ECDL/ICDL IT Security
Moduł S3
Sylabus - wersja 1.0

Przeznaczenie Sylabusa
Dokument ten zawiera szczegółowy Sylabus dla modułu ECDL/ICDL IT Security. Sylabus opisuje zakres wiedzy i umiejętności, jakie musi opanować Kandydat. Sylabus zawiera podstawy teoretyczne do pytań i zadań egzaminacyjnych z tego modułu.

Oświadczenie
Mimo tego, że podczas opracowania powyższego dokumentu Fundacja ECDL dołożyła wszelkich starań by zawierał on wszystkie niezbędne elementy, to Fundacja ECDL, jako wydawca opracowania nie udziela gwarancji i nie bierze odpowiedzialności za ewentualne braki.
Fundacja nie bierze również odpowiedzialności za błędy, pominięcia, nieścisłości, straty lub szkody wynikające z tytułu użytkowania poniższej publikacji. Wszelkie zmiany mogą zostać dokonane przez Fundację ECDL na jej odpowiedzialność, bez konieczności zgłaszania tego faktu.

ECDL/ICDL IT Security

Moduł ten wymaga od kandydata zrozumienia głównych kwestii leżących u podstaw bezpiecznego korzystania z technologii informacyjno-komunikacyjnych (ICT) w życiu codziennym oraz umiejętności stosowania odpowiednich metod i aplikacji do zabezpieczenia połączenia sieciowego, umiejętności bezpiecznego korzystania z Internetu i umiejętności właściwego zarządzania informacjami i danymi. Reprezentatywny kandydat będzie przygotowany do bezpiecznego korzystania z ICT i stawiania czoła wyzwaniom bezpieczeństwa rzucanym przez ICT.

Założenia modułu

Aby zaliczyć moduł Kandydat musi posiadać wiedzę i umiejętności z zakresu:

- Głównych aspektów dotyczących znaczenia zabezpieczania informacji i danych.
- Środków zabezpieczania przed niepowołanym dostępem, ochrony prywatności oraz zapobiegania kradzieży tożsamości.
- Ochrony komputera i innych urządzeń oraz sieci przed złośliwym oprogramowaniem oraz nieautoryzowanym dostępem.
- Rozróżniania typów sieci i połączeń oraz różnych zabezpieczeń sieciowych, takich jak firewall.
- Bezpiecznego przeglądania zasobów WWW i komunikowania się przez Internet.
- Kwestii bezpieczeństwa związanych z komunikacją (e-mail i komunikatory) .
- Bezpiecznego rozporządzania danymi i urządzeniami, właściwego wykonywania back- up i przywracania danych.

Osoba posiadająca daną kwalifikację:

