Informationssicherheitsstrategie der BOKU

Die Informationssicherheitsstrategie legt die langfristige Vorgehensweise bei der Umsetzung der Informationssicherheitspolitik der BOKU, basierend auf grundlegenden Prinzipien, fest. Die dabei angestrebten Sicherheitsziele entsprechen den in der Informationssicherheitspolitik der BOKU angeführten Zielen.

Beschlossen durch das Rektorat am 04.06.2019.

Inhaltsverzeichnis

1 Zweck und Inhalt

Die Informationssicherheitsstrategie legt die langfristige Vorgehensweise bei der Umsetzung der Informationssicherheitspolitik der BOKU, basierend auf grundlegenden Prinzipien, fest. Die dabei angestrebten Sicherheitsziele entsprechen den in der Informationssicherheitspolitik der BOKU angeführten Zielen.

2 Geltungsbereich

Diese Sicherheitsstrategie gilt verpflichtend für alle Angehörigen der BOKU sowie für Personen, die in BOKU-nahen Organisationen tätig sind.

Dritte sind über vertragliche und sonstige Vereinbarungen in den jeweils relevanten Punkten zu verpflichten.

Darüber hinaus gilt diese Sicherheitsstrategie ohne zeitliche und örtliche Einschränkungen.

3 Angestrebtes Sicherheitsniveau

Die BOKU setzt Sicherheitsmaßnahmen um, die sich durch einen Kompromiss zwischen Sicherheitsanforderungen einerseits und Funktionalität, Leistungsfähigkeit, Wirtschaftlichkeit sowie Bedienkomfort andererseits auszeichnen.

In Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität und Unverfälschtheit von Daten und Informationen strebt die BOKU an, ein angemessen hohes Sicherheitsniveau zu implementieren.

Aus den ermittelten Schutzbedürfnissen sind folglich entsprechende Maßnahmen[1] abzuleiten, wobei „Good Practices“[2] und „der Stand der Technik“ als Grundlage angesehen werden.

4 Zu behandelnde Themen

Zu behandeln sind zumindest die folgenden Themenkreise[3]:

- Personenbezogene Sicherheit – Human resource security
- Umgang mit Ressourcen (Verwaltung der Werte) – Asset management
- Zugangssteuerung – Access control

[1] Maßnahmen können organisatorischer, technischer und personeller Natur sein.

[2] Darunter wird eine grundsätzliche Normen- und Standardorientierung verstanden, z.B. an ISO/IEC Normen, ITIL, und Branchenstandards (z.B. BSI-Standards).

[3] Entnommen der ISO/IEC 27001:2013 bzw. der ISO/IEC 27002:2013.

- Kryptografie – Cryptography
- Physische und umgebungsbezogene Sicherheit – Physical and environmental security
- Betriebssicherheit – Operations security
- Kommunikationssicherheit – Communications security
- Anschaffung, Entwicklung und Instandhalten von Systemen – System acquisition, development and maintenance
- Lieferantenbeziehungen – Supplier relationships
- Handhabung von Informationssicherheitsvorfällen – Information security incident management
- Informationssicherheitsaspekte beim Business Continuity Management – Information security aspects of business continuity management
- Einhaltung gesetzlicher und vertraglicher Anforderungen – Compliance

Die BOKU-IT ist im Rahmen der Informationssicherheitspolitik und des etablierten ISMS (Information Security Management System) berechtigt, Richtlinien bzw. Änderungen an bestehenden Richtlinien (insbesondere kleine Updates und bei „Gefahr im Verzug“) auszuarbeiten und für die BOKU vorläufig in Kraft zu setzen. Themen die den Schutz personenbezogener Daten berühren, müssen dabei mit dem Datenschutzbeauftragten abgestimmt werden. Die Bestätigung von zwischendurch seitens der BOKU-IT vorläufig in Kraft gesetzten Richtlinien und Richtlinien-Updates erfolgt regelmäßig durch das Rektorat.

