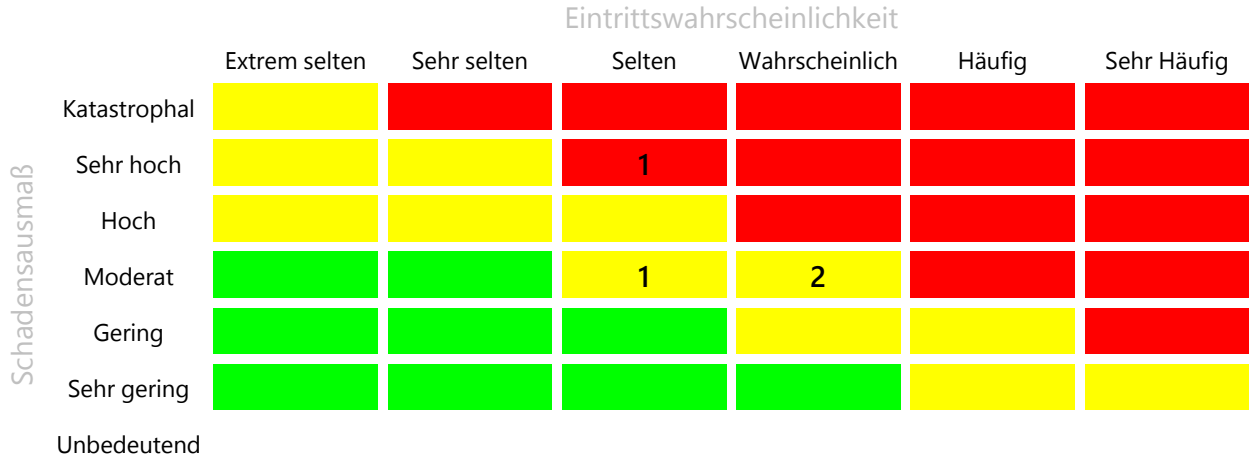
Risikobericht

Zu Strukturelementen: DAS, Fileshare, Cloud Service

Inhaltsverzeichis

Risiken im Überblick



RKZ	Kürzel	Beschreibung	Status
15	Schuba_C_HR Management	Schutzbedarfsklasse C / HR Management	Aktiv
12	KRY_001	Mangelnde kryptographische Kontrollen	Aktiv
12	RLK_001	D: IT-Compliance Risiko	Aktiv
9	Schuba_B_CloudCRM	Schutzbedarfsklasse B / Cloud CRM Fragen	Aktiv

D: IT-Compliance Risiko (RLK_001)

Identifiziert am:	10.01.2018	Letzte Änderung:	04.04.2019 13:50
Eintrittswahrscheinlichkeit:	Wahrscheinlich	Schadensausmaß:	Moderat
Verantwortliche(r):	Clarissa Hammer		
Managementsystem:	Informationssicherheitsmanagement		
Beschreibung:	es sind nicht alle Vorschriften berücksichtigt bzw. nicht alle nötigen Regelungen getroffen		
Schutzziele:	Vertraulichkeit Verfügbarkeit Integrität		
Zugewiesene Entitäten:	TeSA (OrgEh) SEC (OrgEh) DAS (OrgEh) MuG (OrgEh)		

Offene Maßnahmen:

Sicherstellung der Einhaltung der IT-Compliance (ISMS_RLK M01.01)

OrgEH:	TeSA
Beschreibung:	- Prüfen Sie alle relevanten gesetzlichen, amtlichen und vertraglichen Anforderungen im Sinne der Informationssicherheit wie beispielsweise die Folgenden: - Gesetze - Verordnungen - Vorschriften - Normen - Industriestandards - Interne Vorschriften (Anweisungen, Betriebsvereinbarungen) - Vertragliche Vereinbarungen - Erstellen Sie daraus eine Liste der für Ihr Unternehmen relevanten Anforderungen und ihrer Quellen. - Prüfen Sie die Einhaltung der Vorgaben - Leiten Sie bei der Abweichung von Vorgaben Maßnahmen ab und teilen Sie diesen Verantwortlichen zu. Definieren Sie dafür auch Umsetzungsfristen.
Fortschritt:	0%

geistiges Eigentum sicherstellen (ISMS_RLK M01.02)

