SEC4YOU

Advanced IT-Audit Services

PUBLIC TLP:CLEAR

Webinar

Klassifizierung von Informationen nach ISO 27001 — schnelle Umsetzung

20. Juni 2024 / V1.0

Ing. Andreas Schuster, SEC4YOU
DI. Bianca Danczul, M.Sc., SEC4YOU

Agenda

- Anforderungen bezüglich Informationsklassifizierung aus ISO 27001:2022, TISAX®, NIS-2 und DORA
- Das klassische Klassifizierungsschema: ÖFFENTLICH / INTERN / VERTRAULICH / STRENG VERTRAULICH
- Das SEC4YOU Klassifizierungsschema in Piktogrammen
- Praktische Tipps für die Kennzeichnung von klassifizierten Informationen

SEC4YOU

Advanced IT-Audit Services

Anforderungen bezüglich Informationsklassifizierung aus ISO 27001:2022, TISAX®, NIS-2 und DORA

Vortragender: Andreas

Drei Maßnahmen in ISO 27001:2022, Anhang A

- A5.12: Informationen sollten entsprechend den Anforderungen der Organisation an die Informationssicherheit klassifiziert werden, und zwar auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien.
- A5.13: In Übereinstimmung mit dem von der Organisation angenommenen Informationsklassifizierungsschema sollten geeignete Verfahren zur Kennzeichnung von Informationen entwickelt und umgesetzt werden.
- A5.10: Es sollten Regeln für die zulässige Nutzung und Verfahren für den Umgang mit Informationen und anderen zugehörigen Vermögenswerten festgelegt, dokumentiert und umgesetzt werden.

