gängige Kriterien zur Klassifizierung und Beispiele für jede Schweregradkategorie zur Einstufung in gering, mittel, hoch oder kritisch:

- **Vertraulichkeit:**
  Welche Art von Informationen sind möglicherweise offengelegt worden?
  Gering: Öffentlich zugängliche Informationen sind betroffen.
  Mittel: Interne Geschäftsinformationen wurden kompromittiert.
  Hoch: Vertrauliche Kundeninformationen oder persönliche Daten wurden offengelegt.
  Kritisch: Geheimhaltungsbedürftige Informationen, strategisches Eigentum oder Sicherheitsdaten wurden kompromittiert.
- **Integrität:**
  Welche Daten wurden verändert oder manipuliert?
  Gering: Es gab keine Beeinträchtigung der Datenintegrität.
  Mittel: Nicht kritische Daten wurden verändert, aber die Auswirkungen sind begrenzt.
  Hoch: Kritische Geschäftsdaten wurden verändert, was zu Fehlentscheidungen führen könnte.
  Kritisch: Manipulierte Daten könnten schwerwiegende rechtliche, finanzielle oder operationelle Folgen haben.
- **Verfügbarkeit**:
  Wie stark ist die Verfügbarkeit von Systemen oder Diensten beeinträchtigt?
  Gering: Kurzfristige Störung eines unwichtigen Systems, schnell behoben.
  Mittel: Einschränkung der Verfügbarkeit eines wichtigen Systems für mehrere Stunden.
  Hoch: Längerfristige Ausfallzeit eines kritischen Systems, das Geschäft wird erheblich beeinträchtigt.
  Kritisch: Komplettausfall von Kernsystemen über längere Zeit, was die Geschäftsfähigkeit massiv beeinträchtigt.
- **Umfang des Vorfalls:**
  Wie viele Systeme oder Daten sind betroffen?
  Gering: Ein einzelner Arbeitsplatzrechner ist betroffen.
  Mittel: Mehrere Rechner oder ein Teilnetzwerk sind betroffen.
  Hoch: Ein gesamtes Netzwerksegment oder mehrere kritische Systeme sind betroffen.
  Kritisch: Der gesamte Unternehmensbetrieb ist betroffen oder der Vorfall betrifft kritische Daten.
- **Geschäftsauswirkungen:**
  Welche direkten und indirekten Auswirkungen hat der Vorfall auf das Unternehmen?
  Gering: Keine nennenswerten Auswirkungen auf Geschäftsprozesse.
  Mittel: Moderate finanzielle Verluste oder Störungen in Geschäftsfunktionen.
  Hoch: Signifikante finanzielle Verluste, rechtliche Probleme oder langfristige Störungen.
  Kritisch: Existenzbedrohende Auswirkungen auf das Unternehmen, massiver Verlust von Marktanteilen oder Kundenvertrauen.

- **Reputationsrisiko:**
  Wie stark könnte der Vorfall dem Ruf des Unternehmens schaden?
  Gering: Kein oder minimaler Reputationsschaden, Vorfall bleibt intern.
  Mittel: Möglicher, aber kontrollierbarer Reputationsschaden, Kundenanfragen müssen begrenzt reagiert werden.
  Hoch: Bedeutender Reputationsschaden, der eine öffentliche Stellungnahme erfordert.
  Kritisch: Schwere Schäden am öffentlichen Image, mögliche langfristige negative Folgen für das Unternehmen.
- **Gesetzliche und regulatorische Auswirkungen**:
  Inwieweit hat der Vorfall rechtliche oder regulatorische Konsequenzen?
  Gering: Keine rechtlichen oder regulatorischen Anforderungen betroffen.
  Mittel: Mögliche Verstöße gegen interne Richtlinien, aber keine externen Meldepflichten.
  Hoch: Mögliche Verstöße gegen regulatorische Anforderungen, die zu Bußgeldern führen könnten.
  Kritisch: Schwere Verstöße gegen gesetzliche Vorgaben, die rechtliche Schritte oder erhebliche Bußgelder nach sich ziehen könnten.

Diese Kriterien sollten regelmäßig überprüft und an die spezifischen Bedürfnisse des Unternehmens und die Risikotoleranz angepasst werden.