OrgEH:	TeSA
Beschreibung:	Ergreifen Sie dazu folgende Maßnahmen: - Bei Gebrauch und Veröffentlichung müssen Copyrights sowie Warenzeichen beachtet werden - Die Einhaltung von Lizenzbestimmungen insbesondere bei Software ist zu beachten - Regelungen in Kauf-, Miet- und Leasingverträgen sowie in Wartungsverträgen sind zu beachten Dazu sollten klare Arbeitsanweisungen verfasst werden die die Mitarbeiter hinsichtlich dieser Themen sensibilisieren.
Fortschritt:	0% am 18.04.2019 13:44
Fortschrittsmeldung:	

Überprüfung nationaler Gesetze zur Anwendung kryptographischer Verfahren (ISMS_RLK M01.05.02)

OrgEH:	TeSA
Beschreibung:	Es sollte erhoben werden, ob alle nationalen Gesetze und Anforderungen hinsichtlich Anwendung von kryptographischen Verfahren bekannt sind und ob diese bzw. ihre Anforderungen für das Unternehmen relevant sind und eingehalten werden. Diese Compliance Überprüfung sollte nach initialer Einführung in regelmäßigen Abständen hinsichtlich Vollständigkeit wiederholt werden. Weiters sind beim Erkennen von Abweichungen hinsichtlich relevanter Anforderungen risikoadäquate Maßnahmen abzuleiten.
Fortschritt:	90% am 19.04.2019 10:27
Fortschrittsmeldung:	test

Abgeschlossene Maßnahmen:

Sicherstellung des angemessenen Schutzes von Aufzeichnungen (ISMS_RLK M01.03)

OrgEH:	TeSA
Beschreibung:	Sie sollten folgende Faktoren berücksichtigen wenn Sie Aufzeichnungen nach gesetzlichen, vertraglichen und geschäftlichen Anforderung vor Verlust, Zerstörung, Fälschung etc. anforderungskonform schützen wollen: - Einhaltung der Vorgaben der Datenklassifikation (siehe dazu auch Maßnahme ISMS_WMG M02.01) - die verwendeten Speichermedien und ihre Lebensdauer sollten regelmäßig überwacht und geprüft werden - die Zugriffsrechte auf die Aufzeichnungen sind regelmäßig zu überprüfen - der festgelegten Aufbewahrungs- bzw. Löschfristen sind zu erhaben und einzuhalten
Fortschritt:	100% am 01.05.2017 8:45
Fortschrittsmeldung:	Prozess wurde definiert und Verfahrensanweisung an die verantwortlichen Abteilungen übermittelt

Sicherstellung des angemessenen Schutzes von personenbezogenen Daten (ISMS_RLK M01.04)

OrgEH:	TeSA
Beschreibung:	Um den Schutz von personenbezogenen Daten sicherzustellen, sollte den relevanten Datenschutzgesetzen bzw. der Datenschutz-Grundverordnung sowie etwaigen bereichsspezifischen Gesetzen und Verordnungen zum personenbezogenen Datenschutz entsprochen werden. Ebenso ist auf die Einhaltung von internen Vereinbarungen (Betriebsvereinbarungen, Dienstvereinbarungen, ...) und entsprechenden Vertragsbedingungen zu achten. Sofern der Nutzen erkannt werden kann und die Ressourcen zur Verfügung gestellt werden können, wäre die Einrichtung eines nachhaltiges Datenschutzmanagementsystem zu empfehlen. Weiterführende Informationen zu diesem sehr umfangreichen Thema finden Sie auch in der Wissensdatenbank der TogetherSecure GmbH zum Thema EU-Datenschutz Grundverordnung.
Fortschritt:	100% am 01.05.2018 12: 0
Fortschrittsmeldung:	Datenschutzprojekt im Zuge der Umsetzung der DSGVO gestartet. Projekt wird vom neu ernannten DSB übernommen und in eigenem Managementsystem umgesetzt

