Die Niederösterreichische Versicherung

Informationssicherheitsleitlinie

Leitlinie

Unternehmensname:	Niederösterreichische Versicherung AG und ihre Tochter- bzw. Schwestergesellschaften, nachfolgend als „**NV**“ bezeichnet
Dokumentverantwortlicher:	Informationssicherheitsbeauftragter
Änderungsdatum:	13.10.2020
Freigabeverantwortlicher:	Vorstand
Freigegeben am:	siehe Unterschrift
Version:	4.0
Vertraulichkeitsstufe:	öffentlich
Veröffentlichung:	Das Dokument ist im Intranet abgelegt und für betroffene Mitarbeiter einsehbar. Weiters wird es für die Einsichtnahme durch weitere (gegebenenfalls externe) interessierte Parteien ebenfalls auf der Homepage der NV abgelegt.

Dokumenthistorie

Version	Änderungs-datum	Beschreibung	Bearbeiter
1.0	05.12.2019	Ersterstellung	Simonov I., Müllner W.
1.1	28.01.2020	Änderung der Formatierung	Sukic K.
2.0	03.02.2020	Werbebotschaft gelöscht, Vertraulichkeitsstatus geändert, Stehsatz f. Ablageort hinzugefügt	Sukic K.
3.0	22.09.2020	Hinzufügen von Leitsätzen Nichtkonformitäten und kontinuierliche Verbesserung Hinzufügen der Dokumentenverweise und auch in der Umsetzung Hinzufügen des Dokuments „Übersicht Dokumente“ Überarbeitung der Schutzziele Pflichten jedes Einzelnen	Rom K.
4.0	13.10.2020	Formulierungen zu den Verpflichtungen des Vorstands geändert, Anpassungen zur Publizierung auf der Homepage	Müllner W.

Hinweis:

1.1 wird zu 1.2: Rechtschreibung oder Grammatik verändert sich

1.4 wird zu 2.0: Inhaltliche Änderungen

INHALTSVERZEICHNIS

1 EINLEITUNG

1.1 ZIEL UND ZWECK DIESES DOKUMENTS

Die Abhängigkeit von Daten und Informationssystemen, deren zunehmende Komplexität und die damit verbundenen Gefährdungen machen es notwendig, Anforderungen an die Informationssicherheit zu regeln.
Innerhalb der Informationssicherheitsleitlinie wird die Bedeutung der Informationssicherheit, die Ziele des Informationssicherheitsmanagementsystems und die Verantwortungshaltung innerhalb der Niederösterreichischen Versicherung beschrieben. Das Dokument legt die Informationssicherheits-prinzipien sowie die Informationssicherheitsziele auf Unternehmensebene fest.

Die konkreten Aufgaben und Verantwortungen innerhalb des Informationssicherheits-managementsystems werden separat im Dokument „Informationssicherheitsorganisation“ geregelt.

Ziel ist es somit, den internen und externen Mitarbeitern, den Partnern, Lieferanten, Kunden der Niederösterreichischen Versicherung AG sowie der Öffentlichkeit die Bedeutung der Informationssicherheit mitzuteilen und ihnen zu zeigen, wie die Niederösterreichische Versicherung AG mit Anforderungen umgeht.

Die vorliegende Leitlinie beschreibt die strategische Bedeutung für ein Informationssicherheits-managementsystem. Sie bildet den Rahmen für alle Richtlinien, Prozesse, Tätigkeiten und Ziele innerhalb des Informationssicherheitsmanagementsystems. Sie ist somit eine Handlungsvorschrift mit bindendem Charakter, aber nicht gesetzlicher Natur.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

1.2 GELTUNGSBEREICH

Dieses Dokument gilt organisatorisch für alle internen und externen Mitarbeiter, die regelmäßig am Standort der Niederösterreichischen Versicherung tätig sind. Ebenfalls gilt sie für Geschäfts- und Kooperationspartner, welche im Rahmen ihrer Tätigkeit aufgefordert sind, ihren Beitrag durch konstruktive Mitarbeit zur Einhaltung der Anforderungen bzgl. Informationssicherheit innerhalb des Unternehmens zu leisten.

Von dieser Informationssicherheitsleitlinie umfasst sind Informationen in allen Erscheinungsformen, sei es in elektronischer, schriftlicher, mündlicher oder anderer Form.

