ECDL/ICDL IT Security
Moduł S3
Sylabus – wersja 2.0

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.

Rozszerzenie
Zgodnie ze standardem wymagań dla kompetencji cyfrowych, realizowanych w projektach w obszarze edukacji, w ramach Programu Operacyjnego Wiedza Edukacja Rozwój i Regionalnych Programów Operacyjnych, współfinansowanych ze środków Europejskiego Funduszu Społecznego w latach 2014 – 2020, sylabus modułu *ECDL/ICDL IT Security* został rozszerzony o elementy oznaczone gwiazdką (*). Rozszerzenie to pozwala zapewnić pełne pokrycie modułem *ECDL/ICDL IT Security* obszaru Bezpieczeństwo ramy kompetencji na poziomach zaawansowania A i B. Egzamin z modułu *ECDL/ICDL IT Security* jest dostępny zarówno w wersji podstawowej jak i rozszerzonej.

ECDL/ICDL IT Security

Moduł ten swoim zakresem obejmuje zagadnienia odnoszące się do bezpiecznego użycia ICT (TIK) w życiu codziennym i umiejętności używane do nawiązania i utrzymania bezpiecznego połączenia sieciowego, bezpiecznego korzystania z Internetu oraz właściwego zarządzania danymi i informacjami.

Założenia modułu

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

- Bezpiecznego przechowywania informacji i danych oraz głównych zasad przechowywania danych, ochrony i kontroli danych oraz prywatności.
- Rozpoznawania zagrożeń bezpieczeństwa osobistego w zakresie kradzieży tożsamości i potencjalnych zagrożeń dla danych, wynikających z użycia przetwarzania w chmurze.
- Używania haseł i szyfrowania dla ochrony plików i danych.
- Zagrożeń ze strony złośliwego oprogramowania i ochrony przed nim komputera, urządzeń lub sieci, a także identyfikacji ataków złośliwego oprogramowania.
- Głównych typów ochrony sieci (także sieci bezprzewodowych) i skutecznego stosowania osobistego firewall'a i osobistego hotspot'u.
- Ochrony komputera lub urządzenia przed nieautoryzowanym dostępem i bezpiecznego zarządzania hasłami.
- Poprawnego używania ustawień przeglądarki internetowej i potwierdzania tożsamości stron internetowych i bezpiecznego przeglądania tych stron.
- Zagadnień bezpieczeństwa, pojawiających się przy korzystaniu z hasła poczty elektronicznej, sieci społecznościowych, telefonii internetowej Voice over IP, komunikatorów i urządzeń mobilnych.
- Archiwizowania i przywracania plików lokalnie i w chmurze oraz kasowania i trwałego usuwania danych a także bezpiecznego odłączania urządzeń.
- Ochrony środowiska w aspekcie oszczędzania energii i wpływu TIK na środowisko naturalne.*

* Rozszerzenie pozwalające zapewnić pełne pokrycie modułem *ECDL/ICDL IT Security* obszaru Bezpieczeństwo na poziomach zaawansowania A i B w ramie kompetencji, zgodnie ze standardem wymagań dla projektów unijnych, współfinansowanych ze środków EFS.

