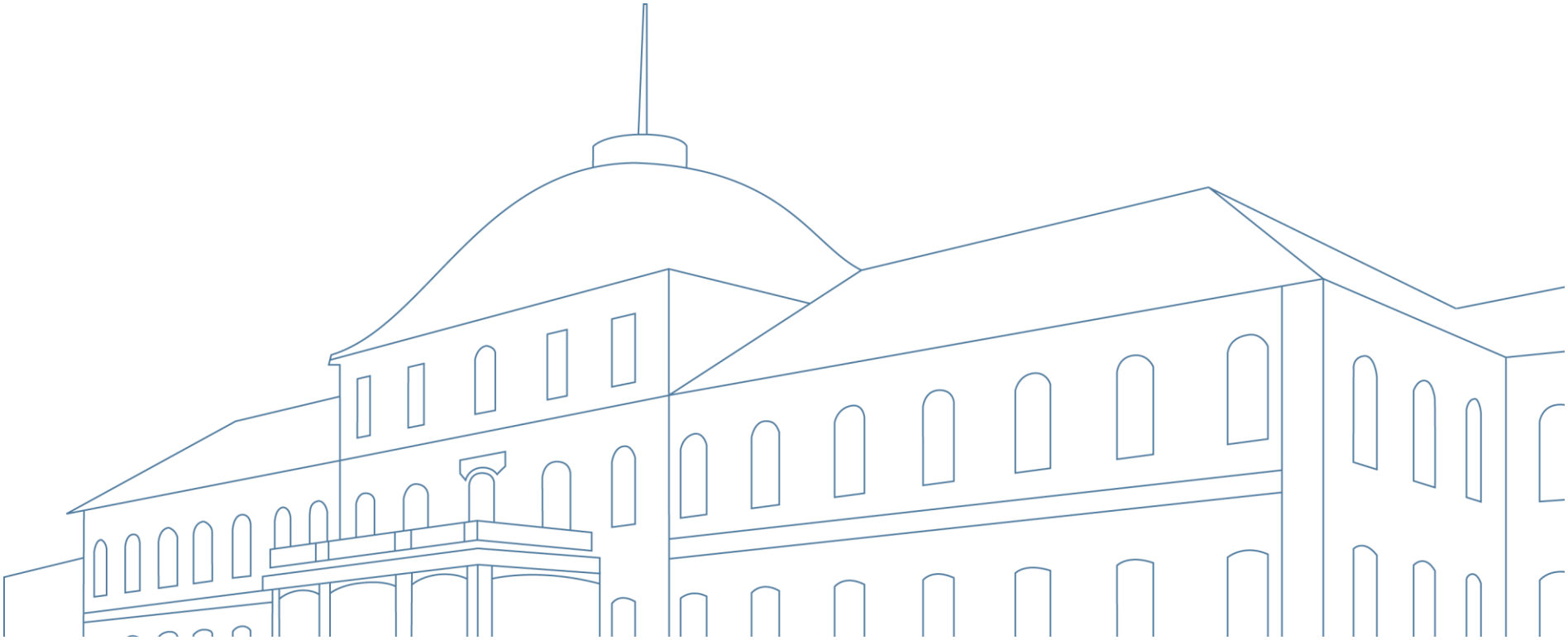
UNIVERSITÄT HOHENHEIM

Die Universität Hohenheim



AGENDA

1. Information und Kennzahlen zur Universität Hohenheim

2. Strukturelle Modellierung eines IT-Sicherheitskonzepts

    a. Rahmenbedingungen organisatorischer Natur
    b. Normen und Vorschriften generell-abstrakter Natur

3. Pragmatische Umsetzung

    a. Konzeptionelle Auditierung und abzuleitende Maßnahmen
    b. Reflexionen zu Leitlinie und Richtlinien
    c. IT-Sicherheitsstandards

Information und Kennzahlen zur Universität Hohenheim

Die Universität Hohenheim, älteste Universität Stuttgarts, ist am 20. November 1818 durch König-Wilhelm I von Württemberg als landwirtschaftliche Unterrichts-, Versuchs- und Muster-anstalt gegründet worden.

Der „schönste Campus des Landes“ (Unicum 2009) beherbergt drei Fakultäten:

- Agrarwissenschaften (26,9 % Studierende)
- Naturwissenschaften (18,9 % Studierende)
- Wirtschafts- und Sozialwissenschaften (54,1 % Studierende)

Information und Kennzahlen zur Universität Hohenheim

- Im Wintersemester 2016/2017 sind 9.638 Studierende immatrikuliert:
  - 1.407 Studierende mit internationalem Hintergrund.
  - Jährliche Fluktuation durch 2.900 Anfangende & 2.300 Absolventen.
- Die Universität Hohenheim beschäftigt 2.041 Mitarbeiter:
  - 123 Professoren/-innen,
  - 818 Wissenschaftlich Beschäftigte,
  - 1.100 Beschäftigte in Administration, Technik und Service.
- Die Finanzeinnahmen betragen ca. 144,2 Mio. Euro.
- Die Gesamtfläche beträgt ca. 838 ha (8,38 km² oder 1.170 Fußballfelder).