5 Prinzipien zur Erreichung der angestrebten Ziele

5.1 Berücksichtigung der Informationssicherheit in allen Projekten[4]

Informationssicherheit wird bei Projekten mit Bezug zu informationssicherheitsrelevanten Zielen als ein eigenständiges Projektziel betrachtet.

In Bezug auf Projekte ist Informationssicherheit ein gleichwertiges Ziel neben Funktionalität und Leistungsfähigkeit bei der Entwicklung, der Beschaffung und dem Einsatz von informationsverarbeitenden Systemen.

5.2 Orientierung an Good Practice-Ansätzen

Informationssicherheit bei der BOKU orientiert sich an anerkannten Normen sowie Good Practice-Ansätzen – diese sind zumindest folgende:

[4] Die projektverantwortliche Person ist dafür zuständig, sicherzustellen, dass der Schutzbedarf der Daten und Informationen erhoben und berücksichtigt wird.

- ISO/IEC 27001 und ISO/IEC 27002
- Österreichisches Informationssicherheitshandbuch
- BSI-Standards

Darüber hinaus können auch andere, international oder national anerkannte Normen und Best Practice-Ansätze verwendet werden, die auf Besonderheiten einer Einsatzumgebung abgestimmt sind oder zwingend berücksichtigt werden müssen.

5.3 Klassifizierung durch die InformationsEigentümer/innen

Die Klassifizierung (Schutzbedarfsfeststellung) sowie Autorisierung zur Nutzung der Daten und Informationen erfolgt durch deren Eigentümer/innen[5] (engl. Owner), die Umsetzung der Autorisierung durch deren Verwalter/innen[6] (engl. Custodians).

Eigentümer/innen im Kontext dieses Dokuments besitzen die legitimierte Verfügungsberechtigung über Daten und Informationen und sind für diese verantwortlich. Sie legen deren Schutzbedarf fest.

Verwalter/innen sind im Kontext dieses Dokuments Organisationen, Organisationseinheiten oder Personen, die im Rahmen ihrer Funktion beauftragt und zuständig sind, Daten und Informationen im Sinne des Eigentümers/der Eigentümerin zu verwenden, zu verarbeiten, zu übermitteln etc.

5.4 Anwendung des Need-to-Know-Prinzips

Die Autorisierung zur Nutzung von Daten und Informationen orientiert sich an der auszuführenden Aufgabe. Das bedeutet, jeder Person sind nur jene Daten und Informationen zugänglich zu machen, die für die Erfüllung ihrer Aufgaben bzw. Ausübung Ihrer Rolle notwendig sind (Prinzip des notwendigen Wissens).

5.5 Anwendung des Least-Privilege-Prinzips

Personen, BenutzerInnen, Systeme, Programme etc. verfügen über so wenig Zutritts- bzw. Zugriffsrechte wie möglich. Das bedeutet, dass Rechte zum Betreten, Lesen bzw. Anlegen, Schreiben, Ändern, Löschen, Ausführen oder zur Übertragung von Berechtigungen, gemessen an der durchzuführenden Aufgabe, im jeweils geringstmöglichen Ausmaß erteilt sind (Prinzip der Vermeidung überschießender Rechte).

[5] Dieser Begriff ist vergleichbar mit dem des Auftraggebers im Datenschutzrecht. Eigentümer sind z.B. Fachabteilungen, Institute, Tochtergesellschaften, assoziierte Vereine, Kooperationspartner, Projektteams).

[6] Dieser Begriff ist vergleichbar mit dem des Dienstleisters im Datenschutzrecht.

6 Vorgehensweisen zur Erreichung der angestrebten Ziele

Die zu wählenden Sicherheitsmaßnahmen sind anhand von anerkannten Methoden und Standards nachvollziehbar herzuleiten, zu begründen und anschließend regelmäßig, aber auch anlassbezogen, auf ihre Wirksamkeit hin zu untersuchen.

6.1 Erfassung

Daten- und Informationsbestände inklusive dazugehöriger Prozesse und Ressourcen[7] sind strukturiert zu erfassen.

