ABl 13/2020, S. 447-452

# Leitlinie zur Informationssicherheit

## 1 Einleitung

Informationen sind wertvolle und schützenswerte Güter des Bistums Augsburg. Die Sicherheit und Zuverlässigkeit der Informationssysteme ist deshalb ebenso wie der vertrauenswürdige Umgang mit Informationen grundlegend für ein verantwortliches Handeln.

Unzureichend geschützte Informationen stellen unkalkulierbare Risiken dar. Voraussetzung für ein angemessenes Sicherheitsniveau ist die Implementierung und der Betrieb eines risikobasierten Managementsystems für die Informationssicherheit.

Die Zielsetzung dieser Leitlinie ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für das Informationssicherheitsmanagement. Sie beschreibt die wesentlichen Anforderungen und Ziele im Hinblick auf die Sicherheit der Informationsverarbeitung im Bistum Augsburg.

Die Diözesanleitung verabschiedet diese Leitlinie zur Informationssicherheit als Bestandteil einer bistumsweiten Sicherheitsstrategie.

## 2 Geltungsbereich und Inkraftsetzung

Diese Leitlinie gilt für das Bischöfliche Ordinariat Augsburg und die der Aufsicht der Diözese unterstehenden Rechtsträger. Auftragnehmer und sonstige externe Dritte, die Einrichtungen oder Informationen des Bistums Augsburg nutzen, werden auf diese Leitlinie gesondert verpflichtet.

Dieses Dokument tritt nach der Bekanntgabe in Kraft, gilt in der jeweils aktuellen veröffentlichten Form und ist verpflichtend anzuwenden.

## 3 Begriffsdefinitionen

Die **Schutzziele** der Informationssicherheit sind die Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen.

Die **Vertraulichkeit** stellt sicher, dass Daten nur von den Personen verändert oder eingesehen werden dürfen, die dazu auch berechtigt sind.

Die **Integrität** stellt sicher, dass Informationen nur von berechtigten Personen geändert werden können.

Die **Verfügbarkeit** stellt sicher, dass die Informationen den zugriffsberechtigten Personen zur Verfügung stehen, wenn ein Zugriff notwendig ist.

Die **Informationssicherheit** hat das Ziel, die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

Das **Informationssicherheitsmanagementsystem** ist ein Teil des gesamten Managementsystems, das auf der Basis eines Risikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.

## 4 Ziele der Informationssicherheit

Informationen und IT-Systeme sind so verfügbar zu halten, dass die zu erwartenden Ausfallzeiten toleriert werden können (Verfügbarkeit). Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). Die Einhaltung der Vertraulichkeit wird über alle Kommunikationsschnittstellen sichergestellt.

Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden. Die Sicherheitsmaßnahmen müssen dabei in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen.

Alle Mitarbeiter tragen zur Informationssicherheit bei und verpflichten sich, die damit verbunden einschlägigen Gesetze und vertraglichen Regelungen einzuhalten und umzusetzen. Negative finanzielle und immaterielle Folgen für das Bistum sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter und Leitungsfunktionen des Bistum Augsburg sind sich ihrer Verantwortung beim Umgang mit Informationen bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

Um dies zu erreichen, bekennt sich das Bistum Augsburg zur Einrichtung, Aufrechterhaltung, Pflege und Weiterentwicklung eines wirksamen Informationssicherheitsmanagementsystems (ISMS) auf Grundlage des international gültigen Standards ISO/IEC 27001.

## 5 Leiter der Stabsstelle Informationssicherheit

Der Leiter der Stabsstelle Informationssicherheit ist durchführungsverantwortlich für den ordentlichen Betrieb und die Aufrechterhaltung des ISMS auf Grundlage dieser Sicherheitsleitlinie.

Der Leiter der Stabsstelle Informationssicherheit ist verpflichtet und berechtigt bei möglichen Gefährdungen der Informationssicherheit andere Mitarbeiter direkt auf die Gefährdung und erforderliche Maßnahmen hinzuweisen.

