Syllabus 1.0
Ez a dokumentum részletesen ismerteti az ECDL IT-biztonság modult és megfelelő alapokat ad az elméleti és gyakorlati vizsgához is.

A modul célja
Az IT-biztonság ECDL modul célja, hogy a vizsgázó megértse az IKT (infokommunikációs technológiai) eszközök mindennapos biztonságos használatának, a biztonságos hálózati kapcsolatok fenntartásának feltételeit; képes legyen a biztonságos és magabiztos Internet-használatra, és az adatok és információk megfelelő kezelésére.

A vizsga követelményei:

- a biztonságos információ és adat fontosságára, a fizikai biztonságra, a személyes adatok védelmére és a személyazonosság-eltulajdonításra vonatkozó kulcsfogalmak;
- a számítógép, egyéb eszközök és a hálózat megvédése rosszindulatú szoftverektől és a jogosulatlan hozzáférésektől;
- a hálózatok típusai, a kapcsolódási típusok és hálózat-specifikus kérdések, ideértve a tűzfalakat is;
- biztonságos böngészés a World Wide Weben és biztonságos kommunikáció az interneten
- az e-mailekre és azonnali üzenetküldőkre vonatkozó biztonsági kérdések
- az adatok biztonságos mentése és visszaállítása; adatok biztonságos megsemmisítése.

Kategória	Tudásterület	Hivatkozás	Tudáselem
12.1 Biztonsággal kapcsolatos fogalmak	12.1.1 Az adatok fenyegetettsége	12.1.1.1	Az adat és az információ közötti különbség
		12.1.1.2	A kiberbűnözés fogalma
		12.1.1.3	A hackelés, a crackelés és az etikus hackelés közötti különbségek

Kategória	Tudásterület	Hivatkozás	Tudáselem
		12.1.1.4	Az adatok előre nem látható körülmények általi fenyegetettségének felismerése (tűz, áradás, háború, földrengés)
		12.1.1.5	Az adatok munkatársak, szolgáltatók és külső személyek általi fenyegetettségének megismerése
	12.1.2 Az információ értéke	12.1.2.1	A személyesinformáció-védelem szükségessége (személyazonosság-lopás, és a csalások megelőzése)
		12.1.2.2	Az üzletileg érzékeny információk védelmének fontossága (ügyfelek adatainak megszerzése, vagy a pénzügyi adatok ellopása, illetve jogosulatlan felhasználása)
		12.1.2.3	A jogosulatlan adat-hozzáférést megakadályázó védelmi intézkedések (titkosítás és a jelszavak)
		12.1.2.4	Az információbiztonság alapvető jellemzői (bizalmasság, sértetlenség és rendelkezésre állás)
		12.1.2.5	A főbb információ- és adatvédelmi, megőrzési, valamint a védelmi intézkedésekre vonatkozó követelmények Magyarországon

Kategória	Tudásterület	Hivatkozás	Tudáselem
		12.1.2.6	Az IKT használatra vonatkozó szabályzatok és útmutatók jelentősége
	12.1.3 Személyi biztonság	12.1.3.1	A számítógépes szélhámosság (social engineering) fogalmának és jelentőségének megértése (információ-gyűjtés, csalás, számítógépes rendszerek való hozzáférés)
		12.1.3.2	A számítógépes szélhámosság módszerei (telefonhívások, adathalászat (phishing), kifigyelés (shoulder surfing).
		12.1.3.3	A személyazonosság-lopás fogalma és következményei (személyes, pénzügyi, üzleti, törvényi)
		12.1.3.4	A személyazonosság-lopás módszerei (információ búvárkodás (information diving), bankkártya-lemásolás (skimming), kikérdezés (pretexting).
	12.1.4 Fájl-biztonság	12.1.4.1	A makró engedélyezésének és tiltásának biztonságra gyakorolt hatásai
		12.1.4.2	Fájlok jelszavas védelemmel való ellátása (dokumentumok, tömörített fájlok, táblázatok)
		12.1.4.3	A titkosítás előnyei és korlátai
12.2 Rosszindulatú szoftverek	12.2.1 Definíciók és funkcionalitások	12.2.1.1	A rosszindulatú szoftver (malware) fogalma

