

Prüfungsordnung für die Prüfung zu zertifizierten fachkundigen IT-Sicherheitsbeauftragten der udis Ulmer Akademie für Datenschutz und IT-Sicherheit gGmbH

§1 Geltungsbereich

Diese Prüfungsordnung gilt für die Prüfung zum fachkundigen IT-Sicherheitsbeauftragten bei udis, der Ulmer Akademie für Datenschutz und IT-Sicherheit gGmbH (im Folgenden udis genannt). Sie basiert auf einem von international anerkannten Fachleuten auf dem Gebiet der IT-Sicherheit speziell für diese Ausbildung entwickelten Fächerkanon (siehe Anlage).

§2 Voraussetzung für die Zulassung zur Prüfung

(1) Voraussetzung für die Zulassung zur Prüfung ist ein Nachweis einer hinreichenden Vorbereitung auf die Prüfung. Dieser Nachweis wird durch Teilnahme an einem von der udis anerkannten Seminar mit den Inhalten des Kanons der Ausbildung zu zertifizierten fachkundigen IT-Sicherheitsbeauftragten bei udis erbracht. Die Teilnahme hat an allen Tagen dieses Seminars zu erfolgen. Über die Teilnahme wird eine Anwesenheitsliste geführt. Wird die Ausbildung ganz oder teilweise als Online-Seminar durchgeführt, weisen die Teilnehmenden zu diesen Zeiten ihre Anwesenheit über die Kamera ihres Teilnahmegeräts nach. Die an einer solchen Online-Veranstaltung Teilnehmenden sind schriftlich darauf hinzuweisen.

(2) Von dem Erfordernis nach Abs. 1 kann udis absehen, wenn der Bewerber aufgrund langjähriger Berufstätigkeit oder durch eine entsprechende Ausbildung oder Fortbildung ausreichende Kenntnisse auf dem Fachgebiet der IT-Sicherheit nachweist.

(3) Es werden Prüfungsgebühren erhoben. Die Prüfungsgebühren sind in den Seminargebühren enthalten. Für Wiederholungsprüfungen sind gesonderte Prüfungsgebühren zu entrichten.

(4) Prüfungsleistungen können erst erbracht werden, wenn die Prüfungsgebühr entrichtet ist.

§3 Prüfungsleistungen

(1) Die Fächer, in denen Prüfungsleistungen zu erbringen sind, sowie die Art der zu erbringenden Prüfungsleistungen ergeben sich aus dem Fächerkanon der Ausbildung.

(2) Prüfer im Seminar sind die Angehörigen des Lehrkörpers, die bei der Vorbereitung auf die Prüfung die entsprechende Lehrveranstaltung eigenverantwortlich durchführen. Im Verhinderungsfall entscheidet der Prüfungsausschuss, wer Prüfer ist.

(3) Termine für die Erbringung von Prüfungsleistungen werden vom Prüfungsausschuss festgelegt und spätestens vier Wochen vorher bekannt gegeben.

(4) Prüfungen können in geeigneten Fällen auch mit Unterstützung elektronischer Medien und in elektronischer Dokumentation durchgeführt werden.

(5) Wenn es in Fällen höherer Gewalt udis unmöglich ist, die Prüfungsleistung in der vorgesehenen Form zu erbringen, kann die Anerkennung gleichwertiger Prüfungsleistungen an ihre Stelle treten.

§4 Prüfungsausschuss

(1) udis richtet für die Durchführung der Prüfung jeweils einen eigenen Prüfungsausschuss ein. Dem Prüfungsausschuss gehören als Mitglieder die Lehrkräfte an, die auf die Prüfung mit ihren Lehrveranstaltungen vorbereiten

(2) Der wissenschaftliche Leiter von udis ist in jedem Falle Mitglied und Vorsitzender des Prüfungsausschusses. Der Prüfungsausschuss hat folgende Aufgaben:

1. Beschlussfassung über Organisation und Durchführung der Prüfungsleistungen.
2. Entscheidungen über Härtefälle nach § 6 Abs. 2.
3. Entscheidung über Täuschung und Ordnungsverstoß nach § 8 Abs.1.
4. Entscheidung über Versäumnis und Rücktritt nach § 8 Abs. 2.
5. Entscheidung über die Ungültigkeit des Zeugnisses nach § 11 Abs. 1 und 2.

(3) Der Prüfungsausschuss kann einzelne Aufgaben seinem Vorsitzenden übertragen.

