

## Zertifizierungsordnung zum Informationssicherheitsspezialist

### A) Gegenstand

#### (was legt die Ordnung fest)

Diese Zertifizierungsordnung gilt für die Weiterbildung zum Informationssicherheitsspezialist. Sie bestimmt die Soll-Definition des Qualifikationsniveaus, Regelungen der Prüfung des Nachweises durch die Teilnehmer und der Bestätigung durch ein Personenzertifikat.

### B) Qualifikationsniveau

#### (welche Qualifikation soll erreicht werden)

Verständnis wesentlicher Grundlagen, Prinzipien und Methoden zur Realisierung von Informationssicherheit durch Betrachtung aus einer übergreifenden Perspektive, damit Zurechtfinden in der Komplexität der Informationssicherheit, Erstellen gesamthafter Lösungen, Erreichen eines besseren Verständnisses und Anwenden und Übertragen der Prinzipien auf neue Techniken oder verwandte Gebiete mit Themen und Kompetenzen mit einem Umfang von 16 Unterrichtseinheiten, eine Unterrichtseinheit beträgt 60 Minuten reine Lernzeit. Die Themenbereiche sind:

#### **Grundlagen:**

Begriffe und Motivation / Nutzen (Schutz, Rechtskonformität, ...); Ziele / Anforderungen (Vertraulichkeit, Integrität, Verfügbarkeit, ...); Schutzbedarfsfeststellung und Informationssicherheitsniveau; Herausforderungen.

#### **Management:**

Zur Realisierung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus mit Bedeutung, Prinzip, Komponenten und Zusammenwirken, Informationssicherheits-Management, -Politik, -Strategie, -Organisation, -Prozess, -Richtlinien, -Kontrolle mit Angriffserkennung und -behandlung, Lebenszyklus.

#### **Prinzipien, Methoden, Maßnahmen:**

Zum allgemeinen Verstehen von Sicherheitsprinzipien mit -methoden und -maßnahmen strukturiert gemäß dem Zusammenwirken in neun wesentliche Prinzipien in Sicherheitsmanagement, Sichere Nutzung (Sensibilisierung, Einstellung, Schulung, Wissen und Können), Sicherer Betrieb (Infrastruktur, Durchführung, Detektion / Reaktion, Hard- / Software, Datensicherung / Datenwiederherstellung, Übergabe / Übernahme), Sichere Entwicklung (Schutzbedarfsfeststellung, Gefährdungs-/Risikoanalyse, Sicherheitskonzeption), Auditierung (Audits, Protokollierung und Auswertung, Manipulations-/ Angriffserkennung (optional mit Reaktion)), Administration (Organisation / Prozess, Modellierung / Spezifikation, Umsetzung / Implementierung), Authentifikation (Wissen, Besitz, Eigenschaft, Mehr-Faktor, Passwort-Container, Einmal-Passwörter), Autorisierung (Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC)), Protektion (Einfachheit, Datenlokalität, Datenminimierung, Härtung, Kommunikationskontrolle, Verschlüsselung, Malware-Schutz, Tracking-Schutz, Minimale Rechte, Funktionalitätsbeschränkung, Einsatz sichererer Software, Aktualisierung, Mehrstufigkeit, Replikation, Sicheres Löschen, Logische Trennung, Physische Trennung, Physischer Schutz)

#### **Gefahren und Lösungen:**

Zum konkreten und anwendbaren Verständnis von Gefahren und typischen Schutzmaßnahmen mit Arten von Gefahren, Sicherheitsebenen, Gefahrenstrukturierungen und zahlreichen Gefahren mit typischen, beispielhaften Lösungsmethoden wie Höhere Gewalt; Fehlplanung, Fehlfunktion, Fehlhandlung, Missbrauch; Ausfall, Diebstahl / Verlust / Zerstörung von Geräten, Datenträgern, Dokumenten; Social Engineering mit Social Hacking, Phishing, Vishing, Smishing, Spear-Phishing, CEO-Fraud, Whaling; Soziale Netze; Identitätsmissbrauch, Erpressung, Korruption; Passwort-Angriffe (Abschauen, Cracken,



Credential-Stuffing, ...); Unbefugtes Eindringen, Exploits-, Script-, Buffer-Overflow-Attacken; Lauschangriffe / Datendiebstahl, Hoaxes und Malware mit Virus, Wurm, Scareware, Spyware, Ransomware, Kryptominer, Adware, Malvertising, Trojaner, Blended Malware; Angriffe auf Verschlüsselung (Brute-Force, Man-in-the-Middle); Denial-of-Service-Attacken (DoS, DDoS, Defacement, Botnetze, ...) und Web-basierte Angriffe (Webserver Poisoning, CrossSite-Scripting, ...).

