IB002 SICHERHEITSNACHWEIS

Unser Nachweis zu Informations-, IT- und Cybersicherheit

Unser Unternehmen hat grundlegende organisatorische, technische und personelle Sicherheitsmaßnahmen umgesetzt, um Informationen, IT-Infrastruktur und digitale Geschäftsprozesse angemessen zu schützen. Die Maßnahmen gelten unternehmensweit und bilden ein solides Basisniveau für einen sicheren und verlässlichen Geschäftsbetrieb.
Dieses Dokument dient als Nachweis unserer Aktivitäten für unsere Kunden und Partner.

Normative Grundlagen

Unser Informationssicherheitsmanagement berücksichtigt die für unser Unternehmen anwendbaren Anforderungen und Grundsätze etablierter Standards wie ISO/IEC 27001 sowie nötiger, gültiger, sinnvoller und anwendbarer Richtlinien aus Cyber Trust Label Austria und NIS2.

Sicherheitsorganisation und Verantwortlichkeiten

Die wesentlichen Anforderungen an die Informations-, IT- und Cybersicherheit sind in internen Richtlinien und Vorgaben dokumentiert. Zuständigkeiten und Verantwortlichkeiten sind eindeutig festgelegt. Benannte Personen koordinieren die Umsetzung der Sicherheitsmaßnahmen, beobachten aktuelle Cyberrisiken und veranlassen bei Bedarf geeignete Verbesserungen.

Authentifizierung

Für den Zugang zu unseren Systemen und Anwendungen bestehen verbindliche Authentifizierungsverfahren der PMS IT. Dazu gehören Vorgaben zur sicheren Auswahl und Verwaltung von Passwörtern, die Nutzung von SSO zur zentralen und sicheren Anmeldung sowie der Einsatz zertifikatsbasierter Authentifizierungsverfahren mit MFA.

Zugriffsberechtigungen

Berechtigungen werden nach dem Grundsatz der geringsten Privilegien vergeben. Mitarbeitende erhalten ausschließlich jene Zugriffsrechte, die sie für ihre jeweiligen Aufgaben oder Rollen benötigen. Die Vergabe, Änderung und Entziehung von Berechtigungen erfolgen nach dokumentierten Prozessen. Für kritische Freigaben wird das Vier Augen Prinzip als Kontrollfunktionen eingesetzt.

Schutz von Endgeräten und IT-Systemen

Unsere Endgeräte wie auch zentralen IT-Systeme werden durch geeignete Cybersecurity-Maßnahmen geschützt. Dazu gehören insbesondere laufend aktualisierte Viren- und Schadsoftware-Schutzlösungen (XDR/EDR), sichere Systemkonfigurationen, Vulnerability-Scans, regelmäßige Sicherheitsupdates und geeignete Anwendungskontrollen. Nicht mehr unterstützte Systeme werden rechtzeitig ersetzt oder durch dokumentierte Ausnahmeregelungen und kompensierende Maßnahmen abgesichert. Netzwerke und aus dem Internet erreichbare Systeme werden durch geeignete Firewall-, Segmentierungs-, und Zugriffsschutzmaßnahmen vor unberechtigten Zugriffen geschützt.

Penetrationstests und Überwachung der Angriffsfläche

Zur regelmäßigen Überprüfung unserer Sicherheit führen wir im Jahresverlauf in definierten Intervallen risikobasierte Penetrationstests durch. Ergänzend überwachen wir unsere externe Angriffsfläche laufend auf neue oder ungeschützte Systeme, Fehlkonfigurationen und bekannte Schwachstellen. Festgestellte Risiken werden bewertet, priorisiert, zeitnah mitigiert und bis zur Lösung nachverfolgt.

Protokollierung und Nachvollziehbarkeit

Sicherheitsrelevante Aktivitäten auf Systemen, die kritische Daten abrufen, speichern oder verarbeiten, werden angemessen protokolliert. Die Protokolle unterstützen die Erkennung, Analyse und nachvollziehbare Aufarbeitung möglicher Sicherheitsvorfälle. Die aktiven Protokollierungsquellen und Speicherorte sind dokumentiert. Der Zugriff auf Protokolldaten ist auf berechtigte Personen beschränkt. Die Aufbewahrungsdauer richtet sich nach der Schutzbedürftigkeit der Systeme sowie den gesetzlichen, vertraglichen und internen Anforderungen.

SOC- und ROC-Teams

Unser Security Operations Center (SOC) überwacht und analysiert sicherheitsrelevante Ereignisse, erkennt potenzielle Cyberangriffe und koordiniert die erforderlichen Reaktionsmaßnahmen. Ergänzend konzentriert sich unser Ransomware Operations Center (ROC) gezielt auf die Prävention, Erkennung und Behandlung von Ransomware-Bedrohungen. Dazu gehören die Bewertung verdächtiger Aktivitäten, die rasche Eindämmung möglicher Angriffe sowie die Koordination von Wiederherstellungs- und Kommunikationsmaßnahmen. Beide Teams tragen proaktiv zur kontinuierlichen Weiterentwicklung unserer Sicherheitskonzepte und zur stetigen Stärkung unserer Cyberresilienz bei.

Backup und Wiederherstellung

Für Geschäftsdaten und unsere Systeme bestehen dokumentierte Backup- und Wiederherstellungsverfahren. Die Sicherungen werden regelmäßig durchgeführt und so geschützt, dass sie auch bei einem schwerwiegenden Cyberangriff verfügbar bleiben. Zur Absicherung gegen Ausfälle, Fehlbedienungen, technische Defekte sowie Cyberangriffe werden Sicherungen auf unterschiedlichen Speichermedien und an voneinander getrennten Standorten gespeichert. Ein Teil der Sicherungen wird unveränderbar aufbewahrt und ist physisch von den Produktivsystemen getrennt, um die Verfügbarkeit der Daten auch im Falle eines schwerwiegenden Sicherheitsvorfalls sicherzustellen. Die Wiederherstellung wichtiger Daten und Services wird regelmäßig getestet. Die dabei gewonnenen Erkenntnisse fließen in die laufende Verbesserung unserer Sicherheits- und Wiederherstellungsmaßnahmen ein.

Kontinuierliche Verbesserung und Nachweis

Informations-, IT- und Cybersicherheit verstehen wir als kontinuierlichen Prozess.
Wir überprüfen unsere Maßnahmen regelmäßig und passen sie an neue Bedrohungen, technische Entwicklungen, betriebliche Veränderungen sowie gesetzliche und vertragliche Anforderungen an.
Die Umsetzung dieser Informations-, IT- und Cybersicherheitsmaßnahmen weisen wir unter anderem durch unser gültiges Cyber Trust Austria Standard Label nach.