(4) Der Prüfungsausschuss ist beschlussfähig, wenn mindestens die Hälfte seiner Mitglieder an einer Abstimmung teilnehmen. Der Prüfungsausschuss kann seine Beschlüsse auch im Umlaufverfahren fassen.

§5 Bewertung von Prüfungsleistungen

(1) Eine schriftliche Prüfungsleistung wird in den Themenbereichen erbracht, die sich aus dem Fächerkanon der Ausbildung bei udis ergeben.

(2) Die einzelnen Prüfungsleistungen werden von dem jeweiligen Prüfer nach § 3 Abs.1 bzw. § 4 Abs.4 Nr. 2 bewertet. Für die Bewertung der einzelnen Prüfungsleistungen sind die folgenden Noten zu verwenden:

1,0 und 1,3	= sehr gut = eine besonders hervorragende Leistung;
1,7, 2,0 und 2,3	= gut = eine erheblich über dem Durchschnitt liegende Leistung;
2,7, 3,0 und 3,3	= befriedigend = eine Leistung, die in jeder Hinsicht durchschnittlichen Anforderungen entspricht;
3,7 und 4,0	= ausreichend = eine Leistung, die trotz ihrer Mängel durchschnittlichen Anforderungen entspricht;
5,0	= nicht ausreichend = eine Leistung mit erheblichen Mängeln

(3) Eine Prüfungsleistung bzw. Einzelleistung ist erbracht, wenn mindestens die Note "ausreichend" (4,0) erreicht wurde.

(4) Besteht eine Prüfungsleistung aus mehreren Einzelleistungen, so werden zur Ermittlung der Note der Prüfungsleistung die Noten der Einzelleistungen entsprechend ihrem Anteil an der jeweiligen Prüfungsleistung gewichtet und gemittelt.

(5) Bei der Berechnung der Gesamtnote für das Zeugnis werden die Prüfungsleistungen gemittelt und das Notenmittel auf die nächstliegende Note im Sinne von Abs. 3 aufgerundet bzw. abgerundet. Hierbei wird 1,5 zu 1,7, 2,5 zu 2,7 und 3,5 zu 3,7.

§6 Wiederholung von Prüfungsleistungen

(1) Nicht bestandene Prüfungsleistungen können einmal wiederholt werden. Die Wiederholung muss zum festgelegten Termin innerhalb einer Jahresfrist erfolgen.

(2) In besonderen Härtefällen kann der Prüfungsausschuss auf Antrag des Kandidaten eine zweite Wiederholung von Prüfungsleistungen genehmigen.

(3) Ein besonderer Härtefall liegt nur vor, wenn der Kandidat die Gründe für das Nichtbestehen der Wiederholungsprüfung nicht zu vertreten hat und wenn seine bisherigen Leistungen insgesamt die Erwartung begründen, dass er die Prüfung erfolgreich abschließen kann. Anträge auf Anerkennung von Härtefällen bei Nichtbestehen der Wiederholungsprüfung müssen mit allen Beweismitteln spätestens 4 Wochen nach Bekanntgabe des Prüfungsergebnisses beim Vorsitzenden des Prüfungsausschusses eingegangen sein (Ausschlussfrist).

(4) Eine dritte Wiederholung einer Prüfungsleistung ist ausgeschlossen.

(5) Die Wiederholung einer bereits erfolgreich erbrachten Prüfungsleistung ist nicht möglich.

§7 Erlöschen der Zulassung zur Prüfung und des Prüfungsanspruches

(1) Der Prüfungsanspruch erlischt, wenn ein Kandidat

1. die Prüfung nicht innerhalb von 1 Jahr nach Ende des Seminars erfolgreich abgeschlossen hat oder
2. eine Prüfungsleistung endgültig nicht bestanden hat.

(2) In Härtefällen kann der Prüfungsausschuss Ausnahmen von Absatz 1 Nr. 1 zulassen.

§8 Täuschung und Ordnungsverstoß

(1) Versucht ein Kandidat das Ergebnis seiner Prüfungsleistung oder das eines anderen Kandidaten durch Täuschung oder Benutzung nicht zugelassener Hilfsmittel zu beeinflussen oder führt er nach Bekanntgabe der Aufgaben nicht zugelassene Hilfsmittel mit sich, so gilt die betreffende Prüfungsleistung als "nicht bestanden"; die Feststellung trifft der Prüfungsausschuss auf Bericht des zuständigen Prüfers oder Aufsichtsführenden.

