Sehr geehrte Damen und Herren,

Sie bekommen eine Aufgabenstellung als PDF-Datei, aber ***keine Word-Dateien als Vorlage*** für die Abgabe - Formvorschriften beachten!

ACHTUNG:

- **Sie müssen 2 Word-Dateien abgeben, die die Dokumentlenkung berücksichtigt:**
    - **Leitlinie 4A - Anforderungen für die sichere Verwendung eines CLOUD-Services in der „SPENGER-KLINIK“**
    - **Leitlinie 4U - Umsetzungshinweise für die sichere Verwendung eines CLOUD-Services in der „SPENGER-KLINIK“, die in Leitlinie 4A beschrieben ist.**

Wie Sie erkennen können, bestehen die Leitlinien immer aus der <fortlaufenden Nummer> und dem Buchstaben <A> oder <U>.

<A> = Anforderung: Eine Leitlinie-Anforderung ist einzuhalten, um ein Mindestmaß an Informationssicherheit beim Nutzen zu gewährleisten. Eine Leitlinie richtet sich hinsichtlich der Umsetzung der Anforderung an IKT-Verantwortliche, IKT-Sicherheitsbeauftragte (CISO) und IKT-Betriebspersonal sowie mit der IKT-Beschaffung beauftragte Stellen. Andere interessierte Personen können zur Erhöhung der Informationssicherheit eingebunden werden.

<U> = Umsetzung: Eine Leitlinie-Umsetzung unterstützt IKT-Verantwortliche, IKT-Sicherheitsbeauftragte (CISO) und IKT-Betriebspersonal sowie mit der IKT-Beschaffung beauftragte Stellen bei der Interpretation und der Umsetzung des Mindestmaßes an Informationssicherheit.

ACHTUNG:

1. Lesen Sie die Aufgabenstellung genau durch!
2. Bitte, beantworten Sie die Aufgabenstellung so genau wie möglich und gehen Sie nicht davon aus, dass ich Ihre Überlegungen erraten kann.

DIE ABGABE IST NUR BIS 15:10 AM 20.01.2020 MÖGLICH!

Viel Glück!

Notenschlüssel:

1: 100,0% - 87,6%
2: 87,5% - 75,1%
3: 75,0% - 62,6%
4: 62,5% - 50,1%
5: 50,0% - 0%

1. Ausgangssituation

Die Firma „**MED-CLOUD-SYSTEM**“ hat von der Geschäftsführung der „SPENGER-KLINIK“ den Auftrag erhalten, eine Leitlinie für die Anforderungen der sicheren Verwendung eines externen CLOUD-Services und eine Leitlinie mit Umsetzungshinweise für diese Anforderungen zu schreiben.

2. Aufgabenstellung

Als Hilfsmittel sind alle im MIS-Unterricht verwendeten Unterlagen zulässig.

2.1 Erstellen der Leitlinie 4A (50 Punkte):

Die Leitlinie 4A beschreibt die Anforderungen für die sichere Verwendung eines CLOUD-Services in der „SPENGER-KLINIK“

Die Leitlinie besteht aus:

Aufbau der Leitlinie	**Was sollen Sie beschreiben:** (z.B.: Anforderung = An)		**Ihre Aufgabe**
1. Präamble	Das Ziel der Leitlinie ist ...		beschreiben
2. Sicherheitsanforderungen	Welche Datenklassen gibt es und welches Risiko ergibt sich durch die Nutzung.		beschreiben
3. Anforderung bei der Beschaffung des Cloud-Services (Vertrag)	A1	Systembeschreibung des Anbieters ...	beschreiben **4** dieser Anforder-ungen
	A2	Zertifizierungen des Anbieters ...	
	A3	Sicherheitsnachweise des Anbieters ...	
	A4	Zusätzliche Anforderungen an den Anbieter ...	
	A5	Rechte auf Prüfung des Anbieters ...	
	A6	Umgang mit Unterauftrag-nehmern des Anbieters ...	
	A7	Umgang mit Verpflichtungen (Offenlegung) gegen Sicherheitsbehörden des Anbieters ...	
	A8	Beendigung des Vertrags-verhältnisses regeln	
4. Anforderungen beim Betrieb des Cloud-Services	A9	ISMS Anforderungen mit dem Anbieter ...	
	A10	Sicherheitsüberprüfung mit dem Anbieter ...	