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 pojęcia cyberprzestępczości i piractwa komputerowego (hacking).
		1.1.3	Rozpoznaje złośliwe i przypadkowe zagrożenia dla danych ze strony osób postronnych, dostawców usług, zewnętrznych organizacji.
		1.1.4	Identyfikuje zagrożenia danych ze strony sił wyższych, takich jak: pożar, powódź, wojna i trzęsienie ziemi.
		1.1.5	Rozpoznaje możliwości zagrożenia danych ze strony zastosowań przetwarzania w chmurze: możliwości zewnętrznej kontroli danych i utraty prywatności.
	1.2 Wartość informacji	1.2.1	Definiuje elementarne cechy bezpieczeństwa informacji, takie jak: poufność, integralność, dostępność.
		1.2.2	Wyjaśnia przyczyny konieczności ochrony danych osobowych – zapobieganie kradzieży tożsamości i oszustwa oraz zachowanie prywatności.
		1.2.3	Wskazuje przyczyny ochrony danych na komputerach i urządzeniach w miejscu pracy – przeciwdziałanie kradzieży czy oszustwom, przypadkowej utracie danych i sabotażowi.
		1.2.4	Rozpoznaje główne zasady przechowywania danych, ochrony i kontroli danych oraz prywatności, takich jak: przejrzystość, względy prawne, proporcjonalność - wg Dyrektywy 95/46/EC o ochronie danych (https://en.wikipedia.org/wiki/Data_Protection_Directive).
		1.2.5	Wyjaśnia pojęcia podmiot danych osobowych i administrator danych osobowych jak i zasady przechowywania danych, ochrony i kontroli danych oraz prywatności w kontekście tych pojęć.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		1.2.6	Podkreśla wagę stosowania zasad użycia ICT (TIK) i wie gdzie je znaleźć.
	1.3 Bezpieczeństwo osobiste	1.3.1	Wyjaśnia pojęcie socjotechnika i możliwe następstwa jego stosowania – nieautoryzowany dostęp do komputera i urządzenia, nieautoryzowane zbieranie informacji, oszustwo.
		1.3.2	Rozpoznaje metody socjotechniki: rozmowy telefoniczne, phishing oraz podglądanie (shoulder surfing).
		1.3.3	Definiuje pojęcie kradzieży tożsamości i jego konsekwencje na polu osobistym, finansowym, biznesowym i prawnym.
		1.3.4	Rozpoznaje metody kradzieży tożsamości: information diving, skimming i pretexting.
	1.4 Bezpieczeństwo plików	1.4.1	Wyjaśnia wpływ włączania i wyłączania obsługi makr na bezpieczeństwo.
		1.4.2	Wskazuje zalety i ograniczenia szyfrowania. Podkreśla wagę ujawnienia i utraty hasła szyfrowania, klucza szyfrowania, certyfikatu bezpieczeństwa.
		1.4.3	Szyfruje pliki, foldery, napędy.
		1.4.4	Nadaje hasła dokumentom, arkuszom, plikom skompresowanym.
2 Złośliwe Oprogramowanie	*2.1 Typy i metody*	2.1.1	Wyjaśnia pojęcia złośliwego oprogramowania. Rozpoznaje różne sposoby ukrywania złośliwego oprogramowania na komputerze lub urządzeniu dla takich ich form jak: trojan, rootkit, backdoor.
		2.1.2	Rozpoznaje typy infekcji złośliwego oprogramowania i wyjaśnia jak działają wirusy i robaki.
	2.2 Ochrona	2.2.1	Rozpoznaje działania i ograniczenia oprogramowania antywirusowego.
		2.2.2	Wyjaśnia potrzebę instalacji oprogramowania antywirusowego na komputerze i urządzeniu.
		2.2.3	Podkreśla istotność regularnego uaktualniania oprogramowania, w tym: antywirusów, przeglądarek internetowych, wtyczek, aplikacji i systemu operacyjnego.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		2.2.4	Skanuje wybrane dyski, foldery i pliki oraz skanuje automatycznie przy użyciu programów antywirusowych.
		2.2.5	Identyfikuje ryzyko użycia przestarzałego i niewspieranego oprogramowania – wzrost ryzyka zagrożenia złośliwym oprogramowaniem, niekompatybilność.
	2.3 Rozwiązywanie i usuwanie	2.3.1	Wyjaśnia pojęcie kwarantanny i jej zastosowania w kontekście zainfekowanego lub podejrzanego pliku.
		2.3.2	Stosuje kwarantannę, usuwa zainfekowane/ podejrzane pliki.
		2.3.3	Wyjaśnia, że atak złośliwego oprogramowania może być rozpoznany i unieszkodliwiony przy użyciu zewnętrznych zasobów online, takich jak: strony internetowe producentów systemów operacyjnych, oprogramowania antywirusowego, twórców przeglądarek, stron internetowych i właściwych instytucji.
3 Bezpieczeństwo w sieciach	*3.1 Sieci i połączenia*	3.1.1	Definiuje pojęcie sieci i rozpoznaje główne typy sieci, takich jak: sieć lokalna (LAN), bezprzewodowa sieć lokalna (WLAN), siec rozległa (WAN), wirtualna sieć prywatna (VPN).
		3.1.2	Wyjaśnia jak łączenie z sieciami wpływa na bezpieczeństwo w aspekcie: złośliwego oprogramowania, nieuprawnionego dostępu do danych, zachowania prywatności.
		3.1.3	Definiuje rolę administratora sieci w zarządzaniu uwierzytelnianiem, autoryzacją i kontami, monitoringiem i instalacją uaktualnień i właściwych poprawek (łatek) w zakresie bezpieczeństwa, monitorowania ruchu sieciowego oraz zwalczania złośliwego oprogramowania znalezionego w sieci.
		3.1.4	Wyjaśnia funkcje i ograniczenia zapory sieciowej (firewall) na komputerze prywatnym i w miejscu pracy.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		3.1.5	Włącza albo wyłącza zaporę sieciową na komputerze domowym, zezwala albo blokuje działania aplikacji, stosuje wyjątki (usługa/funkcja) w dostępie przez firewall.
	3.2 Sieci bezprzewodowe	3.2.1	Wyjaśnia różne opcje bezpieczeństwa sieci bezprzewodowych i ich ograniczenia pośród takich jak: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC), filtering, ukrywanie Service Set IDentifier (SSID).
		3.2..2	Wyjaśnia, że użycie niezabezpieczonej sieci bezprzewodowej może powodować zagrożenia: podsłuch, przejęcie sieci, atak MITM (Man In the Middle).
		3.2.4	Włącza albo wyłącza zabezpieczenia osobistego hotspota i bezpieczne podłącza albo odłącza urządzenia.
4 Kontrola dostępu	*4.1 Metody*	4.1.1	Wymienia środki zabezpieczeń przed nieautoryzowanym dostępem do danych takich jak: nazwa użytkownika, hasło, PIN, szyfrowanie danych, uwierzytelnianie wieloczynnikowe.
