ECDL IT-Sicherheit 2.0 mit Windows 11				
Kategorie	***Fähigkeit***	***Ref.***	***Aufgabe***	***Kapitel im Lehrmittel***
1 Grundbegriffe zu Sicherheit	1.1 Datenbedrohung	1.1.1	Zwischen Daten und Informationen unterscheiden können	2.1.1 Zwischen Daten und Informationen unterscheiden 2.1.2 Datenund Informationen
		1.1.2	Den Begriff Cybercrime und Hacken verstehen	2.1.3 Cybercrime (Computerkriminalität) 2.1.4 Hacking, Cracking verstehen
		1.1.3	Böswillige und unabsichtliche Bedrohung für Daten durch Einzelpersonen, Dienstleister und externe Organisationen kennen.	2.1.7 Menschliche Fehler 2.2.1 Schutz der persönlichen Daten
		1.1.4	Bedrohung für Daten durch höhere Gewalt kennen, wie: Feuer, Hochwasser, Krieg, Erdbeben	2.1.5 Bedrohung für Daten durch höhere Gewalt
		1.1.5	Bedrohung für Daten durch die Verwendung von Cloud-Computing kennen, wie: Datenkontrolle, möglicher Verlust der Privatsphäre.	2.1.6 Bedrohung für Daten durch die Cloud
	1.2 Wert von Informationen	1.2.1	Grundlegende Merkmale von Datensicherheit verstehen, wie: Vertraulichkeit, Integrität, Verfügbarkeit.	2.2.2 Sensible Firmendaten schützen
		1.2.2	Verstehen, weshalb personenbezogene Daten zu schützen sind, z. B. um Identitätsdiebstahl und Betrug zu verhindern, zum Schutz der Privatsphäre.	2.2.1 Schutz der persönlichen Daten
		1.2.3	Verstehen, weshalb Firmendaten auf Computern und mobilen Geräten zu schützen sind, z. B. um Diebstahl, betrügerische Verwendung, unabsichtlichen Datenverlust und Sabotage zu verhindern.	2.2.2 Sensible Firmendaten schützen
		1.2.4	Allgemeine Grundsätze für Datenschutz/Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle kennen, wie: Transparenz, Notwendigkeit, Verhältnismäßigkeit.	2.2.5 Allgemeine Grundsätze für Datenschutz
		1.2.5	Die Begriffe betroffene Personen und Inhaber der Datensammlung verstehen. Verstehen, wie die Grundsätze für Datenschutz/ Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle für Betroffene und Auftraggeber angewendet werden.	2.2.3 Rechtliche Grundlagen für Datenschutz 2.2.5 Allgemeine Grundsätze für Datenschutz
		1.2.6	Verstehen, dass bei der Nutzung von IKT die Einhaltung von Grundsätzen und Richtlinien wichtig ist; wissen, wie die Richtlinien üblicherweise bekanntgemacht werden bzw. zugänglich sind.	2.2.4 Sicherheitsstrategien und Richtlinien
	1.3 Persönliche Sicherheit	1.3.1	Den Begriff Social Engineering verstehen und die Ziele kennen, wie: unberechtigter Zugriff auf Computer und mobile Geräte, unerlaubtes Sammeln von Informationen, Betrug.	2.3.1 Social Engineering
		1.3.2	Methoden des Social Engineering kennen, wie: Telefonanrufe, Phishing, Shoulder Surfing	2.3.1 Social Engineering
		1.3.3	Den Begriff Identitätsdiebstahl verstehen und die Folgen von Identitätsmissbrauch in persönlicher, finanzieller, geschäftlicher und rechtlicher Hinsicht kennen	2.3.2 Identitätsdiebstahl und Identitätsmissbrauch
		1.3.4	Methoden des Identitätsdiebstahls kennen, wie: Information Diving, Skimming, Pretexting	2.3.3 Methoden des Identitätsdiebstahls
	1.4 Sicherheit für Dateien	1.4.1	Die Auswirkung von aktivierten und deaktivierten Makro-Sicherheitseinstellungen verstehen	2.4.1 Makro-Sicherheitseinstellungen verstehen 2.4.2 Makrosicherheitseinstellungen und ihre Auswirkungen