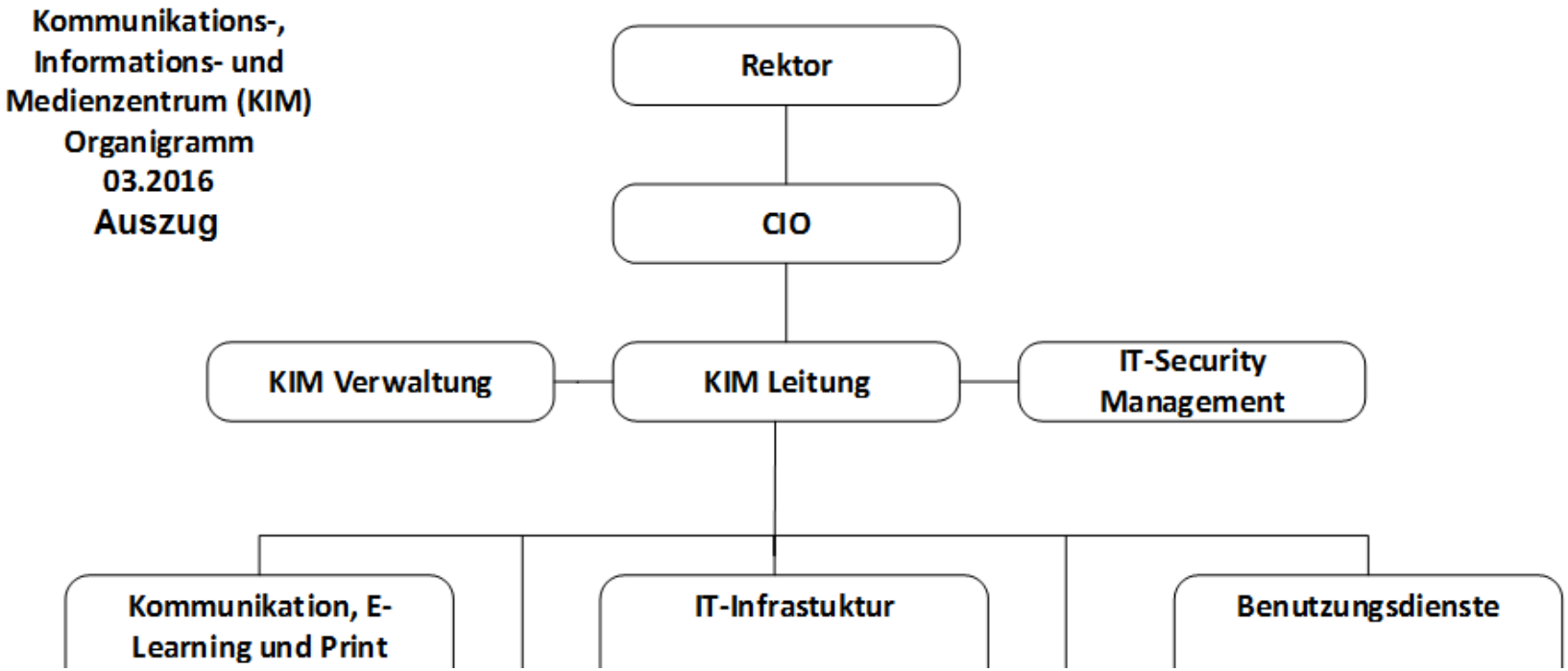
Strukturelle Modellierung eines IT-Sicherheitskonzepts

Rahmenbedingungen organisatorischer Natur

- Erteilen formeller Kompetenz durch Bestellung eines/einer IT-Sicherheitsbeauftragten.
- Die/Der IT-Sicherheitsbeauftragte besitzt, bezogen auf Informationssicherheit, die fachliche Verantwortung und Zuständigkeit für den gesamten Informationsverbund.
- Definieren und konstituieren einer IT-Sicherheitsleitlinie im Konsens mit allen beteiligten Interessengruppen.
- Konkretisierung durch IT-Sicherheitsrichtlinie(n) unter Beachtung struktureller Besonderheiten.
- Dokumentation aller Tätigkeiten und Ergebnisse in einem geeigneten Verfahren (Handbuch zur Informationssicherheit).