		4.1.2	Wyjaśnia termin hasło jednorazowe i zna jego typowe zastosowania.
		4.1.3	Omawia funkcje konta sieciowego.
		4.1.4	Wyjaśnia, że dostęp użytkownika do konta sieciowego powinien być przez nazwę i hasło, a także wie, że w przypadku braku aktywności następuje żądanie ponownego podania hasła albo wylogowanie.
		4.1.5	Omawia główne biometryczne techniki zabezpieczeń: skan odcisku palca, tęczówki oka, rozpoznawania twarzy, geometria dłoni.
	4.2 Zarządzanie hasłami	4.2.1	Wyjaśnia dobre praktyki w zakresie haseł, takie jak: właściwa długość hasła, odpowiednie układy liter, cyfr i znaków specjalnych, nieujawnianie i niewspółdzielenie haseł, cykliczna zmiana haseł, różne hasła dla różnych usług.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		4.2.2	Opisuje możliwości i ograniczenia oprogramowania do zarządzania hasłami.
5 Bezpieczeństwo użycia technologii Web	*5.1 Ustawienia przeglądarki*	5.1.1	Wybiera właściwe ustawienia w celu włączenia, wyłączenia, autouzupełniania oraz autozapisu podczas wypełnianiu formularza.
		5.1.2	Potrafi usunąć takie dane prywatne z przeglądarki jak: historia przeglądania, historia pobierania plików, internetowe pliki tymczasowe, hasła, ciasteczka, dane autouzupełniania.
	5.2 Bezpieczeństwo przeglądania	5.2.1	Wyjaśnia, że aktywność online w postaci robienia zakupów i bankowości internetowej powinna być prowadzona przez bezpieczną stronę z użyciem bezpiecznych połączeń sieciowych.
		5.2.2	Charakteryzuje sposoby potwierdzenia autentyczności stron internetowych: jakość zawartości, aktualność, poprawny URL, informacje o firmie lub właścicielu, dane kontaktowe, certyfikat bezpieczeństwa, sprawdzenie właściciela domeny.
		5.2.3	Wyjaśnia termin pharming.
		5.2.4	Charakteryzuje funkcje i typy oprogramowania służącego do kontroli zawartości: oprogramowanie filtrujące zawartość stron internetowych, oprogramowanie do kontroli rodzicielskiej .
6 Komunikacja	*6.1 E-mail*	6.1.1	Wyjaśnia powody szyfrowania i deszyfrowania poczty elektronicznej.
		6.1.2	Charakteryzuje pojęcie podpisu elektronicznego.
		6.1.3	Rozpoznaje potencjalnie fałszywe i niechciane wiadomości poczty elektronicznej.
		6.1.4	Rozpoznaje główne cechy zjawiska phishing : użycie nazw prawdziwych organizacji, posłużenie się tożsamością wiarygodnych osób, fałszywe linki do stron internetowych, wykorzystanie logo i marek firm, zachęcanie do ujawnienia danych osobowych.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		6.1.5	Charakteryzuje możliwości zgłaszania przez użytkowników prób phishingu do właściwych organizacji i instytucji.
		6.1.6	Wyjaśnia możliwości zainfekowania komputera lub urządzenia złośliwym oprogramowaniem poprzez otwarcie załącznika e-mail, zawierającego makro lub plik wykonywalny.
	6.2 Sieci społecznościowe	6.2.1	Podkreśla wagę zachowania poufności danych oraz informacji umożliwiających identyfikację na stronach serwisów społecznościowych.
		6.2.2	Charakteryzuje potrzebę stosowania i cyklicznego przeglądania właściwych ustawień kont społecznościowych, takich jak: prywatność konta, lokalizacja.
		6.2.3	Stosuje ustawienia kont społecznościowych: prywatność konta, lokalizacja.
		6.2.4	Wyjaśnia potencjalne zagrożenia przy użyciu serwisów społecznościowych, takich jak: cyberdręczenie, grooming, złośliwe ujawnienie prywatnych treści, fałszywa tożsamość, oszukańcze lub złośiwe linki, treści i wiadomości.
		6.2.5	Posiada świadomość możliwości zgłaszania przez użytkowników niewłaściwego użycia serwisów społecznościowych do dostawcy usług i właściwych urzędów.
	6.3 VoIP i komunikatory internetowe	6.3.1	Charakteryzuje wrażliwość zabezpieczeń komunikatorów internetowych i VoIP na takie zjawiska jak: złośliwe oprogramowanie, dostęp z obejściem zabezpieczeń przez backdoor, dostęp do plików, podsłuch.
		6.3.2	Rozróżnia metody zapewnienia poufności przy użyciu komunikatorów internetowych i VoIP poprzez: szyfrowanie danych, nieujawnianie ważnych informacji, ograniczenie udostępniania plików.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
	6.4 Urządzenia mobilne	6.4.1	Identyfikuje możliwe następstwa użycia aplikacji z nieautoryzowanych sklepów internetowych w postaci: złośliwego oprogramowania na urządzenia mobilne, zbędnego zużycia zasobów, dostępu do plików osobistych, niskiej jakości aplikacji, ukrytych kosztów.
		6.4.2	Definiuje pojęcie uprawnień aplikacji.
		6.4.3	Wyjaśnia, że aplikacje mobilne mogą wydobywać dane osobiste z urządzenia w postaci: danych kontaktowych, historii lokalizacji, zdjęć.
		6.4.4	Przedstawia możliwe środki zapobiegawcze i awaryjne w przypadku zagubienia urządzenia mobilnego w postaci: zdalnego wyłączenia, zdalnego czyszczenia zawartości, lokalizacji urządzenia.
7 Bezpieczne Zarządzanie Danymi	*7.1 Zabezpieczanie i archiwizacja danych*	7.1.1	Charakteryzuje środki fizycznej ochrony komputerów i urządzeń w postaci: ciągłego nadzoru, zapisywania szczegółowych informacji o urządzeniu i jego umiejscowieniu, stosowania linki antykradzieżowej oraz kontroli dostępu.
		7.1.2	Wyjaśnia znaczenie posiadania procedury kopii zapasowej (backupu) w przypadku utraty danych z zawartości komputerów i urządzeń.
		7.1.3	Charakteryzuje własności procedury tworzenia kopii zapasowej: regularność/częstotliwość tworzenia kopii zapasowej, planowanie, miejsce zapisu danych, kompresja danych.
		7.1.4	Tworzy kopię zapasową w lokalizacji: dysk lokalny lub zewnętrzny/sieciowy, usługa w chmurze cyfrowej.
		7.1.5	Przywraca dane z kopii zapasowej z lokalizacji: dysk lokalny, dysk zewnętrzny/sieciowy, usługa w chmurze cyfrowej.
	7.2 Bezpieczne usuwanie danych i niszczenie	7.2.1	Odróżnia pojęcia usuwania danych i ich trwałego niszczenia.