		1.4.2	Die Vorteile und die Grenzen von Verschlüsselung verstehen. Wissen, wie wichtig es ist, das Passwort, den Schlüssel und das Zertifikat der Verschlüsselung nicht offenzulegen und nicht zu verlieren.	2.4.1 Vorteile und Grenzen der Daten-Verschlüsselung
		1.4.3	Eine Datei, einen Ordner oder ein Laufwerk verschlüsseln.	2.4.2 Datei, Ordner oder Laufwerk verschlüsseln
		1.4.4	Dateien mit einem Passwort schützen, z. B.: Dokumente, Tabellenkalkulationsdateien, komprimierte Dateien.	2.4.3 Dateien mit einem Passwort schützen

ECDL IT-Sicherheit 2.0 mit Windows 11				
Kategorie	***Fähigkeit***	***Ref.***	***Aufgabe***	***Kapitel im Lehrmittel***
2 Malware	2.1 Arten und Funktionsweise	2.1.1	Den Begriff Malware verstehen; verschiedene Möglichkeiten kennen, wie Malware auf Computern und anderen Geräten verborgen werden kann, wie: Trojaner, Rootkit, Backdoor.	3.1 Definition und Funktionsweise
		2.1.2	Arten von sich selbst verbreitender Malware kennen und ihre Funktionsweise verstehen, wie: Virus, Wurm.	3.1 Definition und Funktionsweise
		2.1.3	Arten von Malware und ihre Funktionsweise für Datendiebstahl, Betrug oder Erpressung kennen, wie: Adware, Ransomware, Spyware, Botnet, Keylogger, Dialer.	3.1.2 Möglichkeiten zum Verbergen von Malware 3.1.3 Malware-Typen
	2.2 Schutz	2.2.1	Die Funktionsweise und die Grenzen von Antiviren-Software verstehen	3.2.1 Funktionsweise und Grenzen von Antiviren-Software
		2.2.2	Verstehen, dass Antiviren-Software auf Computern und mobilen Geräten installiert sein soll.	3.2 Schutz vor Malware
		2.2.3	Die Bedeutung von regelmäßigen Software-Updates für Antiviren-Software, Web-Browser, Plug-ins, Anwendungsprogramme, Betriebssysteme verstehen.	3.2 Schutz vor Malware 3.2.3 Software-Updates und Virensignaturen
		2.2.4	Laufwerke, Ordner und Dateien mit Antiviren-Software scannen; Zeitplan für Scans mit Antiviren-Software festlegen.	3.2.2 Antiviren-Software verwenden
		2.2.5	Verstehen, dass die Verwendung veralteter und nicht mehr unterstützter Software mit Risiken verbunden ist, wie: zunehmende Gefährdung durch Malware, Inkompatibilität.	3.2 Schutz vor Malware
	2.3 Problemlösung und Behebung	2.3.1	Den Begriff Quarantäne verstehen und die Auswirkung auf infizierte oder verdächtige Dateien kennen.	3.2.2 Antiviren-Software verwenden
		2.3.2	Infizierte oder verdächtige Dateien unter Quarantäne stellen oder löschen.	3.2.2 Antiviren-Software verwenden
		2.3.3	Wissen, dass ein Malware-Angriff mithilfe von Online-Ressourcen identifiziert und bekämpft werden kann, wie: Websites der Anbieter von Betriebssystemen, Antiviren-Software und Web-Browser; Websites von zuständigen Behörden/Organisationen.	3.2 Schutz vor Malware
3 Sicherheit im Netzwerk	3.1 Netzwerke und Verbindungen	3.1.1	Den Begriff Netzwerk verstehen und übliche Netzwerktypen kennen, wie: Local Area Network (LAN), Wireless Local Area Network (WLAN), Wide Area Network (WAN), Virtual Private Network (VPN).	4.1 Netzwerke 4.1.1 Netwerktypen
		3.1.2	Verstehen, wodurch sich eine Verbindung zu einem Netzwerk auf die Sicherheit auswirken kann, wie: Malware, unberechtigter Zugriff auf Daten, Schutz der Privatsphäre.	4.1.1 Netzwerktypen 4.1.2 Aufgaben der Netzwerk-Administration