Nicht umfasst von dieser Informationssicherheitsleitlinie sind die Funktionen Objektschutz, Brandschutz, Arbeitsplatzsicherheit, Arbeitsmedizin und sonstige, nicht in erster Linie informationsbezogene Themenkreise.

1.3 STRUKTURELLE EINBINDUNG DER MASSNAHMEN UND ZIELE DER ISO 27001

Die Informationssicherheitsleitlinie ist auch Element der Norm ISO 27001 (2015-03).
Insbesondere in Kapitel 5.2 wird die Anforderung an eine Informationssicherheitsleitlinie beschrieben.

1.4 DOKUMENTENVERWEISE

Im Dokument wird auf folgende andere Dokumente verwiesen:

[1] Informationssicherheitsorganisation;
Ablage: SharePoint

[2] Informationssicherheitsstrategie;
Ablage: SharePoint

[3] Übersicht Dokumente;
Ablage: SharePoint

[4] Kontext und Anwendungsbereich;
Ablage: SharePoint

[5] Allgemeine IT-Benutzerrichtlinie
Ablage: SharePoint

Anmerkung: Die hier angeführten Dokumente sind für die interne Verwendung durch die Niederösterreichische Versicherung AG gedacht und werden daher nicht auf der Homepage der NV publiziert.

1.5 ANSPRECHPARTNER

Jeder Leser hat die Möglichkeit, Anfragen im Zusammenhang mit der Informationssicherheitsleitlinie an den Informationssicherheitsbeauftragten der Niederösterreichische Versicherung AG zu richten.

Dazu steht auch eine eigene Mailadresse zur Verfügung: informationssicherheit@nv.at

2 INFORMATIONSSICHERHEITSPOLITIK

Informationssicherheit und der dadurch verbundene Schutz von Daten sind uns ein großes Anliegen. Wir sind überzeugt, dass unsere Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität nur durch ein angemessenes Niveau an Informationssicherheit sichergestellt werden können.

Neben der Sicherheit von IT-Services und darin gespeicherten Daten umfasst Informationssicherheit auch nicht elektronisch verarbeitete und gespeicherte Daten und Informationen (z.B. Transaktionsflüsse, Informationswege). Zusätzlich wird im Rahmen des Informationssicherheitsmanagementsystems die Infrastruktur der Niederösterreichischen Versicherung (z.B. Netzwerke, IT-Räume) geschützt.

Wir tätigen dafür die notwendigen Investitionen in effizientere Prozesse, notwendige Ressourcen und Kompetenzen. Für uns bildet die Erreichung der erforderlichen Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität und den damit verbundenen Informationssicherheitszielen eine Voraussetzung für eine erfolgreiche Umsetzung eines Informationssicherheitsmanagementsystems.

2.1 SCHUTZZIELE DER INFORMATIONSSICHERHEIT

Unsere Schutzziele, welche den Rahmen für die Informationssicherheitsziele bilden, beziehen sich auf die Eigenschaften Vertraulichkeit, Verfügbarkeit und Integrität. Für uns bedeuten diese Begriffe Folgendes:

Vertraulichkeit

Für uns bedeutet Vertraulichkeit persönliche und sensible Daten, Informationen und Programme unserer Kunden, als auch jene unseres Unternehmens vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.

Im Rahmen des ISMS kontrollieren wir einerseits die Einhaltung aller internen und externen Anforderungen bzgl. Vertraulichkeit und überwachen andererseits Vorbeugemaßnahmen, Korrekturmaßnahmen und die Reaktionen, welche zum Schutz der Vertraulichkeit gesetzt werden.

Integrität

Der Begriff der Integrität bezieht sich bei uns auf interne und kundenbezogene Informationen, Daten, als auch die interne Entwicklung und den Betrieb von IT-Services. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben.

Im Rahmen des ISMS kontrollieren wir einerseits die Einhaltung aller internen und externen Anforderungen bzgl. Integrität und überwachen andererseits Vorbeugemaßnahmen, Korrekturmaßnahmen und die Reaktionen, welche zum Schutz der Integrität gesetzt werden.

Verfügbarkeit

Für uns bedeutet Verfügbarkeit, dass die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen dem Kunden und unseren Anwendern zum richtigen Zeitpunkt am richtigen Ort zur Verfügung.

Im Rahmen des ISMS kontrollieren wir einerseits die Einhaltung aller internen und externen Anforderungen bzgl. Verfügbarkeit und überwachen andererseits Vorbeugemaßnahmen, Korrekturmaßnahmen und die Reaktionen, welche zum Schutz der Verfügbarkeit gesetzt werden.