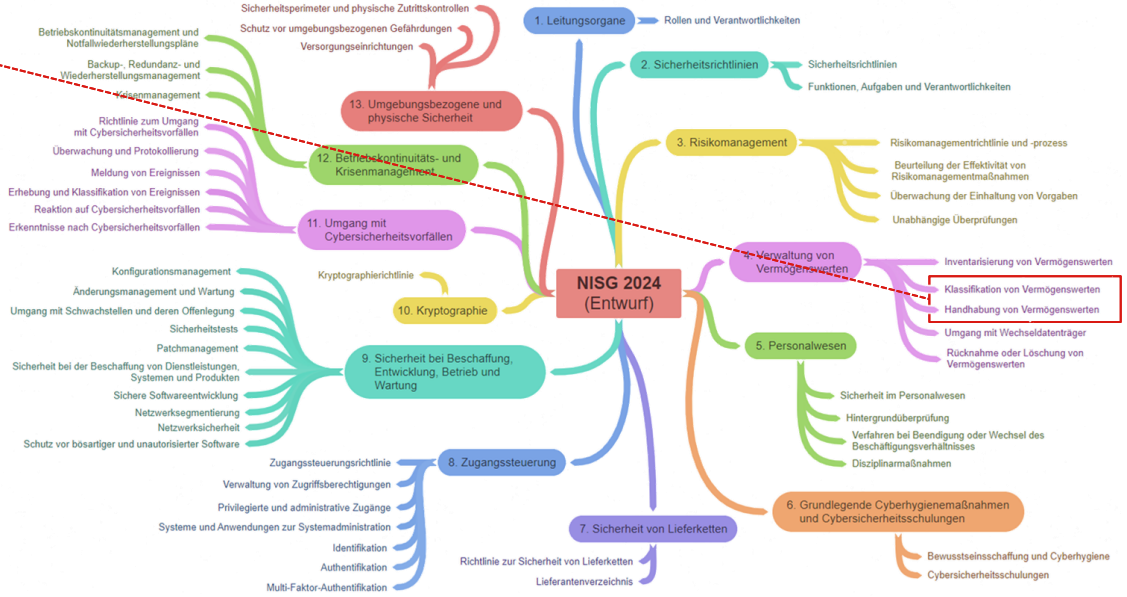
A5.1 InfoSec-Richtlinien	A5.2 InfoSec Verantwortlichkeiten	A5.3 Aufgaben-trennung	A5.4 Verantwortung der Leitung	A5.5 Kontakt mit Behörden	A5.6 Kontakt mit Interessensgruppen	A5.7 Informationen zur Bedrohungslage	A5.8 InfoSec im Projektmanagement	A5.9 Inventar der Informationen / Assets	A5.10 Zulässiger Gebrauch von Assets
A5.11 Rückgabe von Werten	A5.12 Klassifizierung von Informationen	A5.13 Kennzeichnung von Informationen	A5.14 Informations-übermittlung	A5.15 Zugangs-steuerung	A5.16 Identitäts-management	A5.17Authentisierungs-informationen	A5.18 Zugangsrechte	A5.19 InfoSec bei Lieferanten	A5.20 Lieferanten-vereinbarungen
A5.21 InfoSec in der Lieferkette	A5.22 Überwachung Lieferantenleistungen	A5.23 InfoSec bei Cloud-Diensten	A5.24 Management Sicherheitsvorfälle	A5.25 Bewertung Sicherheitsereignisse	A5.26 Reaktion auf Sicherheitsvorfälle	A5.27 Erkenntnisse aus Sicherheitsvorfällen	A5.28 Sammeln von Beweismaterial	A5.29 InfoSec bei Störungen	A5.30 Geschäfts-Kontinuität
A5.31 Compliance	A5.32 Geistiges Eigentum	A5.33 Schutz von Aufzeichnungen	A5.34 DSGVO - Datenschutz	A5.35 Überprüfung d. Informationssicherheit	A5.36 Einhaltung von Richtlinien	A5.37 Dokumentierte Betriebsabläufe			
A6.1 Bewerber Sicherheitsüberprüfung	A6.2 InfoSec in Arbeitsverträgen	A6.3 Security Awareness	A6.4 Maßregelungs-prozess	A6.5 Beendigung von Beschäftigung	A6.6 Vertraulichkeits-Vereinbarungen	A6.7 Remote-Arbeit	A6.8 Meldung von InfoSec Ereignissen		
A7.1 Physischer Sicherheitsperimeter	A7.2 Physischer Zutritt	A7.3 Sichern von Standorten	A7.4 Phys. Sicherheits-überwachung	A7.5 Schutz vor Umweltbedrohungen	A7.6 Arbeiten in Sicherheitsbereichen	A7.7 Arbeitsplatz-sicherheit (Sperre)	A7.8 Schutz von Geräten/Betriebsmittel	A7.9 Werte außerhalb der Räumlichkeiten	A7.10 Speichermedien
A7.11 Versorgungs-einrichtungen	A7.12 Sicherheit der Verkabelung	A7.13 Instandhaltung von Geräten	A7.14 Sichere Entsorgung						
A8.1 Benutzer Endgeräte	A8.2 Privilegierte Zugangsrechte	A8.3 Informations-zugangsbeschränkung	A8.4 Zugriff auf den Quellcode	A8.5 Sichere Authentisierung	A8.6 Kapazitäts-steuerung	A8.7 Schutz gegen Schadsoftware	A8.8 Technische Schwachstellen	A8.9 Konfigurations-management	A8.10 Löschung von Informationen
A8.11 Daten-maskierung	A8.12 Verhinderung von Datenlecks (DLP)	A8.13 Sicherung von Informationen	A8.14 Redundanzen	A8.15 Protokollierung	A8.16 Überwachung von Aktivitäten	A8.17 Uhren-synchronisation	A8.18 Privilegierte Hilfsprogramme	A8.19 Installation von Software	A8.20 Netzwerk-sicherheit
A8.21 Sicherheit von Netzdiensten	A8.22 Trennung von Netzwerken	A8.23 Webfilterung	A8.24 Verwendung von Kryptographie	A8.25 Lebenszyklus sicherer Entwicklung	A8.26 Anforderung an Anwendungssicherheit	A8.27 Sichere Ent-wicklungsgrundsätze	A8.28 Sichere Codierung	A8.29 Sicherheit-prüfung b. Entwicklung	A8.30 Ausgegliederte Entwicklung
A8.31 Trennung von Entwicklung/Test/Prod.	A8.32 Änderungs-steuerung	A8.33 Testdaten	A8.34 Schutz der IT während Tests						

TISAX® Zertifizierung nach ISA 6

- Asset Management Control 1.3.2: + A consistent scheme for the classification of information assets regarding the protection goal of confidentiality is available.
  - **What protection levels are defined** in the company and what criteria are used to classify them?
  - **What measures are defined for each protection level**?
  - How can the classification of the information be recognized by employees?
  - How is information classified?
  - What regulations are derived for the protection of information (storage media/documents)?
  - How do employees know how to classify information?
  - What are the tools for classifying the classification?
  - **How are information objects labelled**?
  - Who is responsible for classifying the classification?
  - **How are unmarked documents handled**?