		3.1.3	Die Aufgaben der Netzwerk-Administration verstehen, wie: Authentifizierung, Benutzerrechte verwalten, Nutzung dokumentieren, sicherheitsrelevante Patches und Updates überwachen und installieren, Netzwerkverkehr überwachen, Malware im Netzwerk bekämpfen.	4.1.2 Aufgaben der netzwerk-Administration
		3.1.4	Die Funktion und die Grenzen einer Firewall bei der privaten Computernutzung und in einer Arbeitsumgebung verstehen.	4.2.1 Funktion und Grenzen einer Firewall
		3.1.5	Personal Firewall ein- und ausschalten; den durch die Personal Firewall laufenden Datenverkehr für eine Anwendung, einen Dienst/Funktion zulassen bzw. blockieren.	4.2.1 Funktion und Grenzen einer Firewall
	3.2 Sicherheit im drahtlosen Netz	3.2.1	Verschiedene Möglichkeiten zum Schutz von drahtlosen Netzwerken und deren Grenzen kennen, wie: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA)/Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC) Filter, Service Set Identifier (SSID) verbergen.	4.4.1 Drahtlose Netzwerke mit Passwort schützen 4.4.2 Verfahren zum Schutz von drahtlosen Netzwerken
		3.2.2	Sich bewusst sein, dass auf ein ungeschütztes drahtloses Netzwerk Angriffe erfolgen können, wie: unbefugter Zugriff durch Eindringlinge, Hijacking, Man-in-the-Middle-Angriff.	4.4 Sicherheit im drathlosen Netz
		3.2.3	Den Begriff Persönlicher Hotspot verstehen.	4.4.5 Persönlicher Hotspot
		3.2.4	Einen sicheren persönlichen Hotspot einschalten und ausschalten; Geräte sicher damit verbinden und trennen.	4.4.4 Verbindung zu einem drathlosen netzwerk herstellen 4.4.5 Persönlicher Hotspot

ECDL IT-Sicherheit 2.0 mit Windows 11				
Kategorie	***Fähigkeit***	***Ref.***	***Aufgabe***	***Kapitel im Lehrmittel***
4 Zugriffs-kontrolle	4.1 Methoden	4.1.1	Maßnahmen kennen, um unberechtigten Zugriff auf Daten zu verhindern, wie: Benutzername, Passwort, PIN, Verschlüsselung, Multi-Faktor-Authentifizierung.	4.5 Zugriffskontrolle
		4.1.2	Den Begriff Einmal-Passwort und die typische Verwendung verstehen.	5.1.4 Einmal-Kennwort
		4.1.3	Verstehen, wozu ein Netzwerk-Konto dient.	4.5.1 Anmeldung mit Benutzername und Passwort
		4.1.4	Verstehen, dass der Zugang zu einem Netzwerk-Konto mit Benutzername und Passwort erfolgen soll, und dass der Zugang bei Nichtgebrauch durch Sperren oder Abmelden geschlossen werden soll.	4.5.1 Anmeldung mit Benutzername und Passwort
		4.1.5	Biometrische Verfahren zur Zugangskontrolle kennen, wie: Fingerabdruck, Auge scannen, Gesichtserkennung, Handgeometrie.	4.5.5 Biometrische Verfahren zur Zugangskontrolle
	4.2 Passwort-Verwaltung	4.2.1	Richtlinien für ein gutes Passwort kennen, wie: angemessene Mindestlänge beachten, aus Buchstaben und Ziffern und Sonderzeichen zusammensetzen, geheim halten, regelmäßig ändern, unterschiedliche Passwörter für unterschiedliche Dienste.	4.5.2 Richtlinien für ein gutes Passwort
		4.2.2	Die Funktion und die Grenzen einer Passwort-Verwaltungssoftware verstehen.	4.5.3 Passwort-Verwaltungssoftware
5 Sichere Web-Nutzung	5.1 Browser-Einstellungen	5.1.1	Einstellungen zum Ausfüllen von Formularen aktivieren und deaktivieren, wie: automatische Vervollständigung, automatisches Speichern.	5.1.6 Autovervollständigung für Formulareingaben ein-/ausschalten