Strukturelle Modellierung eines IT-Sicherheitskonzepts

Rahmenbedingungen organisatorischer Natur



Strukturelle Modellierung eines IT-Sicherheitskonzepts

Normen und Vorschriften generell-abstrakter Natur

Die Einhaltung der Schutzziele zur IT-Sicherheit werden von einer Vielzahl rechtlicher Rechtliche Rahmenbedingungen und Haftungsrisiken gefordert, z. B.:

- BDSG-Neu und EU-Datenschutzgrundverordnung als grundlegende Elemente bei Umsetzung von Aktivitäten zur **Informationssicherheit** und zum **Schutz pbD** (Stichwort „Privacy by Default“ bzw. „Stand der Technik“)

- Mittelbare Drittwirkung gegenüber Studierenden

Pragmatische Umsetzung

Konzeptionelle Auditierung und abzuleitende Maßnahmen

- Anhand eines Basis-Audits den individuellen Bedarf identifizieren.
- Etablieren eines Notfallmanagementsystems
  - „Dienstvereinbarung“ zur Behandlung von Notfällen
  - Ursachen und Modelle von potentiellen Schwachstellen (Angriffen) charakterisieren.
  - Auswahl von Maßnahmen zur Behandlung von Risiken.
- Sensibilisierungsmaßnahmen
  - „IT-Sicherheit am Mittag“
  - Treffen der IT-Beauftragten
  - Individuelle Angebote und Unterstützung

Pragmatische Umsetzung

Reflexionen zu Leitlinie und Richtlinien

Die Zielsetzung von IT-Sicherheit ist es, die Reputation und das Prestige zu wahren und damit die Interessen der Universität Hohenheim zu gewährleisten.

Diesem Vorhaben – Anspruch und Bekundung zugleich – gerecht werden, neben Art und Weise der Implementation von IT-Sicherheit, Aussagen zur Verantwortung der Dienststellenleitung.

Pragmatische Umsetzung

Reflexionen zu Leitlinie und Richtlinien

Die „Leitlinie zur Informationssicherheit“ ist ein **Grundsatzdokument** zu

- Stellenwert,
- verbindlichen Prinzipien und
- anzustrebendem Niveau der Informationssicherheit

an der Universität Hohenheim.

In diesem Dokument wird **für alle Mitarbeiter verständlich** beschrieben, **welche Sicherheitsziele** angestrebt sind und in **welchem organisatorischen Rahmen** diese umgesetzt werden.

Pragmatische Umsetzung

Reflexionen zu Leitlinie und Richtlinien

- Diskussion und Verständigung über Inhalt der Leitlinie mit
  - Leitung der Universität/Einrichtung/Unternehmen;
  - Leitung, Führungsstab und Beschäftigte des KIM (Rechenzentrum);
  - Aufsichtsgremien;
  - Personalabteilung (Mitwirkung oder Mitbestimmung gem. LPVG);
  - Örtlicher Personalrat/Betriebsrat.
- Elementare Eigenschaft: Geduld.

Pragmatische Umsetzung

Reflexionen zu Leitlinie und Richtlinien

- Die IT-Sicherheitsrichtlinien bilden das operative Regelwerk für die Implementierung des IT-Sicherheitskonzepts.
- IT-Sicherheitsrichtlinien sind mit der Umsetzung von „speziellen“ Sensibilisierungs- und Schulungsmaßnahmen flankiert.
- Beispiele für IT-Sicherheitsrichtlinien:
  - Passwort-Richtlinie;
  - Serverrichtlinien;
  - IT-sicherheitsrelevante Teile eines Notfallvorsorgeplans;

Pragmatische Umsetzung

IT-Sicherheitsstandards

- Der Einsatz von Informations- und Kommunikationstechnologien ist kein Selbstzweck. Daher ist auch die Verwendung von Sicherheitsstandards mit einem quantifizierbaren Nutzen zu verbinden.

- Die Einführung und Zertifizierung eines Standards ist mit personellem und finanziellem Aufwand verbunden.

- Standards zum Informationssicherheitsmanagement gewähren einen intensiven Gestaltungsspielraum, welcher viel Erfahrung und Know-how benötigt.