Der Leiter der Stabsstelle Informationssicherheit ist für die Umsetzung von Informationssicherheitstrainings und Programmen zur Sensibilisierung („Awareness“) der Mitarbeiter für die Informationssicherheit zuständig.

## 6 Informationssicherheitsorganisation

Zur Erreichung der Informationssicherheitsziele wird eine entsprechende Sicherheitsorganisation aufgebaut.

Die Diözesanleitung hat zur Umsetzung der Sicherheitsziele innerhalb der Stabsabteilung IT und Digitalisierung des Generalvikars eine Stabsstelle "Informationssicherheit" eingerichtet und dieser Stabsstelle die Aufgabe übertragen, einheitliche Vorgaben für den Sicherheitsprozess zu erstellen, für ausreichende Sensibilisierung aller Mitarbeiter/innen zu sorgen, sowie die Einhaltung aller Sicherheitsrichtlinien angemessen zu überprüfen bzw. überprüfen zu lassen.

Die Informationssicherheitsorganisationen der Rechtsträger, die der Aufsicht der Diözese unterstehen, berichten an den Leiter der Stabsstelle Informationssicherheit.

Alle Organisationseinheiten wirken jeweils durch einen Vertreter / eine Vertreterin in einem Sicherheitsforum mit, in dem die wesentlichen Richtlinien und Arbeiten koordiniert werden. Die Leitung dieses Sicherheitsforums obliegt der Stabsstelle Informationssicherheit. Insbesondere wird im Sicherheitsforum ein Gesamtsicherheitskonzept erarbeitet und dem IT Direktor zur Genehmigung vorgelegt.

Darüber hinaus tragen alle Mitarbeiter des Bistum Augsburg eine Verantwortung für die Gewährleistung der Informationssicherheit innerhalb ihres Arbeitsbereichs. Sie kommen dieser Verantwortung nach, indem Sie die Informationssicherheitsrichtlinien einhalten.

## 7 Unterstützung durch die Diözesanleitung

Der Stabsstelle Informationssicherheit werden von der Diözesanleitung ausreichende

finanzielle, zeitliche und personelle Ressourcen zur Verfügung gestellt, um die festgelegten Informationssicherheitsziele zu erreichen. Die Diözesanleitung unterstützt den Leiter der Stabsstelle Informationssicherheit, sich regelmäßig weiterzubilden, zu informieren und in den notwendigen internen und externen Gremien und Arbeitskreisen mitzuarbeiten.

## 8 Nachweis der Wirksamkeit des ISMS

Vor dem Hintergrund der oben genannten Sicherheitsziele sind angemessene Nachweise über die Einhaltung der Sicherheitsmaßnahmen zu erbringen und zu archivieren.

Die Mitarbeiter der Stabsstelle Informationssicherheit sind deshalb ermächtigt, Audits durchzuführen, die Aufschluss über die tatsächliche Einhaltung der Schutzziele geben. Sie haben in Abstimmung mit der Diözesanleitung das jederzeitige Zutrittsrecht zu allen Stellen des Bistums in dem zur Durchführung dieser Prüfungen erforderlichen Umfang.

Die Sicherheitsorganisation ist durch die Mitarbeiter der Diözese Augsburg und der ihrer Aufsicht unterstehenden Rechtsträger ausreichend in ihrer Arbeit zu unterstützen.

## 9 Informationssicherheitsrisikomanagement

Das wesentliche Instrument zum Erreichen der Informationssicherheitsziele ist eine regelmäßig stattfindende Risikobewertung. Für die ermittelten Risiken werden Maßnahmen festgelegt, die das Sicherheitsrisiko minimieren. Diese Maßnahmen werden auf ihre Wirksamkeit und Wirtschaftlichkeit bewertet und gesteuert.