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
1 Kwestie bezpieczeństwa	*1.1 Zagrożenia dla danych*	1.1.1	Definiuje i rozróżnia pojęcia danych i informacji.
		1.1.2	Wyjaśnia pojęcie cyberprzestępczości.
		1.1.3	Rozróżnia i charakteryzuje pojęcia - hacking, cracking oraz hacking etyczny.
		1.1.4	Identyfikuje zagrożenia danych ze strony sił wyższych, takich jak: pożar, powódź, wojna i trzęsienie ziemi.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		1.1.5	Rozpoznaje możliwości zagrożenia danych ze strony pracowników, serwisantów i osób postronnych.
	1.2 Wartość informacji	1.2.1	Wskazuje przyczyny konieczności ochrony danych osobowych – zapobieganie kradzieży tożsamości i oszustwom.
		1.2.2	Wskazuje przyczyny ochrony danych o charakterze komercyjnym – zapobieganie kradzieżom, nadużywaniu danych klienta i informacji finansowych.
		1.2.3	Identyfikuje metody zabezpieczania danych przed niepowołanym dostępem – szyfrowanie i hasła.
		1.2.4	Wymienia podstawowe własności zabezpieczania informacji - poufność, integralność i dostępność.
		1.2.5	Identyfikuje wymagania i ograniczenia prawne dotyczące zabezpieczania i przetrzymywania danych.
		1.2.6	Wskazuje konieczność stosowania się do określonych norm i zasad podczas korzystania z ICT.
	1.3 Bezpieczeństwo osobiste	1.3.1	Objaśnia pojęcie socjotechnika oraz wymienia możliwe następstwa jego stosowania – information gathering (zbieranie informacji), oszustwa, pozyskiwanie dostępu do komputera i danych.
		1.3.2	Rozpoznaje metody socjotechnik, takich jak: rozmowy telefoniczne, phishing oraz podglądanie.
		1.3.3	Wyjaśnia pojęcie kradzież tożsamości oraz jej konsekwencje na polu osobistym, finansowym, biznesowym i prawnym.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		1.3.4	Rozpoznaje metody kradzieży tożsamości: information diving, skimming i pretexting.
	1.4 Bezpieczeństwo plików	1.4.1	Określa wpływ włączania i wyłączania obsługi makr na bezpieczeństwo.
		1.4.2	Nadaje hasła plikom, takim jak: dokumenty, pliki skompresowane, arkusze kalkulacyjne
		1.4.3	Wymienia zalety i ograniczenia szyfrowania.
2 Złośliwe oprogramowanie	*2.1 Definicja i funkcje*	2.1.1	Objaśnia pojęcie złośliwego oprogramowania.
		2.1.2	Rozpoznaje metody ukrywania i przenoszenia złośliwego oprogramowania: konie trojańskie, rootkity i back-door'y
	2.2 Typy	2.2.1	Rozpoznaje typy i wyjaśnia działanie infekcyjnego złośliwego oprogramowania: wirusy oraz robaki.
		2.2.2	Rozpoznaje typy złośliwego oprogramowania i wyjaśnia jego działanie: spyware, sieci typu botnet, diallery oraz keystroke logging (keylogging).
	2.3 Ochrona	2.3.1	Wyjaśnia działanie i ograniczenia oprogramowania antywirusowego.
		2.3.2	Skanuje wybrane dyski, foldery i pliki oraz skanuje automatycznie przy użyciu programów antywirusowych.
		2.3.3	Charakteryzuje kwarantannę i jej zastosowania w kontekście zainfekowanego lub podejrzanego pliku.
		2.3.4	Przedstawia znaczenie aktualizowania oprogramowania antywirusowego i baz sygnatur wirusów (plików definicyjnych).