Erstellung einer Datenklassifikationsvorgabe (ISMS_WMG M02.01)

OrgEH:	TeSA
Beschreibung:	Die Schutzwürdigkeit von Aufzeichnungen sollte sich nach der Klassifikation der Daten richten: - Die Datenklassifikation sollte besagen, wie die Daten entsprechen ihrer Klassifikation zu erheben, zu speichern, zu übertragen, zu überlassen und zu löschen sind. - Gängig, im Sinne der Unterscheidung der Datenklassen, ist die Einteilung in "öffentlich", "intern", "vertraulich" und "geheim". - Beachten Sie dabei auch die Unterscheidung von personenbezogenen und nicht personenbezogenen Daten. Ggf. macht es auch Sinn die Datenklasse "vertraulich" in "sensible personenbezogene Daten" weiter zu untergliedern. - es kann auch Sinn machen, abhängig von der Größe der Organisation zu unterscheiden, ob die Daten in oder außerhalb der Organisationsgrenzen verarbeitet bzw. übermittelt werden; außerhalb der Organisationsgrenzen werden innerhalb einer Datenklasse oft strengere Vorgaben gemacht, als innerhalb des gemeinsamen Netzwerks
Fortschritt:	100% am 01.05.2017 8:45
Fortschrittsmeldung:	Erstellt und kommuniziert

Aktive Kontrollen:

geistiges Eigentum sicherstellen (ISMS_RLK K01.02)

OrgEH:	Team Secure AG
Umsetzter:	Tom Leisch
Prüfverhalten:	Alle müssen akzeptieren
Erstmalig:	14.01.2019 12:00
Wiederkehrend:	☒ Alle 1 Jahr(e)
Deadline:	☐
Beschreibung:	Überprüfen Sie anlassbezogen bzw. in regelmäßigen geplanten Abständen stichprobenweise die Einhaltung von Arbeitsanweisungen und Vorgaben zum Thema geistiges Eigentum hinsichtlich: - die Beachtung von Copyrights sowie Warenzeichen bei Gebrauch und Veröffentlichung - die Einhaltung von Lizenzbestimmungen insbesondere bei Software - die Einhaltung von Regelungen in Kauf-, Miet- und Leasingverträgen sowie in Wartungsverträgen
Bemerkung:	

Durchgeführte Kontrollen:

1. Kontrolle ausgelöst am 14.01.2019 12:00 Status: Ausstehend

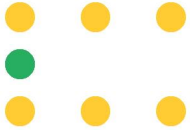
Audits zur Sicherstellung des Schutzes von personenbezogenen Daten (ISMS_RLK K01.04)

OrgEH:	Team Secure AG
Umsetzter:	IT Field Support
Prüfverhalten:	Alle müssen akzeptieren
Erstmalig:	14.01.2019 12:00
Wiederkehrend:	☒ Alle 1 Jahr(e)
Deadline:	☐
Beschreibung:	Um den Schutz von personenbezogenen Daten sicherzustellen, sollte den relevanten Datenschutzgesetzen bzw. der Datenschutz-Grundverordnung sowie etwaigen bereichsspezifischen Gesetzen und Verordnungen zum personenbezogenen Datenschutz entsprochen werden. Ebenso ist auf die Einhaltung von internen Vereinbarungen (Betriebsvereinbarungen, Dienstvereinbarungen, ...) und entsprechenden Vertragsbedingungen zu achten. Um dem gerecht zu werden sollte ein nachhaltiges Datenschutzmanagementsystem betrieben werden. Um die Wirksamkeit eines solchen Systems bzw. etwaiger anderer Maßnahmen zur Sicherstellung des Schutzes personenbezogenen Daten zu gewährleisten, wäre es sinnvoll regelmäßig durchzuführende Datenschutzaudits vorzusehen. Hinweis: Für weitere Kontrollen zum Datzenschutmanagementsystem finden Sie auch in der Wissensdatenbank der TogetherSecure GmbH zum Thema EU-Datenschutz Grundverordnung Vorlagen.
Bemerkung:	