NIS2 → NISG 2024 (Entwurf) in Anlage 3

- Zwei Controls unter
  4. Verwaltung von Vermögenswerten



Digital Operational Resilience Act (DORA), EU Verordnung 2022/2554

- Art. 8 Identifizierung: (4) Finanzunternehmen ermitteln alle Informations- und IKT-Assets, einschließlich derer an externen Standorten, Netzwerkressourcen und Hardware, und erfassen diejenigen, die als kritisch gelten. Sie erfassen die Konfiguration von Informations- und IKT-Assets sowie die Verbindungen und Interdependenzen zwischen den verschiedenen Informations- und IKT-Assets.
- Eine direkte Referenz auf Informationsklassifizierung und Kennzeichnung/Labeling findet sich in DORA nicht.

SEC4YOU

Advanced IT-Audit Services

Das klassische Klassifizierungsschema: ÖFFENTLICH / INTERN / VERTRAULICH / STRENG VERTRAULICH

Vortragender: Andreas

Das klassische Schema

- 4 Schutzklassen: ÖFFENTLICH / INTERN / VERTRAULICH / STRENG VERTRAULICH
- Oft mit farbiger Markierung GRÜN, BLAU, ORANGE, ROT

Öffentlich	Intern	Vertraulich	Streng Vertraulich
Daten sind für jedermann, auch außerhalb der Firma, zugänglich.	Interne Daten werden lediglich den eigenen Mitarbeitern zugänglich gemacht.	Vertraulich definierte Daten sind lediglich einer begrenzten Anzahl an Mitarbeitern zugänglich, z.B. Personaldaten, Kundenlisten, Kalkulationen.	Streng vertrauliche Daten sind punktuell und ausschließlich bestimmten definierten Personen zugänglich. Eine Weitergabe kann das Unternehmen nachhaltig schädigen.

Die Schwächen…

1. **MitarbeiterInnen** sind mit der Kennzeichnung aller Dokumente **überfordert**, bei einem Audit finden AuditorInnen tonnenweise ungekennzeichnete „Interne“ Informationen.
2. MitarbeiterInnen **verstehen den Unterschied** zwischen „Öffentlich“ und „Intern“ **nicht**.
3. Durch die **Kennzeichnung “Intern”** wird signalisiert, dass eine Information dieser Schutzklasse **nur innerhalb des Unternehmens** ausgetauscht werden darf, was nicht stimmt.
4. Besonders fleißige MitarbeiterInnen erkennen in Ihren Arbeitsdokumenten schnell „Vertrauliche“ oder sogar „Streng Vertrauliche“ Informationen und verursachen so **hohen Aufwand** und **hohe Kosten** beim Informationshandling.

	Schutzklasse (Klassifizierung)			
	ÖFFENTLICH	INTERN	VERTRAULICH	STRENG VERTRAULICH
Zulässige Verwendung		TISAX „normal“	TISAX „hoch“	TISAX „sehr hoch“
Kennzeichnung		-		

SEC4YOU

Advanced IT-Audit Services

Das SEC4YOU Klassifizierungsschema in Piktogrammen

Vortragender: Andreas

Die SEC4YOU Empfehlung für A5.11

- 4-stufiges Klassifizierungsschema mit PUBLIC / RESTRICTED / CONFIDENTIAL / STRICTLY CONFIDENTIAL bzw. ÖFFENTLICH / EINGESCHRÄNKT / VERTRAULICH / STRENG VERTRAULICH
- Verzicht auf „INTERN“
- Nutzung von Traffic Light Protocol – TLP 2.0

	Schutzklasse (Klassifizierung)			
Zulässige	PUBLIC	RESTRICTED	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Verwendung		TISAX „normal“	TISAX „hoch“	TISAX „sehr hoch“
Kennzeichnung	PUBLIC TLP:CLEAR	RESTRICTED TLP:AMBER	CONFIDENTIAL TLP:AMBER+STRICT	STRICTLY CONFIDENTIAL TLP:RED
Speicherung				

Zulässiger Gebrauch von Assets (ISO 27001:2022 A5.10)

Regeln Sie zumindest die folgenden Handhabungsmethoden pro Schutzklasse:

1. Kennzeichnung
2. Speicherung
3. Speicherung in der Cloud
4. Nutzung von mobilen Geräten und Datenträgern
5. Emailnutzung
6. Weitergabe intern und an Dritte
7. Physischer Versand
8. Informations- bzw. Datenvernichtung