		5.1.2	In einem Browser persönliche Daten löschen, wie: Browserverlauf, Downloadverlauf, temporäre Internetdateien, Passwörter, Cookies, Formulardaten.	5.1.7 Temporäre Internetdateien speichern und löschen 5.1.8 Cookies
	5.2 Sicheres Surfen	5.2.1	Sich bewusst sein, dass bestimmte Online-Aktivitäten (Einkaufen, E-Banking) nur auf sicheren Webseiten über eine gesicherte Netzwerkverbindung erfolgen sollen.	5.1.1 Wann brauche ich einen sicheren Webzugang? 5.1.2 Merkmale einer sicheren Website
		5.2.2	Kriterien zur Beurteilung der Vertrauenswürdigkeit einer Website kennen, wie: inhaltliche Qualität, Aktualität, gültige URL, Information zum Inhaber der Webseite (Impressum), Kontaktdaten, Sicherheitszertifikat, Überprüfung der Domain-Inhaberschaft.	4.5.2 Richtlinien für ein gutes Passwort
		5.2.3	Den Begriff Pharming verstehen.	5.1.3 Pharming
		5.2.4	Den Zweck und die Funktionsweise von Software zur Inhaltskontrolle kennen, wie: Internet-Filterprogramme, Kinderschutz-Software.	5.2 Software zur Inhaltskontrolle

ECDL IT-Sicherheit 2.0 mit Windows 11				
Kategorie	***Fähigkeit***	***Ref.***	***Aufgabe***	***Kapitel im Lehrmittel***
6 Kommuni- kation	6.1 E-Mail	6.1.1	Verstehen, weshalb eine E-Mail verschlüsselt und entschlüsselt wird	6.1.1 E-Mail-Verschlüsselung und digitale Signatur
		6.1.2	Den Begriff Digitale Signatur verstehen	6.1.1 E-Mail-Verschlüsselung und digitale Signatur
		6.1.3	Arglistige und unerwünschte E-Mails erkennen.	6.1.2 Arglistige und unerwünschte E-Mails
		6.1.4	Typische Merkmale von Phishing kennen, wie: Verwendung der Namen von seriösen Unternehmen und Personen, Verwendung von Logos und Markenzeichen, Links zu gefälschten Webseiten, Aufforderung zur Bekanntgabe persönlicher Daten.	6.1.3 Phishing und gefälschte Websites
		6.1.5	Wissen, dass Phishing-Attacken den betroffenen seriösen Unternehmen und zuständigen Behörden/Organisationen gemeldet werden können.	6.1.3 Phishing und gefälschte Websites
		6.1.6	Sich der Gefahr bewusst sein, dass ein Computer oder mobiles Gerät mit Malware infiziert werden kann, wenn ein E-Mail-Attachment geöffnet wird, das ein Makro oder eine ausführbare Datei enthält.	6.1.4 Attachments
	6.2 Soziale Netzwerke	6.2.1	Verstehen, dass es wichtig ist, vertrauliche oder personenbezogene Informationen nicht in sozialen Netzwerken zu veröffentlichen.	5.3 Soziale Netzwerke
		6.2.2	Sich der Notwendigkeit bewusst sein, in sozialen Netzwerken geeignete Konto-Einstellungen auszuwählen und regelmäßig zu überprüfen, wie: Privatsphäre, Standort.	5.3.1 Gefahren im sozialen Netzwerk
		6.2.3	Konto-Einstellungen in sozialen Netzwerken anwenden: Privatsphäre, Standort.	5.3.2 Privatsphäre schützen
		6.2.4	Mögliche Gefahren bei der Nutzung von sozialen Netzwerken kennen, wie: Cyber-Mobbing, Cyber-Grooming, bösartige Veröffentlichung persönlicher Inhalte, falsche Identitäten, betrügerische oder arglistige Links, Inhalte oder Nachrichten.	5.3.1 Gefahren im sozialen Netzwerk
		6.2.5	Wissen, dass missbräuchliche Verwendung oder Fehlverhalten in sozialen Netzwerken dem jeweiligen Service-Provider und zuständigen Behörden/Organisationen gemeldet werden kann.	5.3.1 Gefahren im sozialen Netzwerk