Kategória	Tudásterület	Hivatkozás	Tudáselem
		12.2.1.2	A rosszindulatú szoftverek különböző elrejtési módjai (trójaiak (trojans), rendszerszinten rejtőző kártékony kód (rootkit) és hátsó kapuk (back door)
	12.2.2 Típusok	12.2.2.1	A rosszindulatú fertőző szoftverek típusai (vírusok, férgek)
		12.2.2.2	Az adatlopások típusai, és a profit-generáló/zsaroló rosszindulatú szoftverek (reklám-szoftver (adware), kém-szoftver (spyware), zombi-hálózat szoftver (botnet), billentyűzet-leütés naplózó (keystroke-logging) és modemes tárcsázó (diallers).
	12.2.3 Védekezés	12.2.3.1	Az antivírus szoftverek működése és korlátai
		12.2.3.2	A kiválasztott meghajtók könyvtárak, fájlok vizsgálata és a vizsgálatok ütemezése antivírus szoftverrel
		12.2.3.3	A karantén fogalma és a fertőzött vagy gyanús fájlok elkülönítése
		12.2.3.4	A vírusirtó-szoftver frissítése és vírus-definíciós fájl letöltése; a telepítés fontossága

Kategória	Tudásterület	Hivatkozás	Tudáselem
12.3. Hálózatbiztonság	12.3.1 Hálózatok	12.3.1.1	A hálózat fogalma és az általános hálózat-típusok (helyi hálózatok /LAN/, nagy kiterjedésű hálózatok /WAN/, illetve virtuális magánhálózatok /VPN/.
		12.3.1.2	A hálózati adminisztrátor szerepe a hálózaton belüli hitelesítés, feljogosítás és számonkérés kezelésében
		12.3.1.3	A tűzfal funkciója és korlátai
	12.3.2 Hálózati kapcsolatok	12.3.1.1	A hálózatokhoz való kapcsolódási lehetőségek (kábeles és drótnélküli kapcsolat)
		12.3.1.2	a hálózati kapcsolódás hatása a biztonságra (rosszindulatú szoftverek, jogosulatlan adat-hozzáférés, privátszféra fenntartása)
	12.3.3 Drótnélküli (wireless) biztonság	12.3.3.1	A jelszóhasználat fontossága a drótnélküli hálózatok védelmében
		12.3.3.2	A drótnélküli biztonság különböző típusai (kábeles kapcsolódással megegyező privátszféra /WEP/, WiFi védett hozzáférés /WPA/, média hozzáférés-védelem /MAC/)
		12.3.3.3	A nem védett drótnélküli hálózat használatának kockázatai: adataink megismerése a drót nélkül lehallgatók számára

Kategória	Tudásterület	Hivatkozás	Tudáselem
		12.3.3.4	Kapcsolódás védett/nem védett drótnélküli hálózathoz
	12.3.4 Hozzáférés-védelem	12.3.4.1	A hálózati fiók célja és a felhasználói név-jelszó párral való hozzáférés szükségessége
		12.3.4.2	A jó jelszó-szabályozások (a jelszavak másokkal való nem- megosztása, időszakos megváltoztatása, megfelelő jelszó-hossz, megfelelő jelszó-karakterek – betűk, számok és speciális karakterek – együttes használata
		12.3.4.3	A hozzáférés-védelemben általánosan használt biometriai biztonsági technikák (ujjlenyomat, retina-szkenner)
12.4 Biztonságos web-használat	12.4.1 Böngészés a weben	12.4.1.1	Bizonyos online tevékenységek (vásárlás, pénzügyi tranzakciók) biztonságos web-oldalakon végzésének jelentősége
		12.4.1.2	A biztonságos weboldalak beazonosítása (https, zár-szimbólum)
		12.4.1.3	Az eltérítéses adathalászat (pharming) fogalma
		12.4.1.4	A digitális tanúsítvány fogalma, érvényessége
		12.4.1.5	Az egyszerhasználatos jelszó (one time password - OTP) fogalma