Einfache Kommunikation über Piktogramme

- Die Piktogramme sind kostenfrei auf unsere Webseite verfügbar
- Das Auge steht für überwachter bzw. ausgewählter Dienst
- Der Gebrauch regelt sowohl elektronische als auch physische Dokumente (Ausdrucke)

	Schutzklasse (Klassifizierung)			
Zulässige Verwendung	PUBLIC	RESTRICTED	CONFIDENTIAL	STRICTLY CONFIDENTIAL
		TISAX „normal“	TISAX „hoch“	TISAX „sehr hoch“
Kennzeichnung	PUBLIC TLP:CLEAR	RESTRICTED TLP:AMBER	CONFIDENTIAL TLP:AMBER+STRICT	STRICTLY CONFIDENTIAL TLP:RED
Speicherung	✓			
Verarbeitung in der Cloud	✓			
Mobile Datenträger	✓			
E-Mail	✓			
Weitergabe (Extern)	✓	NDA	NDA	NDA NDA
Weitergabe (intern)	✓	✓		
Versand / Transport	✓			
Entsorgung	✓			
Vernichtung	✓			

Verzicht auf Kennzeichnung von „RESTRICTED“

- Beschreiben Sie in Ihrer Richtlinie, dass Informationen der Schutzklasse “RESTRICTED” - entspricht TISAX „normal“ - keine Kennzeichnung benötigen.
  Dies ist auch eine Handlungsempfehlung der Norm ISO 27002:2022 Absatz 5.13.

	Schutzklasse (Klassifizierung)			
Zulässige	PUBLIC	RESTRICTED	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Verwendung		TISAX „normal“	TISAX „hoch“	TISAX „sehr hoch“
Kennzeichnung	PUBLIC TLP:CLEAR	OPTIONAL	CONFIDENTIAL TLP:AMBER+STRICT	STRICTLY CONFIDENTIAL TLP:RED
Speicherung				

SEC4YOU

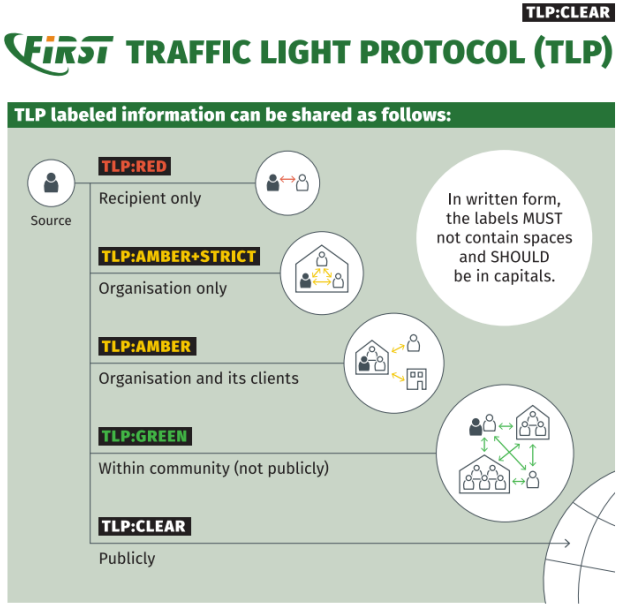
Advanced IT-Audit Services

Praktische Tipps für die Kennzeichnung von klassifizierten Informationen

Vortragende: Bianca

Kennzeichnung von klassifizierten Informationen (ISO 27001:2022 A5.12)

- Durch die Nutzung von TLP 2.0 können Informationen sowohl am Speicherort als auch bei der Übermittlung gekennzeichnet werden.
- Von den 5 Stufen eignet sich jedoch **TLP:GREEN** nicht für unser 4-stufiges Klassifizierungsschema



PUBLIC **TLP:CLEAR**

- Diese Informationen sind öffentlich und können ohne Einschränkungen frei zugänglich gemacht sowie weitergegeben werden.
- Es gibt keine Beschränkung hinsichtlich des Zugriffes oder der Verbreitung dieser Informationen.