	6.3 VoIP und Instant Messaging	6.3.1	Schwachstellen bei der Sicherheit von Instant Messaging (IM) und Voice over Internet Protocol (VoIP) verstehen und Gefahren kennen, wie: Malware, Backdoor-Zugang, Zugriff auf Dateien, Lauschangriff.	6.2.2 Schwachstellen bei der Sicherheit von IM
		6.3.2	Methoden kennen, um beim Gebrauch von IM und VoIP Vertraulichkeit sicherzustellen, wie: Verschlüsselung, Nicht-Veröffentlichung von wichtigen Informationen, Zugriff auf Daten einschränken.	6.2.2 Schwachstellen bei der Sicherheit von IM
	6.4 Mobile Geräte	6.4.1	Verstehen, welche Folgen die Verwendung von Anwendungen aus inoffiziellen App-Stores haben kann, wie: mobile Malware, unnötiger Ressourcenverbrauch, Zugriff auf persönliche Daten, schlechte Qualität, versteckte Kosten.	6.2.3 Kommunikation auf mobilen Geräten
		6.4.2	Den Begriff App-Berechtigungen verstehen.	6.2.3 Kommunikation auf mobilen Geräten
		6.4.3	Wissen, dass mobile Anwendungen private Informationen von mobilen Geräten auslesen können, wie: Kontaktdaten, Standortverlauf, Bilder.	6.2.3 Kommunikation auf mobilen Geräten
		6.4.4	Für den Fall, dass ein mobiles Gerät abhandenkommt, Sofortmaßnahmen und Vorsichtsmaßnahmen kennen, wie: Fernsperrung, Fernlöschung, Geräteortung.	6.2.3 Kommunikation auf mobilen Geräten

ECDL IT-Sicherheit 2.0 mit Windows 11				
Kategorie	***Fähigkeit***	***Ref.***	***Aufgabe***	***Kapitel im Lehrmittel***
7 Sichere Daten-verwaltung	7.1 Daten sichern und Backups erstellen	7.1.1	Maßnahmen zur physischen Sicherung von Computern und mobilen Geräten kennen, wie: nicht unbeaufsichtigt lassen, Standort der Geräte und weitere Details aufzeichnen, Sicherungskabel verwenden, Zugangskontrolle.	7.1.1 Massnahmen zur physischen Sicherung von Geräten
		7.1.2	Wissen, wie wichtig eine Sicherungskopie für den Fall des Datenverlusts auf Computern und anderen Geräten ist.	7.1.2 Sicherungskopie (Backup)
		7.1.3	Wesentliche Merkmale eines Konzepts zur Datensicherung kennen, wie: Regelmäßigkeit/Häufigkeit, Zeitplan, Ablageort, Datenkompression.	7.1.3 Konzept zur Datensicherung
		7.1.4	Backup an einem Speicherort erstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.	7.1.4 Backup erstellen 7.1.5 Sichern wie unter Windows 7
		7.1.5	Daten von einem Backup-Speicherort wiederherstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.	7.1.4 Backup erstellen 7.1.5 Sichern wie unter Windows 7 7.1.6 Systemwiederherstellung
	7.2 Daten sicher löschen und vernichten	7.2.1	Den Unterschied zwischen der Löschung von Daten und der endgültigen Löschung/Vernichtung von Daten kennen.	7.2.2 Unterschied zwischen Löschen und Vernichten von Daten
		7.2.2	Den Sinn und Zweck einer endgültigen Löschung/Vernichtung von Daten auf Laufwerken oder Geräten verstehen.	7.2.1 Sinn einer endgültigen Vernichtung von Daten
		7.2.3	Sich bewusst sein, dass das Löschen von Inhalten bei manchen Diensten nicht endgültig ist, wie: Soziale Netzwerke, Blogs, Internetforen, Cloud-Dienste.	7.2.4 Das Löschen von Dateien in sozialen Netzwerken und Cloud-Diensten
		7.2.4	Methoden zur endgültigen Datenvernichtung kennen, wie: Laufwerke/Datenträger zerstören, z. B. schreddern; Entmagnetisierung; Software zur Datenvernichtung verwenden.	7.2.3 Methoden zur endgültigen Vernichtung von Daten