(2) Ein Kandidat, der sich eines Verstoßes gegen die Ordnung der Prüfung schuldig gemacht hat, kann von dem jeweiligen Prüfer oder Aufsichtsführenden von der Fortsetzung der Prüfungsleistung ausgeschlossen werden; in diesem Fall gilt die betreffende Prüfungsleistung als "nicht bestanden".

§9 Versäumnis und Rücktritt

(1) Eine Prüfungsleistung gilt als "nicht bestanden", wenn der Kandidat zu einem Prüfungstermin ohne triftige Gründe nicht erscheint, oder wenn er nach der Anmeldung ohne triftige Gründe zurücktritt.

(2) Die Gründe für ein Versäumnis oder einen Rücktritt müssen dem Vorsitzenden des Prüfungsausschusses unverzüglich schriftlich angezeigt und glaubhaft gemacht werden. Bei Krankheit hat der Kandidat ein ärztliches Attest über die Prüfungsunfähigkeit vorzulegen. Spätestens 4 Wochen nach dem Versäumnis oder Rücktritt (Ausschlussfrist) müssen die schriftliche Begründung und die Beweismittel beim Vorsitzenden des Prüfungsausschusses eingegangen sein. Über die Anerkennung der Gründe entscheidet der Prüfungsausschuss

(3) Ablehnende Entscheidungen des Prüfungsausschusses sind dem Kandidaten schriftlich mitzuteilen.

§10 Zeugnis

(1) Hat ein Kandidat alle Prüfungsleistungen erfolgreich erbracht, so ist die Prüfung abgeschlossen. Über die Ergebnisse wird ein Zeugnis ausgestellt.

(2) Das Zeugnis wird vom wissenschaftlichen Leiter der udis Ulmer Akademie für Datenschutz und IT-Sicherheit gGmbH und vom Seminarleiter bzw. einem weiteren Prüfer im Sinne von § 3 Abs. 2 unterzeichnet und mit dem Siegel der udis versehen.

(3) Das Zeugnis bescheinigt, dass die Teilnehmerin / der Teilnehmer die zur Ausübung der Tätigkeit einer / eines IT-Sicherheitsbeauftragten (IT-Security-Manager) gehörende Fachkunde besitzt.

§11 Ungültigkeit des Zeugnisses

(1) Hat der Kandidat bei einer Prüfungsleistung getäuscht und wird diese Tatsache erst nach der Aushändigung des Zeugnisses bekannt, so kann der Prüfungsausschuss nachträglich die Prüfung ganz oder teilweise für "nicht bestanden" erklären.

(2) Waren die Voraussetzungen für die Zulassung zu einer Prüfungsleistung nicht erfüllt und wird diese Tatsache erst nach der Erbringung der Prüfungsleistung bekannt, kann der Prüfungsausschuss die ergangene Prüfungsentscheidung zurücknehmen und aussprechen, dass die Prüfungsleistung nicht erfolgreich erbracht wurde.

(3) Dem Kandidaten ist vor einer Entscheidung Gelegenheit zur Äußerung zu geben.

(4) Das unrichtige Zeugnis ist einzuziehen. Eine Entscheidung nach Abs. 1 und Abs. 2 ist nach einer Frist von 5 Jahren ab dem Datum des Zeugnisses ausgeschlossen.

§12 Aufbewahrung der Prüfungsunterlagen und Akteneinsicht

(1) Die schriftlichen Prüfungsleistungen werden fünf Jahre ab der letzten Prüfungsleistung bei udis oder beim Prüfer gem. §3 Abs. 2 aufbewahrt.

(2) Der Kandidat kann bei den Prüfungsberechtigten die Einsichtnahme in seine schriftlichen Prüfungsleistungen beantragen; der Antrag muss spätestens 4 Wochen nach Bekanntgabe des Ergebnisses der betreffenden Prüfungsleistung gestellt werden.

§13 Inkrafttreten

Diese Prüfungsordnung tritt am 10. März 2022 in Kraft.