5. Anforderungen beim Beendigen des Cloud-Services	A11	ISMS Datenrückgabe mit dem Anbieter ...	
	A12	ISMS Datenlöschung mit dem Anbieter ...	

2.2 Beispiel für die Leitlinie 4A - Anfang:

Vorwort

Die Leitlinie 4A *„Anforderungen für die sichere Verwendung eines CLOUD-Services in der SPENGER-KLINIK“* definiert die Sicherheitsanforderungen an die Nutzung eines solchen Services.

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IKT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.

Externe Cloud-Dienste im Sinne dieser Leitlinie sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netzwerke und Anbieter der Wirtschaft außerhalb der Spenger-Klinik erbracht werden.

Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Beschaffungs-, die Einsatz- sowie die Beendigungsphase von externen Cloud-Diensten. Diese sind einzuhalten, um ein Mindestmaß an Informationssicherheit zu gewährleisten. Sie können jedoch bei Bedarf durch zusätzliche Anforderungen erweitert werden. Vor der Nutzung externer Cloud-Dienste ist zusätzlich zur Schutzbedarfsfeststellung eine vorgelagerte Datenkategorisierung und Risikoanalyse durchzuführen.

Im Rahmen der Datenkategorisierung der Vertraulichkeit sind die Daten den nachfolgenden Klassen zuzuordnen:

Öffentlich ... (ergänzen),

Vertraulich ... (ergänzen),

Geheim ... (ergänzen)

hier **ergänzen Sie 4 Anforderungen** von A1 – A12

2.3 Erstellen der Leitlinie 4U (50 Punkte):

Die Leitlinie 4U beschreibt die Umsetzungshinweise für die sichere Verwendung eines CLOUD-Services in der „SPENGER-KLINIK“ und referenziert auf die gleiche Nummer der Anforderung

Die Leitlinie besteht aus:

Aufbau der Leitlinie	**Was sollen Sie beschreiben:** (z.B.: Umsetzungshinweis = Un)		**Ihre Aufgabe**
1. Präamble	Das Ziel der Leitlinie ist ...		beschreiben
2. Umsetzungshinweise für die Sicherheitsanforderungen	Umsetzungshinweise welche Datenklassen es gibt und welches Risiko sich durch die Nutzung in der Cloud ergeben kann.		beschreiben
3. Umsetzungshinweis für die Anforderung bei der Beschaffung des Cloud-Services (Vertrag)	U1	Umsetzungshinweise für die Systembeschreibung des Anbieters ...	beschreiben **4** dieser Umsetzungshinweise für die Anforderungen
	U2	Umsetzungshinweise für die Zertifizierungen des Anbieters ...	
	U3	Umsetzungshinweise für die Sicherheitsnachweise des Anbieters ...	
	U4	Umsetzungshinweise für die Zusätzliche Anforderungen an den Anbieter ...	
	U5	Umsetzungshinweise für die Rechte auf Prüfung des Anbieters ...	
	U6	Umsetzungshinweise für den Umgang mit Unterauftragnehmern des Anbieters ...	
	U7	Umsetzungshinweise für den Umgang mit Verpflichtungen gegen Sicherheitsbehörden des Anbieters ...	
	U8	Umsetzungshinweise für die Beendigung des Vertragsverhältnisses regeln	
4. Umsetzungshinweis für die Anforderungen beim Betrieb des Cloud-Services	U9	Umsetzungshinweise für die ISMS Anforderungen mit dem Anbieter ...	
	U10	Umsetzungshinweise für die Sicherheitsüberprüfung mit dem Anbieter ...	