### **Gesamtzusammenfassung:**

zu Informationssicherheit und zu den zehn wichtigsten Schutzmaßnahmen

## **C) Prüfungsregelungen**

**(wie wird gemessen, ob Teilnehmer das Qualifikationsniveau haben)**

### **Gegenstand**

In einer Prüfung wird festgestellt, ob der Teilnehmer das Qualifikationsniveau erfüllt.

### **Anmeldung**

Die Anmeldung erfolgt in einer eigenständigen Prüfungsanmeldung.

### **Rücktritt**

Will ein Teilnehmer an der Prüfung nicht teilnehmen, so hat er dies vor Beginn der Prüfung, spätestens am Anfang der Prüfung, dem Prüfer mitzuteilen. In diesem Fall gilt die Prüfung als nicht durchgeführt.

Tritt ein Teilnehmer ansonsten nach Beginn der Prüfung zurück, so gilt die Prüfung als nicht bestanden.

### **Identitätsnachweis**

Der Prüfling muss sich vor Prüfungsbeginn mit einem gültigen Lichtbildausweis ausweisen.

### **Termin, Ort, Form, Dauer, Sprache**

Die Prüfung erfolgt als eigenständige Prüfung.

Termin und Ort gemäß Ankündigung bzw. Vereinbarung.

Der Prüfling sollte sich rechtzeitig vor dem angesetzten Prüfungszeitpunkt einfinden.

Bei verspäteten Eintreffen kann der Zutritt und die Teilnahme durch den Prüfer verweigert werden.

Die Prüfung dauert 45 Minuten. Die Prüfungszeit läuft während der Abwesenheit des Prüflings (z.B. beim Aufsuchen der Toiletten) weiter. Zusätzliche Zeit wird nicht gewährt.

Dazu werden Fragebögen ausgeteilt und von jedem Teilnehmer eigenständig, ohne Hilfsmittel und schriftlich beantwortet und an den Prüfer zurückgegeben.

Die Prüfung erfolgt in deutscher Sprache.

### **Online-Prüfung:**

Zur geeigneten Beaufsichtigung hat der Teilnehmer das von der DresPleier GmbH eingesetzte Videokonferenz-System zu nutzen und die Übertragung von Bild (Video mit sichtbarem Teilnehmer), Ton (Audio) und Monitor (Desktop-Teilen) zu aktivieren. Die Prüfung hat daher als Einzelprüfung zu erfolgen und das Equipment des Teilnehmers muss dies ermöglichen.

Ablauf: Zur Prüfung des Raums auf unerlaubte Hilfsmittel ist vor der Prüfung ein Mal 360 Grad mit der Kamera durch den Raum zu schwenken. Der Teilnehmer erscheint 15 Minuten vor Prüfungsbeginn, schaltet das Videokonferenz-System zur Ansicht frei und weist sich über gültigen Lichtbildausweis aus. Zum Prüfungsbeginn bekommt er die Prüfungsfragen per Mail zugesendet im Open Document Format (ODT für Textdokumente). Er beantwortet die Fragen direkt im Dokument durch Ankreuzen. Zum Ende speichert er das Dokument als PDF ab und sendet es sofort per Mail als PDF an den Prüfer zurück. Zusenden, PDF-Speichern und Zurücksenden erfolgen außerhalb der Prüfungs-



zeit. Ein Austreten während der Prüfung ist nur zeitlich begrenzt (wenige Minuten) gestattet. Bei gravierenden technischen Störungen wird die Prüfung abgebrochen und kostenlos wiederholt.

### **Fragen, Bewertung**

Zu den Themenfeldern ist ein Fragenpool erstellt mit mindestens 100 Fragen, die alle Themenfelder abdecken und mit Ja oder Nein zu beantworten sind. Zu den einzelnen Themenfeldern sollten folgende Anzahl von Fragen im Fragenpool enthalten sein: Grundlagen 14, Management 20, Prinzipien, Methoden, Maßnahmen 28, Gefahren und Lösungen 28, Gesamtzusammenfassung 10. Zur Prüfung werden daraus per Zufall die jeweilige Anzahl an Fragen gemäß den Themenfeldern ausgewählt: Grundlagen 7, Management 10, Prinzipien, Methoden, Maßnahmen 14, Gefahren und Lösungen 14, Gesamtzusammenfassung 5, damit insgesamt 50 Fragen.

Zum Bestehen der Prüfung müssen 50%, also 25 Fragen korrekt beantwortet sein, jede korrekt beantwortete Frage wird gewertet, jede nicht korrekt beantwortete nicht.