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
3 Bezpieczeństwo w sieciach	*3.1 Sieci*	3.1.1	Definiuje pojęcie sieci i rozpoznaje jej typy: LAN, WAN i VPN.
		3.1.2	Charakteryzuje rolę administratora sieci w zarządzaniu kontami, uwierzytelnianiu oraz autoryzowaniu ruchu sieciowego.
		3.1.3	Wymienia możliwości i ograniczenia oprogramowania firewall.
	3.2 Połączenia sieciowe	3.2.1	Rozpoznaje fizyczne możliwości połączenia sieciowego: przewodowe i radiowe.
		3.2.2	Identyfikuje potencjalne zagrożenia związane z połączeniami sieciowymi: złośliwe oprogramowanie, niepowołany dostęp i utrata prywatności.
	3.3 Sieci bezprzewodowe	3.3.1	Wskazuje konieczność nadawania hasła podczas korzystania z połączenia radiowego.
		3.3.2	Rozpoznaje sposoby zabezpieczania połączenia bezprzewodowego: WEP, WPA oraz MAC.
		3.3.3	Przedstawia konsekwencje używania niezabezpieczonej sieci bezprzewodowej, gdy osoby niepowołane (podsłuchiwacze) mogą poznać prywatne dane.
		3.3.4	Łączy się z zabezpieczoną i niezabezpieczoną siecią.
	3.4 Kontrola dostępu	3.4.1	Wyjaśnia przyczyny istnienia konta sieciowego i korzysta z niego przy użyciu nazwy użytkownika i hasła.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		3.4.2	Wylicza i charakteryzuje zasady właściwego postępowania z hasłami: zachowywanie haseł dla siebie, konieczność regularnej zmiany hasła, odpowiednia długość hasła, budowa hasła kombinacją cyfr, liter oraz znaków specjalnych.
		3.4.3	Opisuje powszechne biometryczne techniki zabezpieczeń: skan odcisku palca i tęczówki oka.
4 Bezpieczeństwo w Internecie	*4.1 Przeglądanie Internetu*	4.1.1	Wskazuje konieczność przeprowadzania pewnych operacji (np. finansowych) jedynie poprzez bezpieczne witryny.
		4.1.2	Rozpoznaje bezpieczne witryny poprzez: https, symbol kłódki.
		4.1.3	Charakteryzuje zjawisko pharmingu.
		4.1.4	Definiuje pojęcie certyfikatu uwierzytelniającego strony. Weryfikuje certyfikat.
		4.1.5	Wyjaśnia pojęcie hasła jednorazowego.
		4.1.6	Włącza i wyłącza funkcję autouzupełniania i autozapisu podczas wypełniania formularza.
		4.1.7	Objaśnia pojęcia ciasteczka.
		4.1.8	Włącza i wyłącza obsługę ciasteczek.
		4.1.9	Usuwa prywatne dane z przeglądarki – historię przeglądania, pliki tymczasowe, hasła, ciasteczka, dane autouzupełniania.
		4.1.10	Charakteryzuje przeznaczenie, możliwości oraz typy programów kontrolujących zawartość stron: filtr rodzicielski i oprogramowanie filtrujące treść.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
	4.2 Portale społeczno-ściowe	4.2.1	Wykazuje znaczenie nieudostępniania poufnych danych na portalach społecznościowych.
		4.2.2	Wskazuje konieczność nadania ustawień prywatności konta posiadanego na portalu społecznościowym.
		4.2.3	Identyfikuje potencjalne zagrożenia niesione przez korzystanie z portali społecznościowych: cyberdręczenie, grooming, fałszywe i niebezpieczne informacje, fałszywe tożsamości, zwodnicze linki i e-maile.
5 Komunikacja	*5.1 E-maile*	5.1.1	Przedstawia cel szyfrowania i deszyfrowania e-maili.
		5.1.2	Definiuje pojęcie podpisu elektronicznego.
		5.1.3	Tworzy i dołącza podpis elektroniczny do wiadomości e-mail.
		5.1.4	Identyfikuje możliwość otrzymywania fałszywych i niechcianych e-maili.
		5.1.5	Wyjaśnia pojęcie phishingu. Rozpoznaje techniki phishingu: stosowanie danych istniejących firm i osób, fałszywe linki.
		5.1.6	Identyfikuje niebezpieczeństwo zainfekowania komputera złośliwym oprogramowaniem poprzez otwarcie załącznika e-maila zawierającego makro lub plik wykonawczy.
	5.2 Komunikatory	5.2.1	Wyjaśnia pojęcie komunikatora internetowego i sposób z jego korzystania.
		5.2.2	Charakteryzuje podatność komunikatorów na poniższe zagrożenia: złośliwe oprogramowanie, dostęp poprzez backdoor'y, dostęp do plików.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		5.2.3	Przedstawia metody zapewniające prywatność: szyfrowanie, nieudostępnianie poufnych informacji osobom postronnym, ograniczanie wymiany plików.
6 Bezpieczne zarządzanie danymi	*6.1 Zabezpieczanie i backupowanie danych*	6.1.1	Identyfikuje środki i metody ochrony urządzeń przed niepowołanym dostępem: zapisuj adres i dane urządzenia, używaj linki antykradzieżowe i inne urządzenia kontroli dostępu.
		6.1.2	Wyjaśnia znaczenie posiadania kopii zapasowej (backupu) w przypadku utraty danych, rejestrów finansowych, czy zakładek i historii przeglądania.
		6.1.3	Przedstawia własności procedury backupowania: regularność/częstotliwość tworzenia kopii zapasowej, harmonogram, miejsce zapisu danych.
		6.1.4	Backupuje dane (tworzy kopie zapasowe).
		6.1.5	Przywraca i waliduje przywrócone dane.
	6.2 Bezpieczne usuwanie danych	6.2.1	Określa cel trwałego usuwania danych z dysków i nośników.
		6.2.2	Odróżnia usuwanie danych od ich trwałego niszczenia.
		6.2.3	Rozpoznaje metody trwałego niszczenia danych: stosowanie niszczarki, fizyczne niszczenie nośników, demagnetyzacja, wyspecjalizowane przedsiębiorstwa.