Diese drei Schutzziele der Informationssicherheit schaffen die Voraussetzung dafür, Verantwortung und Vertrauen gegenüber unseren Mitarbeitern, Kunden, Partnern und der Gesetzgebung zu schaffen. Dazu setzen wir uns Informationssicherheitsziele und geben mit vereinten Kräften alles, um diese zu erreichen.

2.2 UNSERE INFORMATIONSSICHERHEITSZIELE

Unter Berücksichtigung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit gibt es für uns wesentliche Ziele, deren Erreichung zum Betrieb, zur Aufrechterhaltung und Weiterentwicklung des Informationssicherheitsmanagementsystems beitragen. Jedes Ziel besitzt dabei die gleiche Priorität bei der Umsetzung.

Wir schaffen **Verantwortung**.

- Wir stellen sicher, dass Mitarbeiter mit sicherheitsrelevanten Aufgaben die erforderlichen Kenntnisse und Fähigkeiten besitzen, die notwendig sind, um ein effektives und sich stetig verbesserndes Informationssicherheitsmanagementsystem zu betreiben.
- Wir stellen die Umsetzung der Anforderungen an gesetzliche, amtliche oder vertragliche Vorschriften sicher.
- Wir schützen IT-Systeme mit uns anvertrauten Daten unserer Kunden.
- Wir sind ein zuverlässiger Partner von Lieferanten und erwarten dies auch von unseren Lieferanten. Vertrauensvolle Beziehungen bündeln unsere Kräfte und erhöhen den Nutzen für unsere Kunden.
- Wir entwickeln und fördern ein umfassendes Sicherheitsbewusstsein unserer Mitarbeiter und schaffen dadurch eine Sicherheitskultur.
- Die Arbeit auf IT-Systemen wird sicher und nachvollziehbar gestaltet.
- Wir übernehmen die Verantwortung über ausreichende Ressourcen (Personal, Infrastruktur, …) zur Aufrechterhaltung des Informationsmanagementsystems.
- Wir überprüfen die Einhaltung unserer eigenen Vorgaben wie Prozesse, Richtlinie, Konzepte oder Handbücher in regelmäßigen, geplanten Abständen.
- Wir sind immer vorbereitet, sollte es doch zu einem Notfall kommen. Wir reagieren rasch darauf und informieren alle betroffenen Parteien.
- Als Leitbetrieb Österreichs übernehmen wir Verantwortung für die Gesellschaft und Umwelt. Zusätzlich nehmen wir auch eine Vorbildfunktion im Bereich Informationssicherheit ein.
- Sollten Nichtkonformitäten auftreten, evaluieren wir diese und setzen entsprechende Korrekturmaßnahmen. Wenn notwendig führen wir Ursachenanalysen durch.
- Wir verbessern kontinuierlich die Eignung, Angemessenheit und Wirksamkeit des Informationssicherheitsmanagementsystems.

Wir schaffen **Vertrauen**.

- Wir ermöglichen Voraussetzungen für den Schutz vor Verlust und Zerstörung von Information und Sicherstellung der Aufrechterhaltung und die Kontinuität aller Geschäftsprozesse.
- Wir schaffen Transparenz über unsere Risiken und setzen vorbeugende Sicherheitsmaßnahmen für Schadensvermeidung und -begrenzung. Dadurch senken wir die Risiken auf ein angemessenes Sicherheitsniveau.

Wir schaffen **Zusammenhalt**.

- Die kontinuierliche Verbesserung des Informationssicherheitsmanagementsystems ist eine ständige Aufgabe und Verpflichtung aller Mitarbeiter.
- Unsere Mitarbeiter bemerken Informationssicherheitsvorfälle und melden diese. Dadurch werden Informationssicherheitsvorfälle rasch erkannt und einem möglichen Schaden entgegengewirkt.

3 UMSETZUNG

Der gesamte Umfang des ISMS (Richtlinien, Prozesse, Organisation) wird im Intranet bzw. SharePoint der Niederösterreichischen Versicherung AG abgebildet.