KATEGORIA	OBSZAR WIEDZY I UMIEJĘTNOŚCI	NR	ZADANIE
		7.2.2	Charakteryzuje przyczyny trwałego niszczenia danych z napędów i nośników.
		7.2.3	Wyjaśnia, że informacje zapisane na portalach, serwisach społecznościowych, forach internetowych, w usłudze w chmurze cyfrowej mogą nie zostać trwale usunięte.
		7.2.4	Rozpoznaje metody trwałego niszczenia danych: stosowanie niszczarki, fizyczne niszczenie nośników, demagnetyzacja, wyspecjalizowane narzędzia.
8 Ochrona środowiska*	*8.1 Oszczędzanie energii**	8.1.1*	Rozpoznaje wagę rangi kosztów zasilania energetycznego urządzeń TIK (ICT).*
		8.1.2*	Identyfikuje główne działania w zakresie oszczędzania energii przez urządzenia TIK (ICT), takie jak: wyłączenie urządzeń gdy jest to właściwe, użycie istniejącego oprogramowania narzędziowego do zarządzania zużyciem energii.*
	*8.2 Świadomość wpływu TIK na środowisko naturalne**	8.2.1*	Charakteryzuje i stosuje strategie minimalizacji wpływu urządzeń TIK (ICT) na środowisko naturalne: zastępowanie urządzeń mniej energochłonnymi, stosowanie urządzeń o większej wydajności i trwałości.*
		8.2.2*	Charakteryzuje i stosuje zasady utylizacji sprzętu i wyposażenia TIK (ICT).*
		8.2.3*	Identyfikuje usługi TIK (ICT) dla monitorowania środowiska życia i pracy człowieka, takie jak: prognozy pogody, serwisy alarmowe, aplikacje mierzące poziomy hałasu oraz jakości oświetlenia.*

* Rozszerzenie pozwalające zapewnić pełne pokrycie modułem *ECDL/ICDL IT Security* obszaru Bezpieczeństwo na poziomach zaawansowania A i B w ramie kompetencji, zgodnie ze standardem wymagań dla projektów unijnych, współfinansowanych ze środków EFS.