	Schutzklasse (Klassifizierung)			
Zulässige Verwendung	PUBLIC	RESTRICTED	CONFIDENTIAL	STRICTLY CONFIDENTIAL
		TISAX „normal“	TISAX „hoch“	TISAX „sehr hoch“
Kennzeichnung	PUBLIC TLP:CLEAR	RESTRICTED TLP:AMBER	CONFIDENTIAL TLP:AMBER+STRICT	STRICTLY CONFIDENTIAL TLP:RED
Speicherung	✓			
Verarbeitung in der Cloud	✓			
Mobile Datenträger	✓			
E-Mail	✓			
Weitergabe (Extern)	✓			
Weitergabe (intern)	✓			
Versand / Transport	✓			
Entsorgung	✓			
Vernichtung	✓			

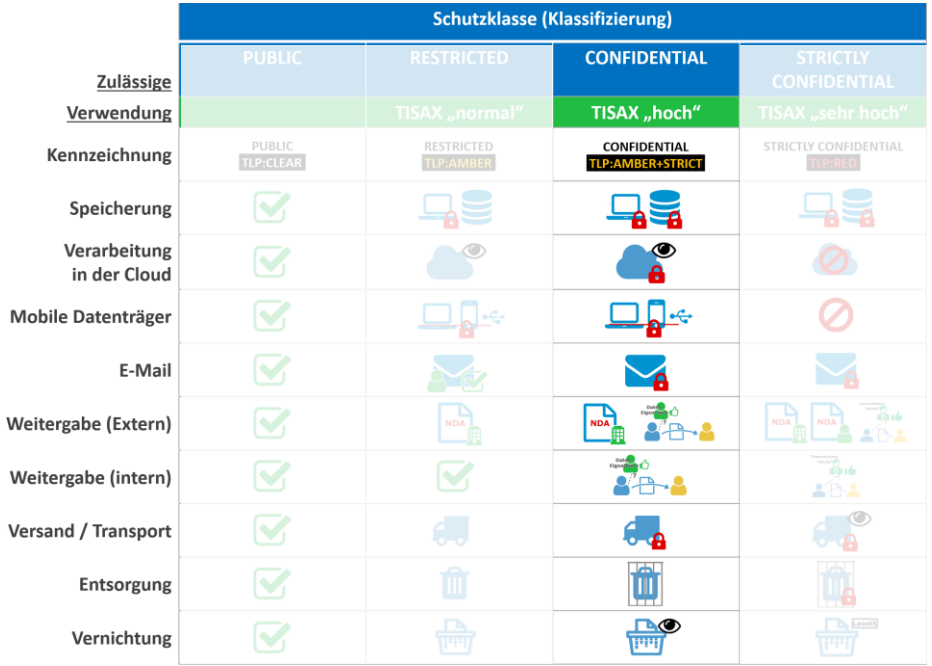
RESTRICTED TLP:AMBER

- Diese Informationen sind für den eingeschränkten organisations-übergreifenden und internen Gebrauch bestimmt.
- EmpfängerInnen dürfen diese Informationen nur an autorisierte Personen in ihrer eigenen Organisation sowie bedarfs-orientiert an GeschäftspartnerInnen weitergeben.

	Schutzklasse (Klassifizierung)			
	PUBLIC	RESTRICTED	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Zulässige Verwendung		TISAX „normal“	TISAX „hoch“	TISAX „sehr hoch“
Kennzeichnung	PUBLIC TLP:CLEAR	RESTRICTED TLP:AMBER	CONFIDENTIAL TLP:AMBER+STRICT	STRICTLY CONFIDENTIAL TLP:RED
Speicherung	✓			
Verarbeitung in der Cloud	✓			
Mobile Datenträger	✓			
E-Mail	✓			
Weitergabe (Extern)	✓			
Weitergabe (intern)	✓			
Versand / Transport	✓			
Entsorgung	✓			
Vernichtung	✓			

