LOGICALIS
Architects of Change

Übersicht: ISMS-Regelungen

Informationen zum Dokument	
Version	1.9
Dokument ID	IS.AL02.7
Klassifikation	Public
Status	Freigabe
Ursprungsversion freigegeben durch	ISB
Aktuelle Version freigeben durch	ISB
Gültig ab	01.08.2018
Review Zyklus	Jährlich
Dokumentendatum	18.03.2025

Einleitung

Diese Aufstellung in Kurzform fasst die Regeln des siticom Informationssicherheit Management Systems (ISMS) als Übersicht zusammen.

Diese Aufstellung dient als Übersicht für interne und externe Mitarbeiter (Vertragsbestandteil). Das ISMS als Teil des Integrierten Management Systems der siticom ist nach ISO27001 zertifiziert.

Introduction

This list here summarizes in short form the rules of the siticom Information Security Management System (ISMS) as an overview.

It serves as an overview for internal employees and external partners (part of their contract). The ISMS as part of the Integrated Management System of siticom is certified according to ISO27001.

Regelwerk

Allgemein

- Sicherheitsprobleme oder Datenschutzprobleme sind sofort an 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 bei siticom intern

Rules and Regulations

General

- Security or data protection problems must be reported immediately to the siticom via soc@siticom.de
- Do not pass on personalized access IDs!

IT security

- All devices (notebooks, smartphones) must be secured against theft
- The data on the work computer must be sufficiently encrypted (notebook, PC, all hard disks)
    - Hard disk encryption e.g. via Bitlocker at siticom internally

- 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! (siticom Software pool)
  - Automatische Aktualisierungsfunktion der Software, des Betriebssystems ist zu nutzen
  - Bereitstellung neuer Versionen im SW pool erfolgt 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 (besser mehr), 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

- Drivers and BIOS versions must be kept up to date, e.g. by
  - Use support software provided by the manufacturer
  - Do maintenance using drivers certified by the manufacturer of the components
- Software and operating system must be kept up to date
  - Only approved software may be used! (siticom software pool)
  - Automatic update function of the software and operating system must be used
  - Provision of new versions in the SW pool is carried out by IT
- All accounts must be secured with a password!
  - Password rules:
    - It must not contain the user name or parts of your own name
    - It must consist of at least 8 characters (preferably more) and at least three of the following criteria:
    - contain at least one capital letter (A-Z without “Ä,Ü,Ö” e.g. German “Umlaute”)
    - contain at least one lowercase letter (a-z “ä,ü,ö” e.g. German “Umlaute”)
    - contain at least one number (0-9)

- mindestens ein Sonderzeichen (! $ # %) enthalten (wenn toolbedingt möglich)
  - Passwörter müssen sicher, aufbewahrt werden (z.B. KeePass)
  - Keine Weitergabe von Passwörtern an Dritte!

- contain at least one special character (! $ # %) (if possible due to the tool)
  - Passwords must be stored securely (e.g. KeePass)
  - Do not pass on passwords to third parties!

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

  - Aktivierung der automatischen Sperre über Bildschirmschoner mit Anmeldesperre

- Always lock the computer during coffee breaks (or other breaks)
  - Manual lock (e.g. Windows key + L)

  - Activation of automatic lock via screen saver with login lock

- Keine automatische E-Mail-Weiterleitungen an private oder externe Mailkonten

- No automatic e-mail forwarding to private or external e-mail accounts

- Keine fremden Links anklicken (wegen Phishing E-Mails, Viren, Trojaner)
  - Zur Kontrolle vollständige E-Mail-Adressen oder Weblinks einblenden lassen (Mouse Over)
  - Vorsicht vor gefälschten E-Mails (Paypal, Amazon, Google, Microsoft, Telekom, Banken, u.ä.)

- Do not click on external links (to avoid e.g. phishing emails, viruses, Trojans)
  - Display complete e-mail addresses or web links for control purposes (Mouse over)
  - Beware of fake e-mails (e.g. concerning Paypal, Amazon, Google, Microsoft, Telekom, banks, etc.)

- Projekt und Kundendaten müssen einem regelmäßigen Backup unterliegen

- Project and customer data must be backed up regularly

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 sicher gelöscht, besser geschreddert werden
- Drucken mit PIN. Alle unsere Laser-Drucker können das!
- Keine Ausdrucke am Drucker liegen lassen!

Office and Physical Security

- Clean Desk Policy. In the shared office, the workplace must be cleared, and documents must be locked in a trolley or office cabinet.
- Notebooks and other devices must be locked away at night or at weekends.
- Access to siticom premises only with transponder, card, key or PIN (for external persons with prior registration)
- It must be ensured that all siticom data is securely deleted (in accordance with DIN 66399).
- Defective hard disks with siticom data must be deleted securely, or still better, shredded
- Printing with PIN. All our laser printers can do this!
- Do not leave any printouts on the printer!

Mobiles Arbeiten

- Daten auf USB-Sticks/SD-Karten etc. müssen verschlüsselt werden, z.B. mit Bitlocker.

Mobile Working

- Data on USB sticks/SD cards etc. must be encrypted, e.g. with Bitlocker.

- Fremde Speichermedien/USB-Sticks/SD-Karten etc. müssen auf Viren gescannt werden.
- USB aus unbekannten Quellen nicht verwenden!

- External storage media/USB sticks/SD cards etc. must be scanned for viruses.
- Do not use USB from unknown sources!

Softwareentwicklung

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

Software Development

- Software development is carried out according to the OWASP standard, unless other project specifications exist**.**