Pragmatische Umsetzung

IT-Sicherheitsstandards

ISO	
ISO/IEC 27001	Anforderungen für ein Informationssicherheits-Managementsystems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation.
ISO/IEC 27002	Leitfaden zum Informationssicherheits-Management.
ISO/IEC 27005	Informationssicherheits-Risikomanagement.
ISO/IEC 27006	Definiert zusätzliche Anforderungen an Zertifizierungsstellen, die Informationssicherheits-Managementsysteme auditieren und zertifizieren.
ISO/IEC 18028 (Revision durch ISO/IEC 27033)	IT Netzwerksicherheit.
ISO/IEC TR 18044	Management von Sicherheitsvorfällen in der Informationssicherheit.
ISO/IEC 18043 (Revision durch ISO/IEC 27039)	Auswahl, Einsatz und Betrieb von Systemen zur Erkennung des Eindringens in Netze und Systeme (IDS).
ISO/IEC 15816	Sicherheitsobjekte für Zugriffskontrolle.
ISO/IEC 24762	Anforderungen an interne und externe Anbieter von „Disaster Recovery Services“ für „Information and communication technology.
BS 25777 (Revision durch ISO/IEC 27031)	Guidelines for information and communication technology readiness for business continuity management.
ISO/IEC 19792	Evaluierung biometrischer Produkte und Systeme
ISO/IEC TR 15443	Rahmenwerk zur Zusicherung der Sicherheit
ISO/IEC 27032	Information technology – Security techniques – Guidelines for cybersecurity (Schnittstelle zwischen BCM und IT-Sicherheit).
ISO/IEC 21827	Weiterentwicklung des Reifegradmodells (Capability maturity model)
Verfügbare Lektüre umfasst ca. 700 Seiten.	

Pragmatische Umsetzung

IT-Sicherheitsstandards

BSI	
BSI - IT-Grundschutzhandbuch (IT-GSHB)	IT-Grundschutzkataloge als Basis für Informationssicherheit.
BSI - Standard 100-1	Managementsysteme für Informationssicherheit.
BSI - Standard 100-2	IT-Grundschutz-Vorgehensweise.
BSI - Standard 100-3	Risikoanalyse auf der Basis von IT-Grundschutz.
BSI - Standard 100-4	Notfallmanagement.
Verfügbare Lektüre umfasst 5383 Seiten.	

Weitere anwendbare Standards	
COBIT	Kontrollziele für Informations- und verwandte Technologie.
ITIL	IT Infrastruktur Verfahrensbibliothek.
IDW PS 330/880	IDW-Standards zur Abschlussprüfung beim Einsatz von Informationstechnologie und Prüfung von Softwareprodukten.
ISO/IEC 15408 (Common Criteria)	Kriterien für die Sicherheitsevaluierung von IT-Produkten und IT-Systemen.
ISO/IEC TR 15446 (Common Criteria)	Angaben zu Sicherheitsvorgaben und Schutzprofilen gemäß ISO 15408.
ISO/IEC TR 19791 (Common Criteria)	Evaluierung von in Betrieb befindlichen IT-Systemen inklusive der organisatorischen Sicherheitsmaßnahmen gem. ISO 15408.
Sektor spezifische Standards	PKI, Digitale Signaturen, Verschlüsselung, Authentifizierung, Zeitstempeldienste, Hash-Funktionen, Payment Card Industry Data Security Standard (PCI DSS), etc.
Verfügbare Lektüre umfasst ca. 2600 Seiten.	

Pragmatische Umsetzung

IT-Sicherheitsstandards

Impedimenti	Curas auferre
Durchsetzung	Substantielle Unterstützung durch Einrichtungsleitung & Führungskräfte
Komplexität von Standards und Richtlinien	Die „lokale“ Kultur bei Planung und Umsetzung berücksichtigen
Fehlendes Bewusstsein für Bedrohungen	Maßnahmen zur Sensibilisierung (z. B. Schulungen)
Fehlende Ressourcen (Zeit, Geld, Aufwand)	Darstellen von Informations-/Wertverlust (Reputation)
Nutzen nicht quantifizierbar	Bewusstsein für IT-Sicherheit (langfristige Verbesserung von Prozessen und Systemen) etablieren
Fehlende Kenntnisse der gesetzlichen Vorgaben	Kollegialen Austausch und Unterstützung staatlicher Stellen

Pragmatische Umsetzung

IT-Sicherheitsstandards

- Die Komplexität der Geschäftsprozesse und bestehender IT-Landschaft setzt in der Regel eine Risikobetrachtung voraus. Dieser Herausforderung begegnet vor allem „ISO 2700x nach BSI“.

- An der Universität Hohenheim besteht eine Komposition aus BSI-IT-Grundschutz, ISO 2700x sowie individuellen Überlegungen.

Zusammenfassung

- Zuständigkeiten, Prozesse und Ressourcen etablieren.
- Definieren und konstituieren einer IT-Sicherheitsleitlinie im Konsens mit allen beteiligten Interessengruppen.
- Konkretisierung durch IT-Sicherheitsrichtlinie(n) unter Beachtung struktureller Besonderheiten.
- IT-Leitlinie und IT-Richtlinien implizieren IT-Sicherheitskonzept.
- Dokumentation und Öffentlichkeitsarbeit.

Haben Sie vielen Dank für Ihre Aufmerksamkeit!

Für Fragen stehe ich Ihnen gerne zur Verfügung:

Universität Hohenheim
Dr. Robert Formanek
IT-Sicherheitsbeauftragter
robert.formanek@uni-hohenheim.de