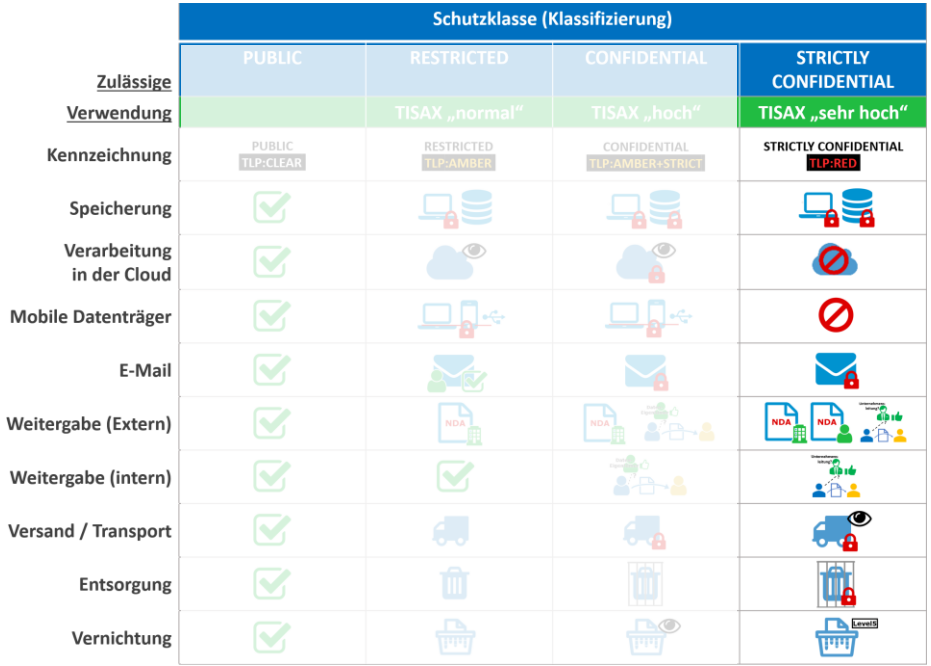
CONFIDENTIAL **TLP:AMBER+STRICT**

- Diese Informationen sind vertraulich und bedürfen eines besonderen Schutzes.
- EmpfängerInnen dürfen diese Informationen nur an legitimierte Personen weitergeben.
- Eine Offenlegung der Informationen außerhalb des definierten EmpfängerInnenkreises bedarf einer dedizierten Freigabe durch InformationseignerInnen.



STRICTLY CONFIDENTIAL TLP:RED

- Die Informationen sind äußerst sensibel.
- EmpfängerInnen dürfen diese Informationen nur an autorisierte Personen nach schriftlicher Freigabe durch ein Mitglied der Unternehmensleitung weitergeben.
- Jegliche Verbreitung außerhalb des festgelegten Personenkreises ist strengstens untersagt.



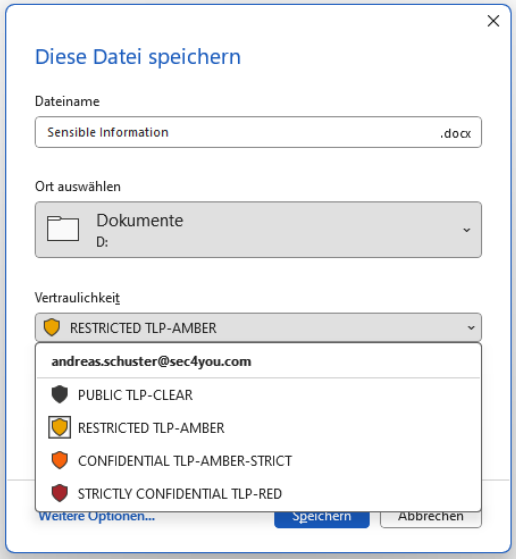
Empfehlungen bei der Kennzeichnung von Informationen

- Etablierung spezieller **gekennzeichneter Bereiche** im Netzwerk mit strikter Benutzer-einschränkung für klassifizierte Informationen, z.B. Share für Finanzdaten, Share für HR, etc.
- **Word, Excel und PowerPoint Vorlagen** für vertrauliche und streng vertrauliche Dokumente (bzw. „hoch“ und „sehr hoch“) auf der die Klassifizierung auf jeder Dokumentenseite deutlich sichtbar ist.
- Bei der Klasse „streng vertraulich“ bzw. BSI „sehr hoch“ müssen die erlaubten EmpfängerInnen am Anfang des Dokumentes aufgelistet sein.
- **Schulen Sie** Ihre MitarbeiterInnen bezüglich der Erstellung von vertraulichen Dokumenten.

Microsoft Sensitivity Labels

- Nutzung von Microsoft 365 Labels für die einfache Kennzeichnung von Microsoft Office Dokumenten
  → *Achtung: Labels sind nur im eigenen Unternehmen sichtbar, nicht extern!*

- *https://learn.microsoft.com/en-us/purview/sensitivity-labels*



Fragen gerne per E-Mail oder LinkedIn an die Vortragenden

Bianca.Danczul@sec4you.com
https://sec4you.com
Tel.: +43 1 2531 797-0

Andreas.Schuster@sec4you.com
https://sec4you.com
Tel.: +43 678 1216943