GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Die neue Informationssicherheitsrichtlinie der Universität

20./27.02.2020

Dr. Holger Beck, Informationssicherheitsbeauftragter
isb@uni-goettingen.de

Die neue Informationssicherheitsrichtlinie

- Veröffentlicht am 24.01.2020 in den Amtlichen Mitteilungen
  - s. http://www.uni-goettingen.de/de/amtliche+mitteilungen+2020/618871.html
- Struktur
  - Grundsätze
  - Organisatorische Festlegungen
  - Inhaltliche Festlegungen
    - inkl. Maßnahmenkatalog als Anlage mit zwei Teilen (wie schon in alten Richtlinien)
    - Maßnahmen für IT-Anwender und
    - Maßnahmen für IT-Personal
- Fokus für die meisten Personen: Maßnahmen für IT-Anwender
  - bisheriges Faltblatt hierzu wird zeitnah ersetzt

Rollen in der Informationssicherheit

Verantwortlichkeiten und Aufgaben für den Informationssicherheitsprozess
Organisation von Informationssicherheit, Konzepte, Kontroll- und Berichtsfunktionen

Verantwortlichkeiten und Aufgaben für Informationsverarbeitung und deren Informationssicherheit
Verantwortlichkeiten für originäre Aufgaben und Berücksichtigung von Informationssicherheit bei der Umsetzung der Aufgaben

Zentral

Datenschutz- und Informationssicherheits-Beirat
Zusammensetzung: ISB, DSBe, ISM, DSM, Vertreter der IT-Dienstleister und der Personalräte, Fakultäten, Krankenversorgung, Verwaltung, Sonstige bei Bedarf
Aufgaben: Abstimmung ISB, DSB, Dienstleister, Fakultäten usw.

Präsidium und Vorstand
Gesamtverantwortung

IT-Steuerungsgruppe und CIO
Zusammensetzung gemäß GeschO
strategische **Aufgaben** gemäß GeschO

Informationssicherheitsbeauftrage(r) ISB
Aufgaben: Koordination des Informationssicherheitsprozesses, Beratung, Erarbeitung von allgemeinen und Stellungnahmen zu spezifischen Informationssicherheitskonzepten.

Informationssicherheitsmanager(in) ISM
je einer für Universität und UMG
Aufgaben: Steuerung und Überwachung der Umsetzung von Informationssicherheit (operativ)

IT-Dienstleister
Aufgaben: IT-Dienstleistungen, Gefahrenabwehr, Beratung und Unterstützung, Informationssicherheit im eigenen Bereich

Dezentral

Zuständige Leitung
Aufgaben: Verantwortung für Informationssicherheit in der Einheit, Beschluss spezifischer Informationssicherheitskonzepte

Informationssicherheitskoordinator(in) ISK
Bestellung durch zuständige Leitung
Aufgaben: Koordination und Überwachung des Informationssicherheitsprozesses in der Einheit, Stellungnahme zu spezifischen Informationssicherheitskonzepten

Fachverantwortliche
Benennung durch zuständige Leitung
Aufgaben: Zuständig für Informationssicherheit in der Fachaufgabe und Informationssicherheitskonzept dafür, veranlasst und kontrolliert Umsetzung von Maßnahmen in der Fachaufgabe

IT-Personal
Aufgaben: Umsetzung von Maßnahmen entsprechend des Maßnahmenkatalog (Teile A und I) und der Konzepte in der eigenen Aufgabe

IT-Anwender
Aufgaben: Umsetzung von Maßnahmen des Maßnahmenkatalogs Teil A

Maßnahmen für Anwender - Überblick

A.1 Anwenderqualifizierung
A.2 Meldung von IT-Problemen
A.3 Konsequenzen und Sanktionen bei Sicherheitsverstößen
A.4 Kontrollierter Softwareeinsatz
A.5 Schutz vor Viren und anderer Schadsoftware
A.6 Zutritts-, Zugangs- und Zugriffskontrolle
A.7 Sperren und ausschalten
A.8 Sicherung von Notebooks, mobilen Speichermedien, Smartphones
A.9 Personenbezogene Nutzerkonten
A.10 Gebrauch von Passwörtern
A.11 Zugriffsrechte
A.12 Netzzugänge
A.13 Telearbeit
A.14 Sichere Netzwerknutzung - Allgemeine Anforderungen
A.15 Sichere Netzwerknutzung - E-Mail
A.16 Datenspeicherung
A.17 Nutzung externer Dienste
A.18 Nutzung privater Hard- und Software
A.19 Datensicherung und Archivierung
A.20 Umgang mit Datenträgern
A.21 Löschen und Entsorgung von Datenträgern
A.22 Sichere Entsorgung vertraulicher Papiere

Maßnahmen für Anwender - Highlights

- Sichere Netznutzung – E-Mail
  - E-Mails als potentielles Problem für den Datenschutz
    - Unberechtigte Weiterleitung personenbezogener Daten
      - Nur dienstliche E-Mail-Konten verwenden
      - Keine automatische Weiterleitung von E-Mails zu externen E-Mail-Diensten
      - Nicht zur Verteilung personenbezogener Daten geeignet
  - E-Mails als potentielles Problem für die Informationssicherheit
    - Haupteinfallstor für Viren, Trojaner und andere Schadsoftware
    - Auslöser für die Totalausfälle z.B. der Uni Gießen waren E-Mails!
      - Umgang mit Anhängen und Links in E-Mails: Nur öffnen / anklicken, wenn ihre Ungefährlichkeit, z.B. durch Herkunft und Kontext, anzunehmen ist.
      - Aber Vorsicht: Die Fälschungen durch Internet-Kriminelle sind sehr gut und teils kaum zu erkennen!

Maßnahmen für Anwender - Highlights

- Datenspeicherung
  - Dienstliche Daten sind grundsätzlich auf IT-Systemen der Universität zu speichern (also nicht bei Dropbox und anderen Clouddiensten) und möglichst auf zentralen Servern
  - Ausnahmen nur wenn dienstlich erforderlich und in einem (zu genehmigenden) Konzept beschrieben und unter bestimmten Rahmenbedingungen
  - Besonderheiten bei personenbezogenen Daten u.ä. zusätzlich:
    - zumindest Verschlüsselung bei Daten auf Arbeitsplatzrechnern oder mobilen Geräten
    - Zusätzliche Restriktionen für externe Speicherung
- Externe Dienste
  - Skype, Teamviewer, … nur zulässig, wenn eine spezifisches Konzept das explizit erlaubt.

Danke für die Aufmerksamkeit!

Fragen?