

Ergebnisse anzeigen

Auskunftsperson

8 Anonym

07:39

Zeit zum
Ausfüllen

1. Unternehmen *

Agilox

2. Ansprechpartner *

P. Reinhofer

3. Besteht bereits eine Zertifizierung nach ISO 27001? *

☐

Ja

☒

Nein

4. Existiert im Unternehmen einen namentlich benannter Informationssicherheitsbeauftragter?

☒

Ja

☐

Nein

5. Name des Informationssicherheitsbeauftragten

P. Scharner

6. Besteht ein Information Security Management System (ISMS)?

☒

Ja

☐

Nein

7. Gibt es im Unternehmen eine Informationssicherheitsleitlinie?

☒

Ja

☐

Nein

8. Wie ist die Informationssicherheit im Unternehmen organisiert?

zentrales ISMS über alle Abteilungen, Nach CIS v 8

9. Werden Mitarbeiter im Bereich der Informationssicherheit unterwiesen und fortlaufend geschult?

☒

Ja

☐

Nein

10. Werden hinsichtlich der Informationssicherheit Interne Audits durchgeführt?

☒

Ja

☐

Nein

11. Wie werden die Mitarbeiter über die Gefahren beim Umgang mit Informationen und deren Verarbeitung geschult sowie sensibilisiert?

Ja, mit jährlicher Auffrischung

12. Existiert ein Zutrittsmanagement in Ihrem Unternehmen?



Ja



Nein

13. Wie ist das Unternehmen gegen äußere und umgebungsbezogene Bedrohungen geschützt?

Zutrittschip für HQ, Rechenzentren via Venenscan

14. In welchem Umfang ist ein Schutz vor Schadsoftware (Viren, Würmer, usw.) im Unternehmen vorhanden?

Vollumfänglich über alle Instanzen

15. Wie werden die Datensicherungen (Back-Up's) erstellt sowie kontrolliert und in welchem Umfang wird die Wiederherstellung (Restores) regelmäßig getestet?

Datensicherungen täglich inkrementel, DR Tests 1 mal jährlich, Backup Recovery Test bei Implementierung neuer Applikationen + 1 - 2 mal jährlich je nach Wichtigkeit der Applikation

16. Wird vor Auftragsvergabe an Fremdfirmen eine Risikoanalyse der personellen u. organisatorischen Risiken durchgeführt?

☒

Ja

☐

Nein

17. Wird das Unternehmensnetzwerk durch aktuelle Firewall Standards vor Zugriff Dritter geschützt?

☒

Ja

☐

Nein

18. Inwiefern gibt es Richtlinien zum Umgang mit mobilen Datenträgern (z.B. Bänder, USB-Speichersticks, USB-Festplatten, CD's, DVD's, usw.)?

interne Betriebsmittelrichtlinie, externe private Datenträger sind verboten

19. Gibt es in Ihrem Unternehmen einen Prozess zur endgültigen und sicheren Entsorgung von Computermedien?

ja via Reisswolf

20. Welche Vorsichtsmaßnahmen werden getroffen, wenn ein elektronischer Austausch von Informationen erforderlich?

nach Informationsklassifizierung unterschiedlich

21. Gibt es eine Leitlinie zur Anwendung kryptografischer Maßnahmen (Verschlüsselung von mobilen Systemen/ Wechseldatenträger/ E-Mail) zum Schutz von Informationen?



Ja



Nein

22. Inwiefern sind Maßnahmen für die Entwicklung und Aufrechterhaltung der Business Continuity (Fortführung des ordnungsgemäßen Geschäftsbetriebs) im Unternehmen eingeführt?

Business Continuity Plan etabliert mit jährlichem Update

23. Inwiefern sind Regeln und Maßnahmen für den Fernzugriff (Remote Access) auf das Unternehmensnetz definiert und umgesetzt?

VPN, Jumphost, Zugriff für externe via Terminalserver auf spezifische Applikationen

24. In wie weit wurde eine Richtlinie entwickelt, die auf die Risiken beim Arbeiten mit mobilen Computern hinweist?

Betriebsmittelrichtlinie

25. In wie weit werden Informationen über die technischen Schwachstellen der eingesetzten Informationssysteme zeitnah beschafft, beurteilt und geeignete Maßnahmen für eine Umsetzung ergriffen (Patch-Management)?

Patchmgmt etabliert, Server werden an jedem ersten Dienstag und Mittwoch im Monat gepatched, vulnerability patches asap

26. Wie wird die Geheimhaltung bei der Zusammenarbeit mit Fremdfirmen sichergestellt?

NDA

27. Wie werden die Netzwerke verwaltet und gesteuert, damit sie vor Bedrohungen geschützt sind?

nach Best Practise Standards von unserem Betriebspartner als full managed service