Nach Maßgabe dieser Leitlinie ist zunächst jede Organisationseinheit des Bistums Augsburg für die Sicherheit der eigenen Daten und deren Verarbeitung verantwortlich ("Informationseigentümer"). Im Rahmen dieser Verantwortung wird jede Organisationseinheit eine Aufstellung ihrer Assets (Daten, Systeme und Prozesse) anfertigen, eine Risikoanalyse und -bewertung nach vorgegebenem einheitlichen Muster dafür durchführen und in regelmäßigen Abständen sowie nach gravierenden Änderungen aktualisieren. Die Stabsstelle Informationssicherheit wird die Organisationseinheiten dabei unterstützen.

Zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen sind auf der Basis der Risikoeinschätzungen geeignete Maßnahmen darzustellen und umzusetzen.

## 10 Informationssicherheitsrichtlinien

Sicherheitsrichtlinien bilden das Regelwerk für die Informationssicherheit. Sie legen für abgegrenzte Themen die erforderlichen Maßnahmen zur Sicherstellung der Schutzziele fest. Die Richtlinien werden regelmäßig auf Angemessenheit geprüft und aktualisiert. Sie sind für alle Mitarbeiter der Diözese Augsburg und der ihrer Aufsicht unterstehenden Rechtsträger verbindlich.

Verstöße gegen die Informationssicherheitsrichtlinien stellen regelmäßig Verstöße gegen arbeitsvertragliche beziehungsweise werkvertragliche Nebenpflichten dar.

## 11 Informationsklassifizierung

Alle Informationen werden vom Informationseigentümer - eine Person, die für eine Organisationseinheit, einen Prozess oder eine Abteilung verantwortlich ist - entsprechend ihres Schutzbedarfs einer Vertraulichkeitsklasse zugeordnet. Der Umgang mit den Informationen und Systemen basierend auf diesen Vertraulichkeitsklassen wird in einer separaten Richtlinie verbindlich geregelt.

## 12 Lenkung von Dokumenten

Für alle die Informationssicherheit betreffenden Dokumente, Berichte und Aufzeichnungen ist ein Prozess der Dokumentenlenkung festgelegt. In diesem ist die Erstellung, Freigabe, Verteilung, Außerkraftsetzung und Archivierung geregelt.

## 13 Sicherheitsbewusstsein

Das geforderte Maß an Informationssicherheit kann nur erreicht werden, wenn alle Mitarbeitenden des Bistums Augsburg auf die Einhaltung der Informationssicherheit sensibilisiert sind, die eigenen Kompetenzen und Pflichten kennen und sich verantwortungsbewusst verhalten.

Sicherheitsrelevante Themen und Regeln werden den Mitarbeitenden durch geeignete Schulungs- und Informationskanäle vermittelt.

## 14 Projekte

Die Stabsstelle Informationssicherheit ist frühzeitig in alle Projekte mit Auswirkungen auf die Informationssicherheit einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.

## 15 Sicherheitsvorfälle

Das Melden von Sicherheitsvorfällen bietet die Möglichkeit, Lücken zu schließen und das ISMS weiter zu verbessern. Alle Mitarbeiter müssen Schwachstellen und Sicherheitsvorfälle an die Stabsstelle Informationssicherheit melden. Im Zweifelsfall, ob es sich um einen Sicherheitsvorfall handelt, ist der Leiter der Stabsstelle Informationssicherheit um Rat zu fragen.

## 16 Ständige Verbesserung der Informationssicherheit

Das Informationssicherheitsmanagementsystem wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, das Sicherheitsniveau kontinuierlich zu verbessern und ständig auf dem aktuellen Stand der Technik zu halten.

Alle Leitungsfunktionen des Bistums Augsburg unterstützen die ständige Verbesserung des Sicherheitsniveaus.

## 17 Berichtswesen

Die Stabsstelle Informationssicherheit berichtet quartalsweise an den IT Direktor über den Stand der Informationssicherheit. Für die Diözesanleitung wird ein jährlicher Bericht zur Sicherheitslage im Bistum Augsburg erstellt.

## 18 Inkrafttreten

Diese Leitlinie tritt zum 01.12.2020 in Kraft.