6.2 Zuordnung

Den Daten- und Informationsbeständen, dazugehörigen Prozessen und Ressourcen sind eindeutige Eigentümer/innen (Owner) und Verwalter/innen (Custodians) zuzuordnen.

6.3 Ermittlung des Schutzbedarfs und Erstellung von Sicherheitskonzepten

Der Schutzbedarf der Daten- und Informationsbestände und der zugehörigen Prozesse und Ressourcen ist zu ermitteln, gegebenenfalls mit Hilfe entsprechend detaillierter Risikoanalysen und nach gängigen, anerkannten Methoden, zumindest entsprechend dem Stand der Technik und gemäß „good practices“. Ausgehend vom Schutzbedarf sind entsprechende Sicherheitskonzepte[8] zu entwickeln.

6.4 Umsetzung der Sicherheitskonzepte

Die entstandenen Sicherheitskonzepte sind mit den vorhandenen Maßnahmen abzugleichen. Die sich daraus ergebenden offenen Maßnahmen sind zu realisieren, und damit das jeweilige Konzept insgesamt umzusetzen. Die Konzepte und Maßnahmen sind laufend an die aktuellen Gegebenheiten anzupassen.

6.5 Übernahme von Restrisiken

Restrisiken sind festzuhalten, zu bewerten und vom Eigentümer/von der Eigentümerin formell zu übernehmen.

[7] Umfasst Menschen, Gebäude und deren Einrichtung, IT-Infrastruktur, IT-Systeme, Anwendungen etc.

[8] Mit dem Begriff Sicherheitskonzept wird ein Bündel aus organisatorischen, technischen und personellen Maßnahmen bezeichnet. Zu diesen Maßnahmen gehören neben der Entwicklung von Richtlinien und Standards auch Prozessbeschreibungen, technische Pläne und Architekturbeschreibungen, Schulungsmaßnahmen etc.

6.6 Überprüfung der Einhaltung der Sicherheitskonzepte

Die Einhaltung der Sicherheitskonzepte ist durch geeignete Kontrollinstanzen, sowohl intern, als auch durch dazu beauftragte Dritte sicherzustellen.

6.7 Dokumentation

Die im Rahmen der Erstellung und Umsetzung von Sicherheitskonzepten, sowie im laufenden Betrieb durchgeführten Aktivitäten und Arbeitsergebnisse sind entsprechend zu dokumentieren, sodass deren Auditierbarkeit gewährleistet ist.

7 Folgen der Nichtumsetzung

Die Einhaltung der Prinzipien und der Vorgehensweise wird regelmäßig, aber auch anlassbezogen überprüft.

Eine Missachtung der sicherheitsbezogenen Vorgaben kann neben entsprechenden disziplinären auch zivil- und strafrechtliche Folgen nach sich ziehen.

Historie

Letzte Änderung: 23. Jänner 2020

Die **aktuelle Version** dieser Dokumentation finden Sie auf den Serviceseiten der BOKU-IT unter: http://short.boku.ac.at/it-guidelines

Dokument		**Informationssicherheitsstrategie der BOKU**	**Informationssicherheitsstrategie_DE_V.1.0.4_2019-02-20.docx**
Quelldokument		BOKU	---
Aktualisierungsdatum / Autor/in	**Version**	**Änderungen**	
2016-06-08 (CK/ZID)	1.0.0	Dokument erstellt	
2016-11-07 (CK/ZID)	1.0.1	Korrekturen	
2017-07-11 (AST, AS/ZID)	1.0.2	Überarbeitung	
2017-10-02 (AST, AS/ZID)	1.0.3	Link für BOKUweb eingefügt, zur Genehmigung freigegeben	
2019-02-20 (AST, AS/ZID)	1.0.4	Passus: Bestätigung vorläufig durch BOKU-IT in Kraft gesetzter Richtlinien durch das Rektorat	
2020-01-23 (AST, BOKU-IT)	1.0.5	Umbenennung ZID in BOKU-IT	