Fragebogen zur Selbsteinschätzung

Ersteinschätzung zu Informationssicherheit, Datenschutz & Compliance

Datenschutz Pöllinger GmbH

Unternehmen	Ansprechpartner	Datum

Bitte bewerten Sie jede Aussage mit Ja, Nein, Teilweise oder Nicht bekannt.
Mehrere Antworten mit „Nein“ oder „Nicht bekannt“ zeigen typischen Handlungsbedarf auf.

1. Organisation & Verantwortung

		Ja	Nein	Teilweise	Nicht bekannt
1	Dokumentiertes Informationssicherheits-managementsystem (ISMS) mit Regeln und Prozessen vorhanden.	○	○	○	○
2	Informationssicherheitsbeauftragter (ISB) benannt.	○	○	○	○
3	ISMS wird regelmäßig überprüft und aktualisiert.	○	○	○	○
4	Management ist über Bedeutung, Chancen und Risiken von Informations-sicherheit informiert.	○	○	○	○
5	Regelmäßige Schulungen zur Informationssicherheit für Mitarbeitende.	○	○	○	○

2. Assets, Standorte & Prozesse

		Ja	Nein	Teilweise	Nicht bekannt
6	Vollständige und aktuelle Inventarliste / Assetverzeichnis vorhanden.	○	○	○	○
7	Physische Informationssicherheit und Zutrittsregelungen bewertet und umgesetzt.	○	○	○	○
8	Kontinuierliches Risikomanagement mit regelmäßigen Risikobewertungen etabliert.	○	○	○	○
9	Geregelte On- und Offboarding-Prozesse sowie Home-Office-/ Mobile-Office-Regelungen vorhanden.	○	○	○	○

3. Technische Schutzmaßnahmen

		Ja	Nein	Teilweise	Nicht bekannt
10	Firewall, Schadschutz und Event Logging sind wirksam umgesetzt.	○	○	○	○
11	Passwortvorgaben und rollenbasierte Zugriffsrechte sind festgelegt.	○	○	○	○
12	Sicherheitsanforderungen bei Subunternehmen / Lieferanten werden kontrolliert.	○	○	○	○
13	Software und IT-Systeme werden regelmäßig auf Schwachstellen geprüft und Schwachstellen behoben.	○	○	○	○
14	Mobile Endgeräte werden über Mobile Device Management (MDM) verwaltet.	○	○	○	○
15	Daten und Systemkonfigurationen werden regelmäßig per Backup gesichert.	○	○	○	○
16	Sichere Authentifizierung, z. B. 2-Faktor-Authentifizierung und Passwortmanager, ist umgesetzt.	○	○	○	○
17	Die Mehrzahl der Nutzer hat keine lokalen Administratorrechte.	○	○	○	○
18	Das Unternehmensnetzwerk ist sinnvoll segmentiert.	○	○	○	○

4. Compliance, Datenschutz & Betrieb

		Ja	Nein	Teilweise	Nicht bekannt
19	Relevante Gesetze und Kunden-anforderungen sind bekannt und werden umgesetzt.	○	○	○	○
20	Datenschutzbeauftragter (DSB) ist – soweit erforderlich – benannt.	○	○	○	○
21	IT-Security ist ein wesentlicher Bestandteil der Aufgaben der IT-Abteilung.	○	○	○	○
22	Nutzung von Cloud-Diensten ist geregelt und erfolgt nach Bewertung und Freigabe.	○	○	○	○
23	Schutz personenbezogener Daten gemäß DSGVO ist sichergestellt.	○	○	○	○
24	Notfallpläne für Ausnahmesituationen sind definiert.	○	○	○	○
25	Änderungen an IT-Systemen und Cloud-Diensten werden dokumentiert und gesteuert.	○	○	○	○
26	Risiken mit Auswirkung auf die Informationssicherheit werden dokumentiert und gemanagt.	○	○	○	○

Zusätzliche Hinweise / beobachteter Handlungsbedarf

Nächster Schritt: Ergebnisse besprechen und Maßnahmen priorisieren

www.datenschutz-poellinger.de | Tel.: +49 9181 2705770