Die konkreten Verantwortungen des ISMS werden in der Informationssicherheitsorganisation geregelt:

[1] Informationssicherheitsorganisation;
Ablage: SharePoint

Die Informationssicherheitsstrategie beschreibt die strategische Bedeutung und bildet den Rahmen für alle Richtlinien, Prozesse, Tätigkeiten und Ziele für ein ISMS:

[2] Informationssicherheitsstrategie;
Ablage: SharePoint

Die Übersicht Dokumente gibt einen Überblick darüber, welche Dokumente in ihrer Gesamtheit das ISMS bilden:

[3] Übersicht Dokumente;
Ablage: SharePoint

Das Dokument Kontext und Anwendungsbereich beschreibt die Räumlichkeiten, zu schützende Informationen, Prozesse, Mitarbeiter und Schnittstellen an welchen das ISMS angewendet wird:

[4] Kontext und Anwendungsbereich;
Ablage: SharePoint

Anmerkung: Die hier angeführten Dokumente sind für die interne Verwendung durch die Niederösterreichische Versicherung AG gedacht und werden daher nicht auf der Homepage der NV publiziert.

4 PFLICHTEN ZUR EINHALTUNG DER LEITLINIE

Aus Sicht der Niederösterreichischen Versicherung ist Informationssicherheit ein zentrales Thema. Die Politik, Schutzziele und daraus abgeleitete Ziele werden von der Niederösterreichischen Versicherung daher in jeder Hinsicht getragen und unterstützt.

Aufgrund der großen Bedeutung der Informationssicherheit sind alle Mitarbeiter sowie alle anderen Personen, die Daten und Informationen der Niederösterreichischen Versicherung verarbeiten, verpflichtet, die entsprechenden Sicherheitsbestimmungen zu beachten und einzuhalten.

Eine besondere Bedeutung kommt dabei der Vorbildfunktion von Führungskräften zu.

4.1 VERPFLICHTUNG DES VORSTANDS

Der Vorstand der Niederösterreichischen Versicherung AG verpflichtet sich auf Basis der Internationalen Norm ISO 27001 die Verantwortung über die im Folgenden angeführten Bereiche zu übernehmen.

Der Vorstand übernimmt:

- Sicherstellung, dass die Informationssicherheitspolitik und die Informationssicherheitsziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbar sind,
- Vermittlung der Bedeutung eines wirksamen Informationssicherheitsmanagementsystems sowie der Wichtigkeit der Erfüllung der Anforderungen des Informationssicherheits-managementsystems,
- Sicherstellung der Integration von Anforderungen des Informationsmanagementsystems in die bestehenden Geschäftsstrukturen,
- Verantwortung über ausreichende (personelle und infrastrukturelle) Ressourcen zur Aufrechterhaltung des Informationssicherheitsmanagementsystems. Personen werden vom Führungskreis unterstützt und angeleitet, sodass diese zur Wirksamkeit und Erfüllung eines Managementsystems beitragen können,
- Unterstützung relevanter Rollen, sodass diese ihre jeweiligen Verantwortungen verdeutlichen und
- die Aufgabe, die Organisation, deren Geschäftsprozesse sowie -beziehungen fortlaufend zu verbessern.

4.2 PFLICHTEN JEDES EINZELNEN

Die Einhaltung von Prozessen, Richtlinien und Leitlinien ist zur erfolgreichen Umsetzung eines ISMS sehr wichtig. Jeder Einzelne trägt dazu bei die Informationssicherheit und somit die Verfügbarkeit, Integrität und Vertraulichkeit zu bewahren. Verhaltensregeln werden entweder in der Allgemeinen IT-Benutzerrichtlinie [5] oder innerhalb von Richtlinien für Betroffene dargestellt.

Wir wollen gemeinsam verhindern:

- den Missbrauch von Daten, der wirtschaftlichen Schaden oder Haftungsrisiken verursachen kann,
- den unberechtigten Zugriff auf Informationen bzw. ihre Änderung und unbefugte Übermittlung,
- die illegale Nutzung von Informationen aus dem Unternehmen,
- die Gefährdung der Informationssicherheit der Mitarbeiter, Geschäftspartner und des Unternehmens und
- die Schädigung des Rufes unseres Unternehmens.

5 ABSICHTSERKLÄRUNG UND INKRAFTTRETEN

Der Vorstand bekräftigt die Informationssicherheitspolitik, die Schutzziele und Ziele zur Informationssicherheit und zur Erfüllung der Normkonformität nach ISO 27001.

St. Pölten, 14. 10. 2020
(Ort, Datum)

Dr. Hubert Schultes

Mag. Bernhard Lackner

DI Christian Freibauer, MBA