.....
Prof. Dr. Gerhard Kongehl
Geschäftsführer und wissenschaftliche Leiter
der udis Ulmer Akademie für Datenschutz
und IT-Sicherheit gGmbH

Fächerkanon
der Ausbildung zu zertifizierten fachkundigen IT-Sicherheitsbeauftragten
(IT-Security-Manager)
der udis Ulmer Akademie für Datenschutz und IT-Sicherheit gGmbH

Block 1

Einführung und Sicherheitsziele (1 Tag)

Motivation, einleitende Beispiele, grundlegende Begriffe, CIA Sicherheitsziele, Kursüberblick

Einführung Kryptografie (1 Tag)

Symmetrische und asymmetrische Verschlüsselung, AES, RSA, diskreter Logarithmus, Zufallszahlen, Hashfunktionen, Signaturen, Sicherheitsbewertung von Kryptografie

Authentifizierung und Zugriffskontrolle (2 Tage)

Klassifikation Authentifikation, Mehrfaktor-Authentifizierung, Passwörter, Challenge- Response Verfahren, Authentifizierungstokens, Biometrie, Privacy-erhaltende Authentifizierung, Zugriffskontrollmodelle, Discretionary und Mandatory Access Control, Zugriffskontrollmatrix, Role Based Access Control, Attribute Based Access Control, Bell-La Padula Modell, Umsetzung in Betriebssystemen, OAuth, XACML

Anwendungsfall: Web Security (1 Tag)

Grundbegriffe, Kategorisierung nach WASC-TC, Angriffsvektoren im World-Wide-Web, Attack-Trees, Sicherheitstests und Risikoanalyse von Webservern

Benutzbare Lösungen für IT-Sicherheit und Datenschutz (1 Tag)

Usability- und HCI-Grundlagen, verhaltenspsychologische Grundlagen, Eigenschaften gut benutzbarer Sicherheitslösungen, Usability-Aspekte ausgewählter Security-Mechanismen wie z.B. von Passwörtern, Benutzbare Lösungen für den Datenschutz, Organisationsstrukturen für benutzbare Sicherheit

Block 2

IT-, Datenschutz- und Softwarerecht (2 Tage)

IT- und Softwarerecht, gesetzlicher Schutz von geistigem Eigentum, Einsatz von Open- Source-Software (OSS), IT-Vertragsrecht, IT-Strafrecht, IT-Sicherheits- und Datenschutzrecht, rechtliche Aspekte der IT- und Datensicherheit, Datenschutzrecht, Rolle des IT-Sicherheitsbeauftragten, zivilrechtliche Verantwortlichkeit, kritische Infrastrukturen

Betriebssystem- und Netzwerksicherheit (2 Tage)

Bedrohungen, Schwachstellen in Systemen, Hacker-Community, netzbasierte Angriffe, Einfluss der Komplexität, Architektur sicherer Betriebssysteme, Isolation, Sicherheitstechniken in Betriebssystemen, Einsatzszenarien sicherer Systeme, Firewalls, Intrusion Detection, Inhaltsfilterung, Virenschutz, mobile Netzkomponenten, Zugriff auf Cloud-Dienste, Schwachstellenanalyse

Block 2 (Fortsetzung)

Malware (1 Tag)

Kategorien von Malware, Virus, Wurm, Trojaner, Infektionswege, Schadroutinen, Phishing, Botnetze, Ransomware und Kryptotrojaner, Schutz vor Malware

Anwendungsfall: Embedded und Wireless Security (1 Tag)

Wireless Security, 802.11 Sicherheit, Bluetooth und Bluetooth Low Energy, NFC, embedded controller und embedded Prozessoren, Smartcards, Hardware Security, Secure Boot, iOS Secure Data Storage

Block 3

Sicherheitsmanagement und Auditierung (2 Tage)

ISMS, ISO-27001, IT-Grundschutz, BSI-Standards, KOMPENDIUM-Vorgehensweise, Risikoanalyse, ISMS aus Auditoren-Sicht, Vollständigkeit, Nachweisbarkeit, Wirksamkeit, ISMS aus Teamleiter-Sicht, Aufgaben und Methoden, KPIs und Wirksamkeitsziele, Auswahl von Risikoanalysemethoden, ISMS-Tools, Praxistipps

Penetration-Testing und Hacking Lab (2 Tage)

Security Assessment, Assessmentarten und deren Abgrenzung, Ablauf und Durchführung, Vorbereitungsphase, initialer Angriff, weiterführende Angriffe, Dokumentation von Security Assessments, Nachbereitung, Web Application Security Assessment, Pentesting Lab, Port-Scans, Schwachstellensuche, Exploitation, Mobile Application Security Assessment, Cloud Security Assessment, Embedded Security Assessment, Social Engineering

Fachkunde-Prüfung (ca. 3,5 Stunden)