Durchgeführte Kontrollen:

1. Kontrolle ausgelöst am 14.01.2019 12:00 Status: Ausstehend

Mangelnde kryptographische Kontrollen (KRY_001)

Identifiziert am:	17.10.2018	Letzte Änderung:	
Eintrittswahrscheinlichkeit:	Wahrscheinlich	Schadensausmaß:	Moderat
Verantwortliche(r):	Max Mustermann		
Managementsystem:	Informationssicherheitsmanagement		
Beschreibung:	Es gibt Mängel hinsichtlich der Vorgaben zur Kyptographie und hinsichtlich kryptographischer Kontrollen		
Schutzziele:	Vertraulichkeit Verfügbarkeit Integrität		
Zugewiesene Entitäten:	TeSA_IT (OrgEh) SEC_IT (OrgEh) Fileshare (Ressource)		

Abgeschlossene Maßnahmen:

Erstellung einer Leitlinie zur Nutzung kryptographischer Kontrollen (ISMS_KRY M10.01.01.01)

OrgEH:	TeSA
Beschreibung:	Dabei sollten Vorgaben zu Mindeststandards von kryptographischen Verfahren, sowie zur Methodik und Pflege gemacht werden Typische Kryptopgrahische Verfahren die bedacht werden sollten: - Symmetrische Verschlüsselungsverfahren - Asymmetetrische Verschlüsseltungsverfahren - Hashfunktionen - Datenauthentisierung - Instanzauthentisierung - Vorgaben zum Einsatz einer PKI Weiters sollte eine Auflistung aller eingesetzter kryptographischer Verfahren im Unternehmen erstellt werden und die Dokumentation ihrer Ausführung bzw. Beurteilung ausreichender Sicherheit erfolgen. Etwaige Absicherungsmaßnahmen sind abzuleiten, wenn die aktuell eingesetzten kryptographischen Verfahren nicht ausreichend sind.
Fortschritt:	100% am 01.05.2017 8:45
Fortschrittsmeldung:	Leitlinie fertiggestellt - siehe Anhang

Vorgaben zur sicheren Verwaltung kryptographischer Schlüssel (ISMS_KRY M10.01.02.01)

OrgEH:	TeSA
Beschreibung:	Die Leitlinie zur Verwendung von kryptographischen Schlüsseln sollte folgendes regeln: - Schutz der öffentlichen Schlüssel vor Änderung und Zerstörung - Schutz der geheimen und privaten Schlüssel vor unberechtigtem Zugriff - Schlüsselmanagement auf Basis von Normen und sicheren Methoden/Zertifikaten - Protokollierung der Aktivitäten zum Schlüsselmanagement - Regelungen zur Gültigkeitsdauer von Schlüsseln und sichere Zerstörung von Schlüsseln
Fortschritt:	100% am 28.10.2017 12: 0
Fortschrittsmeldung:	fertig und freigegeben

Aktive Kontrollen:

Review der Leitlinie zur Nutzung kryptographischer Kontrollen (ISMS_KRY K10.01.01.01)

