siticom
a devoteam affiliate

we enable communication

Übersicht ISMS Regelungen

Informationen zum Dokument	
Version	1.3
Dokument ID	IS.AL07
Klassifikation	Public
Status	Released
Ursprungsversion freigegeben durch	ISB
Aktuelle Version freigeben durch	ISB
Gültig ab	01.08.2018
Review Zyklus	Jährlich
Dokumentendatum	03.11.2020

Einleitung

Diese Aufstellung in Kurzform fasst die Regeln des siticom Informationssicherheit Management Systems (ISMS) als Teil des Integrierten Management Systems (IMS) zusammen, um einen schnellen Überblick über das verwendete Regelwerk zu geben. Diese Aufstellung dient auch als Übersicht für interne und externe Mitarbeiter (Vertragsbestandteil). Das ISMS (IMS) der siticom ist nach ISO27001 zertifiziert.

Regelwerk

Informationssicherheit

- Sicherheitsprobleme oder Datenschutzprobleme sind and das siticom SOC zu melden (soc@siticom.de)
- Keine Weitergabe von personalisierten Zugriffskennungen

IT-Sicherheit

- Alle Geräte (Notebooks, Smartphones) müssen gegen Diebstahl gesichert werden
- Die Daten auf dem Arbeitsrechner müssen ausreichend verschlüsselt abgelegt werden (Notebook, PC, alle Harddisks)
    - Festplattenverschlüsselung z.B. per Bitlocker
- Treiber und BIOS Versionen müssen aktuell gehalten werden z.B. unter
    - Verwendung einer vom Hersteller bereitgestellten Support Software
    - Manuelle Pflege durch vom Hersteller der Komponenten zertifizierte Treiber
- Software und Betriebssystem müssen aktuell gehalten werden
    - Es darf nur freigegeben Software verwendet werden
    - Automatische Aktualisierungsfunktion der Software, des Betriebssystems
    - Bereitstellung neuer Versionen durch IT
- Alle Accounts müssen mit Passwort gesichert sein.
    - Passwortregeln:
        - Es darf nicht den Benutzernamen oder Teile des eigenen Namens enthalten
        - Es muss aus mindesten 8 Zeichen bestehen, außerdem, mindestens drei der folgenden Kriterien:
            - mindestens einen Großbuchstaben enthalten (A-Z ohne Umlaute)
            - mindestens einen Kleinbuchstaben enthalten (a-z ohne Umlaute)
            - mindestens eine Zahl (0-9) enthalten
            - mindestens ein Sonderzeichen (! $ # %) enthalten
    - Passwörter müssen sicher, aufbewahrt werden (z.B. KeePass)
    - Keine Weitergabe von Passwörtern an Dritte

- Bei Kaffeepausen (oder anderen Pausen) Rechner immer sperren
    - Manuelle Sperre (z.B. Windows Taste + L)

      
    - Aktivierung der automatischen Sperre über Bildschirmschoner mit Anmeldesperre
- Keine automatische E-Mail-Weiterleitungen an private oder externe Mailkonten

- Keine fremden Links anklicken (wegen Phishing E-Mails, Viren, Trojaner)
    - Zur Kontrolle vollständige E-Mail-Adressen oder Weblinks einblenden lassen
    - Vorsicht vor gefälschten E-Mails (Paypal, Amazon, Google, Microsoft, Telekom, Banken, u.ä.)
- Projekt und Kundendaten müssen einem regelmäßigen Backup unterliegen

Büro und physische Sicherheit

- Clean Desk Policy. Im Shared Office ist der Arbeitsplatz freizuräumen und Dokumente in Rolli oder Schrank zu schließen.
- Notebooks und anderer Geräte müssen nachts oder am Wochenende weggeschlossen werden.
- Eintritt in siticom Räumlichkeiten nur mit Transponder, Karte, Schlüssel oder PIN (bei Externen mit vorheriger Anmeldung)
- Es muss sichergestellt werden, dass sämtliche Daten von siticom sicher gelöscht werden (entsprechend DIN 66399).
- Defekte Harddisks mit siticom-Daten müssen geschreddert werden
- Drucken mit PIN. Alle unsere Laser-Drucker können das!
- Keine Ausdrucke am Drucker liegen lassen

Mobiles Arbeiten

- Daten auf USB-Sticks/SD-Karten etc. müssen verschlüsselt werden, z.B. mit Bitlocker.
- Fremde Speichermedien/USB-Sticks/SD-Karten etc. müssen auf Viren gescannt werden.
- USB aus unbekannten Quellen nicht verwenden

Softwareentwicklung

- Softwareentwicklung erfolgt nach OWASP Standard, sofern keine anderen Projektvorgaben vorliegen