### **Hilfsmittel**

Der Prüfling darf zur Beantwortung der Fragen keinerlei Hilfsmittel benutzen, sondern muss diese eigenständig beantworten.

### **Betrug, Störung**

Im Falle eines Betrugs dokumentiert der Prüfer dies und entscheidet je nach Bedeutung des Vorfalls über eine Verwarnung oder den Ausschluss aus der Prüfung. Bei einem Ausschluss gilt die Prüfung als nicht bestanden. Werden Verstöße nach der Prüfung festgestellt, so kann ein ausgestelltes Personenzertifikat widerrufen werden.

Stört ein Teilnehmer die Prüfung, so kann er von der Prüfung ersatzlos ausgeschlossen werden. Die Prüfung gilt dann als nicht bestanden.

### **Einsicht, Wiederholung**

Ist die Prüfung nicht bestanden, so kann der Teilnehmer auf Antrag eine Prüfungseinsicht nach Abstimmung mit der DresPleier GmbH vornehmen. Anfallende Kosten hat der Teilnehmer zu erstatten.

Eine nicht bestandene Prüfung kann wiederholt werden.

Dazu ist eine Prüfung mit entsprechenden Kosten zu buchen.

## **D) Zertifikat**

**(wie wird das Qualifikationsniveau bestätigt)**

### **Ausstellung**

Die Prüfung wird zeitnah ausgewertet.

Bei einer erfolgreichen Prüfung wird dem Teilnehmer ein Personenzertifikat als Bestätigung mit der Post zugesendet. Ansonsten wird der Teilnehmer über das Nichtbestehen informiert.

### **Inhalte**

Das Personenzertifikat enthält:

- Familienname, Vorname(n), ggf. Titel, Geburtsdatum
- Bezeichnung
- Qualifikationsniveau (der Umfang an Unterrichtseinheiten ist dabei nur angegeben, wenn diese auch konkret in einem Online-Seminar absolviert werden)
- Prüfungsdatum und Prädikat "mit Erfolg bestanden"
- Gültigkeitsdauer des Zertifikats
- Bei Rezertifizierung eines von der DresPleier GmbH ausgestellten Zertifikats Angaben zum Zertifizierungszeitraum



## Verwendung

Das Personenzertifikat darf nur in der ausgestellten Form verwendet werden.  
Es darf nicht verändert, in Teilen oder in täuschender Absicht genutzt werden.  
Im Falle von Missbrauch kann das Personenzertifikat nachträglich widerrufen werden.

## Dauer, Rezertifizierung

Das Personenzertifikat hat eine zeitlich begrenzte Gültigkeit,  
da es die Aktualität einer Qualifikation bestätigt.  
Das Personenzertifikat hat eine Gültigkeit von fünf Jahren ab dem Zeitpunkt der Prüfung.  
Eine Rezertifizierung ist möglich. Dazu ist eine Prüfung mit entsprechenden Kosten zu buchen  
und erfolgreich zu absolvieren.

## Widerruf

Wird ein Personenzertifikat vom Aussteller widerrufen, so ist dies vom Zertifikatsinhaber  
unverzüglich auf dessen Kosten an den Aussteller im Original per Post zuzusenden und  
darf dieses vom Zertifikatsinhaber nicht weiter verwendet werden.

## E) Sonstiges

(was ist zudem relevant)

### Aufbewahrungsfrist

Prüfungsunterlagen werden 1 Jahr lang aufbewahrt,  
Informationen zum Zertifikat für die Gültigkeitsdauer des Zertifikats.

### Inkrafttreten

Die Zertifizierungsordnung tritt am 16.05.2024 in Kraft  
und ersetzt alle früheren Zertifizierungsordnungen.

Die Geschäftsführung

---

**Firma:** DresPleier GmbH ; **Geschäftsführer:** Dr. Christoph Pleier ; **Sitz und Registergericht:** Landshut HRB 6587 ; **USt-ID:** DE814347435  
**Anschrift:** Vils 8, 84149 Velden ; **Telefon:** 08742/5870894 ; **Telefax:** 03222/4170655 ; **Mail:** info@DresPleier.de ; **Web:** www.DresPleier.de

Copyright © DresPleier GmbH. Alle Rechte vorbehalten. Irrtümer und Änderungen vorbehalten. Angebote der DresPleier GmbH sind stets freibleibend und unverbindlich und werden erst durch die schriftliche Bestätigung (auch per Mail) für die DresPleier GmbH verbindlich. Informationen zum Datenschutz und zur geschützten Kommunikation siehe [www.DresPleier.de](http://www.DresPleier.de)