Regelungshierarchie zu Informationssicherheit der BOKU

Die Regelungshierarchie zu Informationssicherheit der BOKU verdeutlicht die Abhängigkeiten zwischen Regelungen auf unterschiedlichen Stufen in Form einer hierarchischen Struktur und sorgt für die notwendigen begrifflichen Abgrenzungen.

Beschlossen durch das Rektorat am 03.10.2017.

Inhaltsverzeichnis

1 Zweck und Inhalt

Die Regelungshierarchie zu Informationssicherheit der BOKU verdeutlicht die Abhängigkeiten zwischen Regelungen auf unterschiedlichen Stufen in Form einer hierarchischen Struktur und sorgt für die notwendigen begrifflichen Abgrenzungen.

2 Die Regelungshierarchie zu Informationssicherheit

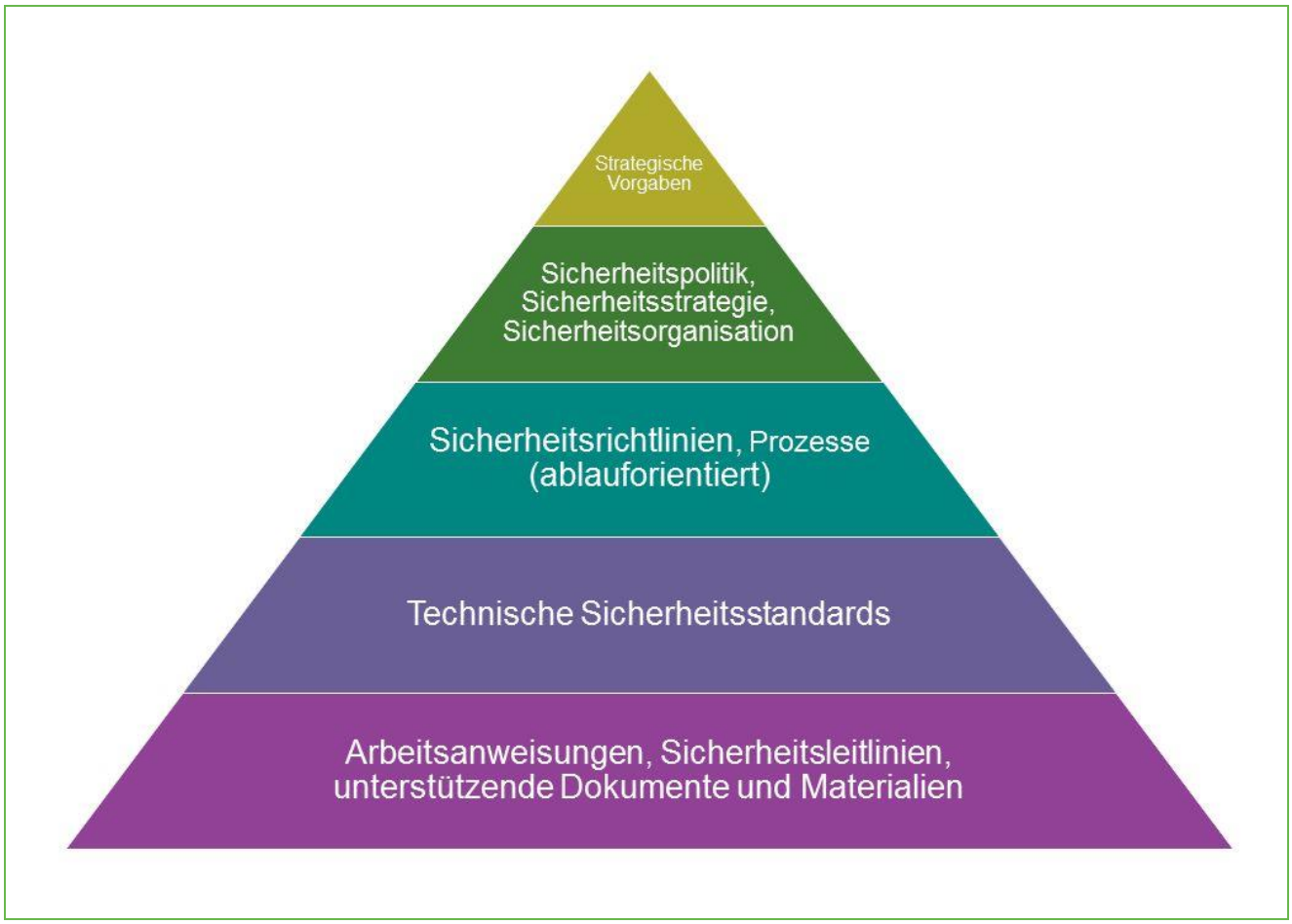

Abbildung 1: Die Regelungshierarchie zu Informationssicherheit

3 Details zu den Ebenen der Regelungshierarchie

Strategische Vorgaben

- Die oberste Ebene **Strategische Vorgaben** umfasst die langfristige Ausrichtung der BOKU, Mission, Vision, Leitbilder, Entwicklungspläne, Schwerpunktprogramme, Leistungsvereinbarungen etc.

