**Hinweis**: Die Seite wird im Interesse der Transparenz als Archiv vorgehalten aber nicht mehr gepflegt, da die TU Ilmenau Audatis als Datenschutzmanagementsystem einsetzt. Aktuelles zu SecDoc findet sich hier: https://zivgitlab.uni-muenster.de/secdoc/secdoc

# SecDoc

## Links

Aktuelles Testsystem der WWU https://www.uni-muenster.de/ZIVtest/secdoc-demo/

Gitlab https://zivgitlab.uni-muenster.de/wwu-cert/secdoc

Testsystem der TU Ilmenau https://dsdoku.tu-ilmenau.de

## 7.2.2019 Treffen DFN-CERT

### Ziel

- Ausfüllen im Browser, geschützter Zugriff von überall
- Automatisches Speichern
- Datenvorschläge
- Integrierte Hilfe
- PDF-Erzeugung
- HTML-Schnipsel Erzeugung zur Verwendung in Datenschutzerklärung (Informationspflichten, Art. 13/14 DSGVO)
- Strukturierte Ablage in Datenbank

### Bekannte Probleme

- Organisationsstruktur fehlt
- kein DSMS
- Verantwortlichkeiten nicht klar geregelt/Nutzung des Tools nur aus eigenem Antrieb
- Schulungen nötig
- Status derzeit nur „Bearbeitung“ oder „Fertig“ möglich, z.B. Freigabe durch DSB fehlt noch

### Technische Realisierung

- Single Page Web Application
    - Umsetzung mit HTML5, CSS, JavaScript, PHP, SQLite

    - Bootstrap3 (Twitter)
    - responsives Design
- Datenübernahme (auch Strukturdaten) von Identity Management möglich

### geplante Erweiterungen

- Mehr Flexibilität bei Verantwortlichen, evtl. auch Differenzierung fachlicher Ansprechpartner und zuständige Führungskraft
- Mehr Dropdown-Auswahlmöglichkeiten (Wo sind Gemeinsamkeiten?)
- Wiedervorlagen
- Checklisten für TOM´s (perspektivisch Einbindung Grundschutzkataloge)
- Dashboard

### Meine Themen

- Dokumenteneinbindung
    - Datenschutzerklärung, (grundsätzlich sind Verlinkungen möglich)
    - AVV (grundsätzlich sind Verlinkungen möglich)
- Verknüpfung zu
    - Spider (grundsätzlich sind Verlinkungen möglich)
    - Dokuwiki (grundsätzlich sind Verlinkungen möglich)
- Mandantenfähigkeit –> derzeit eher nicht, teilweise über freie Auslegung von innerorganisatorisch Verantwortlichen umgesetzt
- Archiv: Schnittsstelle, Abfrage möglich

## 25.04.2019 Workshop WWU Münster

### Begrüßung, Vorstellungsrunde

- BaWü: Landesgesetzgeber schreibt IT-Sicherheitsmanagementsystem zukünftig verbindlich vor.
- iSeed gescheitert
- WWU: Allein im Dezernat Personal 25 bis 30 Verarbeitungstätigkeiten

### Kurzvorstellung SecDoc, Ziele, Wünsche

- (zukünftige) Erleichterungen durch
    - Vorgabe hochschulspezifischer Verarbeitungstätigkeiten auf der Basis von Prozesslandkarten
    - Vordefinierte TOM auf Basis ENISA
    - Vorauswahl Kategorien von betroffenen Personen
    - Versionierung möglich
    - Einbindung von URL mittlerweile möglich (noch nicht in dsdoku übernommen)
    - fertiges VVT kann mittlerweile auch als Webseite eingebunden werden
    - Risikobewertung/Schutzbedarfsfeststellung als einfache Angabe normal-hoch-sehr hoch und ggf. URL zu einem geeigneten Tool unproblematisch, Ausbau später denkbar
- weitere Entwicklung

    - Integration von Risikoanalysen
    - Vorgabe TOM auf Basis Risikoanalysen
    - Einführung/Umsetzung offener Datenschnittstellen
    - Gemeinsamer Zugang für die Informationssicherheit und den Datenschutz
    - Auswertungsmöglichkeiten schaffen
    - Templates
    - CVE-Matching: Problem Aktualisierung und Ermittlung
    - Share-Button als Workflow-Unterstützung bzw. Ticket-System
    - Review-Prozess
- Zugriff auf Daten:
    - per Script auf SQL-Lite Datenbank oder PHP-AD Schnittstelle (AD-Connector)
    - Einbindung mehrerer Quellen denkbar
    - Datenformat für TOM-Katalog definieren
- Erfahrungsberichte etc.
    - Installation erfordert nicht nur Konfigurierung sondern Programmierung
    - LDAP-Schnitte –> können wir Source-Code zur Verfügung stellen? –> Jörg
- Organisatorische Fragen
    - (halb-)offenes GitLab kommt, ggf. von anderer Hochschule (notfalls auch TU?)
    - Glossar

## Standardisierung von TOM

Standardisierung von TOM dringend notwendig aber von den Aufsichtsbehörden eher wenig konkretes.

ENISA hat von seit 2016 Dokumente mit Sicherheitsmaßnahmen zum Schutz personenbezogener Daten erstellt und zwar nach einem risikobasierten Ansatz.

- Guidelines for SMEs on the security of personal data processing
- https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing
- Reinforcing trust and security in the area of electronic communications and online services

Der Ansatz der ENISA ist eng mit ISO 27001 verknüpft; auf Basis BSI-Grundschutz sähe die Liste aber ganz ähnlich aus.

### Tätigkeitsbereiche

Tätigkeitsbereiche nach Guidelines for SMEs on the security of personal data processing im Überblick:

- Organisatorische Sicherheitsmaßnahmen
    - Erfahrungen: Bündel von 20-25 Maßnahmen, erster Zugriff mit ggf. 5 Maßnahmen (Rechte und Rollen, Schulung etc.)
- Technische Sicherheitsmaßnahmen

### Umsetzungshilfen

Zur praktischen Umsetzung von TOM (als Unterlegung des ENISA Ansatzes): Handreichung zum "Stand der Technik" technischer und organisatorischer Maßnahmen

Alternativ könnte auch BSI hilfreich sein.

#### Weiteres Vorgehen

Münster macht einen Vorschlag für Datenformat und Inhalte.

## Verarbeitungstätigkeit

- Template und Prototypen mit Import-/Exportfunktion
- Austauschplattform

## Sonstiges

- Lizenz –> Soll frei bleiben
- Projektanträge ggf. in anderen Ländern –> Thüringen?; notfalls Fork
- weiterer zeitlicher Ablauf - wann Version, deren Datenbank aufwärtskompatibel ist –> ist der Fall, da in Münster im Produktivbetrieb, ggf. werden Skripte an der WWU entwickelt für Übergang

Archiv, 2022