Kategória	Tudásterület	Hivatkozás	Tudáselem
		12.4.1.6	Az űrlapok kitöltésekor a megfelelő engedélyezési, tiltási, automatikus kitöltési, automatikus mentési beállítások kiválasztása
		12.4.1.7	A süti (cookie) fogalma
		12.4.1.8	Megfelelő beállítások kiválasztása a sütik engedélyezéséhez és blokkolásához
		12.4.1.9	A személyes adatok törlése a böngészőkből (böngészési előzmények, ideiglenesen tárolt internet-fájlok, jelszavak, sütik, automatikusan kitöltött űrlap-adatok)
		12.4.1.10	A tartalom-ellenőrző szoftverek célja, funkciója és típusai (internet tartalmát szűrő szoftver, szülői felügyeleti szoftver)
	12.4.2 Közösségi hálózatok	12.4.2.1	A bizalmas információk közösségi oldalakon való nem felfedésének fontossága
		12.4.2.2	A megfelelő privátszféra beállítások alkalmazása a közösségi oldalak felhasználói fiókjaiban

Kategória	Tudásterület	Hivatkozás	Tudáselem
		12.4.2.3	A közösségi oldalak használatából adódó lehetséges veszélyek (internetes zaklatás (cyber bullying), szexuális kizsákmányolás (grooming), félrevezető/veszélyes információk, hamis személyazonosságok, csalárd linkek vagy üzenetek)
12.5 Kommunikáció	12.5.1 E-mail	12.5.1.1	Az e-mailek be- és kititkosításának célja
		12.5.1.2	A digitális aláírás fogalma
		12.5.1.3	Digitális aláírás készítése és hozzáadása
		12.5.1.4	Csalárd és kéretlen levelek fogadásával kapcsolatos ismeretek
		12.5.1.5	Az adathalászat fogalmának megértése, általános jellemzői (létező cég, személy nevének felhasználása, hamis web-linkek)
		12.5.1.6	A makrókat vagy futtatható fájlokat tartalmazó e-mail csatolmányok megnyitásának kockázata (a számítógép rosszindulatú kódokkal való megfertőződésének veszélye)
	12.5.2 Azonnali üzenetküldés (IM)	12.5.2.1	Az azonnali üzenetküldés (Instant Messaging - IM) fogalma és jelentősége

Kategória	Tudásterület	Hivatkozás	Tudáselem
		12.5.2.2	Az azonnali üzenetküldés biztonsági sebezhetősége (rosszindulatú szoftverek, hátsó kapu hozzáférés, fájl-hozzáférés)
		12.5.2.3	Az azonnali üzenetküldés bizalmasságát biztosító módszerek (titkosítás, fontos információk titokban tartása, fájl-megosztás korlátozása)
12.6 Az adatok biztonságos kezelése	12.6.1 Az adatok védelme és mentése	12.6.1.1	Az eszközök fizikai biztonságát biztosító módszerek (eszközök elhelyezésének és részleteinek naplózása, kábelek zárolása, fizikai hozzáférés-védelem)
		12.6.1.2	A mentési eljárás fontossága az adatok, pénzügyi feljegyzések, webes könyvjelzők/előzmények elvesztésének esetében
		12.6.1.3	A mentési eljárás tulajdonságai (ismétlődés/gyakoriság, ütemezés, tárolóhely-elhelyezkedés)
		12.6.1.4	Az adatok mentése
		12.6.1.5	A mentett adatok visszatöltése, a mentés érvényessége
	12.6.2 Biztonságos adat-megsemmisítés	12.6.2.1	A meghajtókról vagy eszközökről való végleges adattörlés jelentősége

Kategória	Tudásterület	Hivatkozás	Tudáselem
		12.6.2.2	Az adatok törlése és végleges megsemmisítése közötti különbség
		12.6.2.3	A végleges adat-megsemmisítés általános módszerei (feldarabolás, meghajtó/média megsemmisítés, demagnetizálás, adat-megsemmisítő eszközök használata)