Sicherheitspolitik inklusive -strategie und -organisation

- Die Sicherheitspolitik und -strategie drückt die Ansichten und Einstellungen, sowie die Verantwortungshaltung des Rektorats aus, unter anderem in Form von Grundsatzaussagen (Prinzipien) und strategischen Formulierungen. Sie beschreibt auf einer übergeordneten Ebene, was zu tun ist, beinhaltet das Mandat für die Umsetzung ihres Inhalts, d.h. erteilt den ausdrücklichen Auftrag dazu, gibt Ziele vor und legt Verantwortlichkeiten fest. Die **Einhaltung** der Sicherheitspolitik und -strategie durch die Angesprochenen ist **verpflichtend**. Eine Abkehr von dieser Verpflichtung bedarf besonderer, ausdrücklicher Genehmigung.
  Um einen Sicherheitsprozess erfolgreich planen, umsetzen und aufrechterhalten zu können, muss eine geeignete Organisationsstruktur für Informationssicherheit vorhanden sein. Es müssen also Rollen definiert sein, die die verschiedenen Aufgaben für die Erreichung der Sicherheitsziele wahrnehmen.

  Beispiel einer Formulierung: „Die Vertraulichkeit von Information muss entsprechend den gesetzlichen Vorgaben und ihrer Sensitivität gewährleistet sein."

Sicherheitsrichtlinien, Prozesse

- Sicherheitsrichtlinien und zugehörige Prozesse sind **verbindliche Regelwerke** zum Zweck der Umsetzung der Sicherheitspolitik und -strategie. Sie erwähnen Personen, Technologien, Methoden und Prozeduren auf prozessorientierter Ebene und erläutern, wie das, was in der Sicherheitspolitik und -strategie festgelegt ist, umzusetzen ist. Ihre Einhaltung ist verpflichtend. Eine Abkehr von dieser Verpflichtung bedarf besonderer, ausdrücklicher Genehmigung.

  Beispiel: „Sensible Daten und Informationen, die über Netzwerke übertragen werden, sind zu verschlüsseln. Dabei sind die Normen X und Y einzuhalten."

Technische Sicherheitsstandards

- Technische Sicherheitsstandards sind verbindliche Regelwerke zum Zweck der Umsetzung der Richtlinie bzw. des Prozesses. Sie beschreiben Prozeduren, Konfigurationsparameter und sonstige Details auf technischer Ebene und erläutern, wie das, was im Prozess festgelegt ist, umzusetzen ist. Ihre **Einhaltung** ist **verpflichtend**. Eine Abkehr von dieser Verpflichtung bedarf besonderer, ausdrücklicher Genehmigung.

  Beispiel: „E-Mails sind mittels S/MIME folgendermaßen zu verschlüsseln: abc. Für die Verschlüsselung von ruhenden Daten auf Windows-Endgeräten ist Bitlocker zu verwenden und folgendermaßen zu konfigurieren: xyz."

Regelungshierarchie zu Informationssicherheit der BOKU

Arbeitsanweisungen, etc.

- Arbeitsanweisungen sind konkrete Anleitungen, die die/den Einzelne/n bei der Einhaltung der Richtlinien und Standards unterstützen. Ihre **Einhaltung** ist **verpflichtend**.

  Beispiel einer Arbeitsanweisung: „Bei der Ausgabe von Smartphones sind folgende Checklisten-Punkte mit dem/der Empfänger/in abzuarbeiten: a, b, c. Die Liste ist binnen 72h per E-Mail an xyz zu übermitteln.“

Sicherheitsleitlinien

- Leitlinien sind **unverbindliche** Vorschläge und Empfehlungen, die die/den Einzelne/n bei der Einhaltung der Richtlinien und Standards unterstützen. Die Einhaltung von Leitlinien durch die Betroffenen ist nicht verpflichtend.

  Beispiel einer Leitlinienformulierung: „Nehmen Sie nicht automatisch an, dass die Empfänger Ihrer E-Mails die selbe Sorgfalt walten lassen wie Sie. Bedenken Sie, dass Sie keinen Einfluss darauf haben, wie E-Mails beim Empfänger /bei der Empfängerin verwaltet werden und wer darauf Zugriff hat.“

Unterstützende Dokumente und Materialien

- Z.B. Sensibilisierungsunterlagen wie Schulungspräsentationen, Poster, Vorlagen, Checklisten, E-Mails etc.

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		**Regelungshierarchie zu Informationssicherheit der BOKU**	**RegelungshierarchieZuInformationssicherheit_DE_V.1.0.3_2017-10-02.docx**
Quelldokument		BOKU	---
Aktualisierungsdatum / Autor/in	**Version**	**Änderungen**	
2016-06-08 (CK/ZID)	1.0.0	Dokument erstellt	
2017-07-11 (AS/ZID)	1.0.1	Überarbeitung	
2017-10-02 (AST, AS/ZID)	1.0.2	Link für BOKUweb eingefügt, zur Genehmigung freigegeben	
2020-01-23 (AST, BOKU-IT)	1.0.3	Umbenennung ZID in BOKU-IT	