5. Umsetzungshinweise für die Anforderungen beim Beendigen des Cloud-Services	U11	Umsetzungshinweise für die Datenrückgabe mit dem Anbieter ...	
	U12	Umsetzungshinweise für die Datenlöschung mit dem Anbieter ...	

2.4 Beispiel für die Leitlinie 4U - Anfang:

Vorwort

Die Leitlinie 4U *„Umsetzungshinweise für die sichere Verwendung eines CLOUD-Services in der SPENGER-KLINIK“* helfen die Sicherheitsanforderungen der Leitlinie 4A anzuwenden.

Die Leitlinie A4 führt einen Prozess ein, mit dem sich Risiken der externen Cloud-Nutzung identifizieren, bewerten und behandeln lassen. Damit bleiben diese für Spenger-Klinik als Cloud-Kunde beherrschbar. Hierfür werden die Phasen Beschaffung, Einsatz und Beendigung von externen Cloud-Diensten betrachtet. Für jede Phase werden entsprechende Sicherheitsanforderungen zur Gewährleistung der Informationssicherheit aufgestellt.

Die Sicherheitsanforderungen sind bereits in existierenden Standards, Normen und Regelungen als relevant identifiziert worden und sind daher den Cloud-Anbietern bereits bekannt. Eine ganz zentrale Bedeutung bei der Bewertung von externen Cloud-Diensten nimmt der, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene, Anforderungskatalog Cloud Computing (BSI C5) ein.

Die Leitlinie A4 greift die Themenkomplexe Informationssicherheit, Transparenz der Cloud-Diensterbringung und Nachweis über diese Aspekte durch geeignete Prüfungen auf. Rahmenbedingungen für die Cloud-Diensterbringung werden konkretisiert. Zudem wird vorgegeben, wie die Prüfnachweise des Cloud-Anbieters für das Informationssicherheitsmanagement der Spenger-Klinik genutzt werden sollen.

Umsetzungshinweise für die Sicherheitsanforderungen

Die Sicherheitsanforderungen teilen sich auf die Beschaffungs-, die Einsatz- sowie die Beendigungsphase von externen Cloud-Diensten auf.

A1 - Systembeschreibung und weitergehende Informationen fordern

„Die Vorlage der Systembeschreibung des Cloud-Dienstes muss in der Leistungsbeschreibung gefordert werden. Sie muss die Vorgaben nach BSI-C5 erfüllen und ist insbesondere auf Mitwirkungspflichten (1) und Maßnahmen hin zu prüfen. Zur Beurteilung des Cloud-Anbieters können weitergehende Informationen im Rahmen der Leistungsbeschreibung gefordert werden. Zudem sind mit Hilfe der Leistungsbeschreibung Basis- und Zusatzleistungen festzulegen.“

Zu (1): Mitwirkungspflichten bei Informationssicherheitsproblemen nehmen bei Cloud-Diensten eine wichtige Rolle ein. Die Anforderung soll daher entsprechend sensibilisieren und im Vertrag festgelegt werden.

hier **ergänzen Sie 4 Umsetzungshinweise** von U2 – U12

3. Wichtige Ausarbeitungshinweise

Sollte es sich im Rahmen der Ausarbeitungen als notwendig erweisen, dass Sie Annahmen treffen müssen, so versehen Sie diese Annahmen eindeutig mit entsprechenden Hinweisen sowie klaren und nachvollziehbaren Begründungen. Diese Annahmen dürfen nicht im Widerspruch zu den Angaben stehen; nicht dokumentierte oder nicht nachvollziehbare Annahmen können nicht in die Bewertung miteinbezogen werden.

Bitte beachten Sie, dass in der schriftlichen Ausarbeitung folgende Kriterien zur Beurteilung Ihrer Leistung herangezogen werden: Umsetzung von Methoden, Techniken und Vorgehensweisen, sowie grafische und tabellarische Darstellungen und allgemein verständliche Formulierungen und Verwendung standardisierter Darstellungsformen.