8. Reaktion auf Ereignisse oder Vorfälle

Die Reaktion auf Sicherheitsvorfälle muss dem nachfolgend genannten Handlungsmuster, in der dargestellten Schrittfolge, entsprechen.

1. **Eindämmung**:
   Sofortige Maßnahmen zur Eindämmung des Sicherheitsvorfalls, um weitere Schäden zu verhindern.
2. **Beseitigung:**
   Behebung der Ursache des Sicherheitsvorfalls und Wiederherstellung der betroffenen Systeme und Daten.
3. **Erholung:**
   Wiederherstellung des normalen Betriebs und Überprüfung der Wirksamkeit der ergriffenen Maßnahmen.

9. Verlust von Geräten und Datenträgern im Unternehmenseigentum

In diesem Falle ist eine Risikoabschätzung über den Informationsverlust mittels Formular Verlustmeldung für IT-Geräte oder Datenträger durchzuführen.

10. Dokumentation und Nachbereitung von Vorfällen

Nach Abschluss der Vorfallsbehandlung wird ein detaillierter Bericht erstellt, der den Verlauf, die Ursache, die getroffenen Maßnahmen und die Lehren aus dem Vorfall dokumentiert. Es müssen darin zumindest folgende Daten aufgezeichnet werden:

- Datum mit Uhrzeit des Eintritts
- Qualifizierung des Informationssicherheitsereignisses
- Betroffene Systeme, Netze oder Benutzer/in
- Auswirkungen und Auflistung der ergriffenen Maßnahmen
- Datum mit Uhrzeit der Bereinigung
- Schritte der Bereinigung und Abhilfemaßnahmen
- Verfahren

Überschneidung von Sicherheitsvorfall und der Verletzung des Schutzes personenbezogener Daten

Sicherheitsvorfälle, die eine Verletzung des Schutzes personenbezogener Daten beinhalten, bzw. diese nicht mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden können, werden diese in der gesonderten Kategorie „Dokumentation Datenschutzvorfall“ mit Leserechten für den/die Datenschutzbeauftragten abgelegt und der/die Datenschutzbeauftragte werden informiert. Informationen über Informationssicherheitsvorfälle sind vertraulich zu behandeln.

Zusammen mit der obersten Leitung, dem/der Informationssicherheitsbeauftragten und dem/der Datenschutzbeauftragen erfolgt eine Beurteilung, ob eine Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde besteht und ob betroffenen Personen von einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen sind.

11. Überprüfung, Sensibilisierung und Verbesserung

Die Richtlinie wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Bedrohungen, gesetzlichen Anforderungen entspricht. Im Rahmen der Schulungsplanung finden regelmäßige Schulungen und Sensibilisierungsprogramme für alle Mitarbeiter statt, um das Bewusstsein für Informationssicherheit und den richtigen Umgang mit Vorfällen zu fördern.

Maßnahmen gegen Mitarbeiter, die gegen die Richtlinie verstoßen, einschließlich Abmahnung, Kündigung oder rechtlichen Schritten.

12. Dokumentenlenkung und Änderungshistorie

Diese Richtlinie wird über das Intranet zur Verfügung gestellt.

Dokumentenlenkung

Lenkungskriterien	
Klassifizierung der Wichtigkeit (1-10)	
Klassifizierung der Vertraulichkeit	☐ Öffentlich ☐ Intern ☐ Vertraulich ☐ Streng vertraulich
Speicherort	[z.B. URL der Datei auf dem Server]
Verantwortlicher	
Aktuelle Version	1.0
Datum Erstellung / letzte Änderung	19.11.2025
Nächstes Dokumenten-Review	19.11.2026

Dokumentenhistorie

Version	Freigegeben am	Freigegeben durch	Kommentar
1.0	19.11.2025		

Hinweise zur Nutzung der Vorlage

Diese Arbeitshilfe soll nur eine ausführliche Vorlage für eine „Richtlinie zum Umgang mit Informationssicherheitsvorfällen“ darstellen. Sie wurde nach bestem Wissen und Gewissen recherchiert, zusammengestellt und überprüft. Sie erhebt aber keinen Anspruch auf Vollständigkeit oder Eignung für den Einzelfall und erlaubt keine ausschließliche Anwendbarkeit für ein Unternehmen.