OrgEH:	Team Secure AG
Umsetzter:	Max Mustermann
Prüfverhalten:	Erste Rückmeldung entscheidet
Erstmalig:	17.12.2018 12:00
Wiederkehrend:	☒ Alle 1 Jahr(e)
Deadline:	☐
Beschreibung:	Die existierende Leitlinie zur Nutzung kryptographischer Kontrollen sollte in regelmäßigen Abständen reviewed werden. Dabei ist vor allem darauf zu achten, ob dir Vorgaben zu den einzusetzenden kryptographischen Verfahren noch dem Stand der Technik entsprechen. Etwaige Anpassungen sind ggf. vorzunehmen.
Bemerkung:	

Durchgeführte Kontrollen:

1. Kontrolle ausgelöst am 22.01.2018 12:00	Status:	**Fehlgeschlagen** (Abgelehnt)
2. Kontrolle ausgelöst am 30.11.2017 12:00	Status:	Ausstehend
3. Kontrolle ausgelöst am 22.01.2018 12:00	Status:	Ausstehend
4. Kontrolle ausgelöst am 17.12.2018 12:00	Status:	Ausstehend

Review der Vorgaben zur sicheren Verwaltung kryptographischer Schlüssel (ISMS_KRY K10.01.02.01)

OrgEH:	Team Secure AG
Umsetzter:	Max Mustermann
Prüfverhalten:	Erste Rückmeldung entscheidet
Erstmalig:	17.12.2018 12:00
Wiederkehrend:	☒ Alle 1 Jahr(e)
Deadline:	☐
Beschreibung:	Die Vorgaben zur sicheren Verwaltung kryptographischer Schlüssel sollten in regelmäßigen Abständen überprüft und nötigenfalls aktualisiert werden.
Bemerkung:	

Durchgeführte Kontrollen:

1. Kontrolle ausgelöst am 22.01.2018 12:00 Status: Abgeschlossen am 12.12.2018 13:52

Geprüft von: Peter Innereiter (Überarbeitung nötig) am 06.12.2018 09:38

Begründung: bitte genauere Angaben, ob Vorgaben noch gepasst haben oder ob Aktualisierung notwendig

Clarissa Hammer (Akzeptiert) am 12.12.2018 13:52

Peter Innereiter (Akzeptiert) am 06.12.2018 09:53

2. Kontrolle ausgelöst am 17.12.2018 12:00 Status: Ausstehend

Schutzbedarfsklasse B / Cloud CRM Fragen (Schuba_B_CloudCRM)

Identifiziert am:	13.02.2019	Letzte Änderung:	
Eintrittswahrscheinlichkeit:	Selten	Schadensausmaß:	Moderat
Verantwortliche(r):	Max Mustermann		
Managementsystem:	Informationssicherheitsmanagement		
Schutzziele:	Vertraulichkeit Verfügbarkeit Integrität		
Zugewiesene Entitäten:	Cloud Service (Ressource)		

Offene Maßnahmen:

Logging der Applikation aktivieren (M_B_03)

OrgEH:	DAS
Beschreibung:	Logging der Applikation aktivieren und anforderungskonform konfigurieren <... weitere Erklärungen ...>
Fortschritt:	10% am 25.03.2019 17:19
Fortschrittsmeldung:	schon dabei

Schutzbedarfsklasse C / HR Management (Schuba_C_HR Management)

Identifiziert am:	13.02.2019	Letzte Änderung:	
Eintrittswahrscheinlichkeit:	Selten	Schadensausmaß:	Sehr hoch
Verantwortliche(r):	Max Mustermann		
Managementsystem:	Informationssicherheitsmanagement		
Schutzziele:	Vertraulichkeit Verfügbarkeit Integrität		
Zugewiesene Entitäten:	Cloud Service (Ressource)		

Offene Maßnahmen:

Zertifizierung einfordern (M_C_02)

OrgEH:	DAS
Beschreibung:	Vom Hersteller bzw. Service Provider eine adäquate Zertifizierung einfordern <... weitere Erklärung ...>
Fortschritt:	40% am 04.04.2019 10:45
Fortschrittsmeldung:	test