BUSINESS IT
Supporting Your Business

Sicherheitspolitik nach ISO 27001

1 Ausgangslage und Geltungsbereich

Die BUSINESS IT AG zertifiziert sich nach der ISO Norm 27001. Dabei umfasst der Geltungsbereich der Zertifizierung die ganze Firma (sämtliche Mitarbeitenden, Standorte, Geschäftstätigkeiten, Prozesse, Services etc.).

2 Ziele der Informationssicherheit

Die BUSINESS IT AG hat sich folgende übergeordnete Ziele gesetzt:

- Angemessener Schutz von Informationen in Bezug auf Verfügbarkeit, Vertraulichkeit sowie Integrität
- Erfüllung der gesetzlichen, vertraglichen und internen Vorgaben im Bereich Informationssicherheit
- ISO 27001 als Alltagswerkzeug nutzen
- Zur Qualitätssicherung
- Zur Effizienzsteigerung der Prozesse
- Zum Aufbau eines IKS
- Zur konstanten Weiterentwicklung der Firma

3 Das Informationssicherheits-Managementsystem (ISMS) der BUSINESS IT AG

Im ISMS der BUSINESS IT AG werden alle Verfahren und Regeln dokumentiert, welche dazu dienen, die Informationssicherheit der BUSINESS IT AG gegenüber ihren Anspruchsgruppen zu gewährleisten. Für einzelne Themen werden separate Policy Dokumente erstellt (z.B. die Arbeitsplatz Policy). Das ISMS ist im Confluence Wiki transparent verfügbar, wird laufend kommuniziert und stufengerecht geschult. Die Anwendung dieser Regelungen ist zwingend und verbindlich.

4 Kontinuierliche Verbesserung

Das ISMS der BUSINESS IT AG 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 Interne Mitarbeitende / Generell

Alle Mitarbeitenden der BUSINESS IT AG, 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.

5.2 CISO

Der CISO ist verantwortlich für die Erarbeitung und Definition, die Überwachung, die Steuerung, den Betrieb und die kontinuierliche Verbesserung des ISMS. Er rapportiert an das Executive Management / die Geschäftsführung.

5.3 Externe Mitarbeitende / Mitarbeitende von Dritten

Die Regelungen der BUSINESS IT AG 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.

5.4 Kontrollen

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

5.5 Sanktionen

Die BUSINESS IT AG 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.