Jede Person, die dieses Produkt erwirbt ist verpflichtet, ihre individuellen Ergänzungen und Anpassungen vorzunehmen und alle Inhalte für den eigenen Anwendungsfall zu prüfen, d.h. diese ggf. mit eigenen Texten zu erweitern oder nicht passende Inhalte zu entfernen.

Die nachfolgende Liste gibt Ihnen einige Hinweise, worauf Sie bei der Ergänzung mit eigenen Texten bzw. Textmodulen unbedingt achten sollten:

1. Wählen Sie einfache, allgemein verständliche Formulierungen und schreiben Sie keine „Bandwurmsätze“.
2. Benutzen Sie eine verständliche Wortwahl und erklären Sie nicht vermeidbares Fachvokabular.
3. Formulieren Sie nicht zu sehr ins Detail gehend.
4. Geben Sie den Mitarbeitern im Rahmen von Workshops die Gelegenheit auf die Formulierungen Einfluss zu nehmen.
5. Schreiben Sie gendergerecht. Die Nennung aller Geschlechter drückt die Wertschätzung gegenüber allen Menschen aus, unabhängig ihres Geschlechts.

Hinweise zur Anpassung des Dokumentes an die Organisation:

Um das Tool an Ihre Dokumentenstruktur anzupassen, gehen Sie (hier am Beispiel der Version MS Office 2010 dargestellt) bitte folgendermaßen vor:

1. Aktivieren Sie in der Leiste „Start“, Gruppe „Absatz“ das Symbol „Alle anzeigen“. Alternativ können Sie in der Leiste „Datei“ auf „Optionen“ klicken, im sich öffnenden Fenster „Anzeige“ auswählen und das Häkchen bei „alle Formatierungszeichen anzeigen“ setzen.
2. Löschen Sie nun zuerst das Textfeld mit dem Titel und danach die Grafik, indem Sie diese Objekte jeweils markieren und die Entfernen-Taste (Entf) betätigen.
3. Danach löschen Sie den verbliebenen Abschnittswechsel (oben), indem Sie diesen markieren und ebenfalls die Entfernen-Taste (Entf) betätigen.
4. Mittels „Doppelklick“ auf die Kopf- oder Fußzeile können Sie diese nun öffnen und die Texte und deren Formatierungen entsprechend Ihren Wünschen gestalten.
5. Löschen Sie das Kopfzeilen-Logo wie vorher, indem Sie dieses markieren und die Entfernen-Taste (Entf) betätigen.
6. Ein neues Logo fügen Sie ein, indem Sie in der Leiste „Einfügen“, Gruppe „Illustrationen“ auf das Icon „Grafik“ klicken und Ihre Datei auswählen.
7. Diese Hinweisseite entfernen Sie, indem Sie (ab dem letzten Seitenumbruch) alles markieren und die Entfernen-Taste (Entf) betätigen.

Nutzungsbedingungen von Fachinformationen:

(1) Für vorsätzliche oder grob fahrlässige Pflichtverletzungen haftet der Lizenzgeber. Dies gilt auch für Erfüllungsgehilfen.
(2) Für Garantien haftet der Lizenzgeber unbeschränkt.
(3) Für leichte Fahrlässigkeit haftet der Lizenzgeber begrenzt auf den vertragstypischen, vorhersehbaren Schaden.
(4) Der Lizenzgeber haftet nicht für Schäden, mit deren Entstehen im Rahmen des Lizenzvertrags nicht gerechnet werden musste.
(5) Für Datenverlust haftet der Lizenzgeber nur, soweit dieser auch bei der Sorgfaltspflicht entsprechender Datensicherung entstanden wäre.
(6) Eine Haftung für entgangenen Gewinn, für Schäden aus Ansprüchen Dritter gegen den Lizenznehmer sowie für sonstige Folgeschäden ist ausgeschlossen.
(7) Der Lizenzgeber haftet nicht für den wirtschaftlichen Erfolg des Einsatzes der Tools oder Trainings.
(8) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.