Inhalt

1. Ausgangslage und Geltungsbereich

Die Equans Switzerland Process Automation AG (EPRA) zertifiziert sich nach der ISO/IEC Norm 27001:2013 und verpflichtet sich zur Erfüllung dieser Anforderungen. Dabei umfasst der Geltungsbereich: Die ganze Firma mit allen Mitarbeitenden und alle Geschäftsprozesse und Infrastrukturen, welche für die Geschäftstätigkeit der EPRA notwendig sind.

2. Ziele der Informationssicherheit

EPRA hat sich folgende Ziele gesetzt:

- Angemessener Schutz von Informationen in Bezug auf Verfügbarkeit, Vertraulichkeit sowie Integrität.
- Erfüllung der gesetzlichen, vertraglichen und internen Vorgaben im Bereich Informationssicherheit.
- ISO/IEC 27001:2013 als Alltagswerkzeug zur Qualitäts-, Wissenssicherung und konstanten Weiterentwicklung der Firma nutzen.

3. Das ISMS der EPRA

Im Informationssicherheits-Managementsystem der EPRA werden alle Verfahren und Regeln dokumentiert, welche dazu dienen, die Informationssicherheit der EPRA gegenüber ihren Anspruchsgruppen zu gewährleisten. Das ISMS wird laufend kommuniziert und stufengerecht geschult. Die Anwendung dieser Regelungen ist zwingend und verbindlich.

4. Kontinuierliche Verbesserung

Das ISMS der EPRA wird laufend überprüft und den aktuellen Gegebenheiten angepasst. Im Sinn einer kontinuierlichen Verbesserung werden die Kompetenzen aller beteiligten Stellen laufend weiterentwickelt.

5. Organisation und Verantwortlichkeiten

5.1. Geschäftsleitung der EPRA

Die Geschäftsleitung der EPRA ist das oberste operative Entscheidungsorgan der Firma und delegiert Aufgaben, Verantwortung und Kompetenzen in der Informationssicherheit an den CISO.

5.2. Mitarbeitende der EPRA

Alle Mitarbeitenden der EPRA, welche Tätigkeiten im Geltungsbereich des ISMS verrichten sind für die Informationssicherheit in ihrem Fachbereich verantwortlich. Die Vorgesetzten aller Hierarchiestufen sind verpflichtet, die dafür nötigen Ressourcen und Skills zur Verfügung zu stellen. Sie sind verpflichtet, sämtliche notwendigen Sicherheitsmassnahmen im Rahmen ihres Verantwortungsbereiches nachhaltig umzusetzen. Sie leiten ihre Mitarbeitenden an und schulen sie bedarfsgerecht.

5.3. CISO

Der CISO ist verantwortlich für die Erarbeitung und Definition, Überwachung, Steuerung und Betrieb und kontinuierliche Verbesserung des ISMS. Er rapportiert an die Geschäftsleitung.

5.4. Asset Owner

Asset Owner legen Regeln für den zulässigen Gebrauch von ihnen zugeteilten Informationen und Werten fest, dokumentieren diese und wenden sie an.

5.5. Risk Owner

Risk Owner führen den Prozess zur Informationssicherheitsrisikobeurteilung und –Behandlung für ihrRisiken. Sie analysieren und bewerten die Risiken und legen entsprechende Massnahmen fest.

5.6. Lieferantenmanager

Der Lieferantenmanager führt den Prozess zur Überwachung und Steuerung der Lieferanten in Bezug auf Informationssicherheit.

5.7. Externe Mitarbeitende / Mitarbeitende von Dritten

Die Regelungen der EPRA im Kontext Informationssicherheit gelten entsprechend auch für Personen, welche als Externe oder Mitarbeitende von Dritten im Geltungsbereich des ISMS Tätigkeiten verrichten und sind durch diese einzuhalten.

6. Kontrollen

Die EPRA überprüft die Informationssicherheit in geplanten und regelmässigen Abständen mit internen und externen Audits. Die Ergebnisse dieser Kontrollen fliessen in die kontinuierliche Verbesserung ein.

7. Sanktionen

Die EPRA vereinbart mit Dritten Konventionalstrafen, welche bei wiederholten oder einzelnen schwerwiegenden Verstössen gegen die Sicherheitsvorschriften und –Weisungen eingefordert werden können. Bei den internen Mitarbeitenden kommen in solchen Fällen die arbeitsrechtlichen Sanktionen zur Anwendung.

8. Begriffsdefinitionen

8.1. Informationssicherheit

Unter der Informationssicherheit werden alle Massnahmen verstanden, die zur Aufrechterhaltung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen angeordnet, durchgeführt, überprüft und kontinuierlich verbessert werden. Diese Massnahmen können u. a. organisatorischer, technischer oder baulicher Natur sein.

- Vertraulichkeit: Gewährleistung des Zugangs zu Informationen nur für die Zugangsberechtigten.
- Integrität: Sicherstellen der Unversehrtheit und Vollständigkeit von Informationen und deren Verarbeitungsmethoden.
- Verfügbarkeit: Gewährleistung des bedarfsorientierten Zugangs zu Informationen und den zugehörigen Werten für berechtigte Benutzer.

8.2. Informationssicherheits-Managementsystem (ISMS)

Unter einem ISMS wird verstanden:

- Sämtliche Regeln, Verfahren und Prozesse innerhalb des Anwendungsbereichs, welche die Informationssicherheit definieren, steuern, durchführen, überprüfen, aufrechterhalten und kontinuierlich verbessern.
- Die Dokumentation erfolgt mittels ISMS Framework, den Controls der SOA (Anwendbarkeitserklärung) und mit entsprechenden Policies, Prozessübersichten und weiteren Nachweisdokumenten.

8.3. CISO (Chief Information Security Officer)

Der CISO ist verantwortlich für die Informationssicherheit in seinem zugewiesenen Geltungsbereich.