



The Digital Skills Standard

# ICDL Workforce

## Cyber Security

Syllabus 2.0

## Kybernetická bezpečnosť

Syllabus 2.0



Syllabus Document – Znenie sylabu



## Účel

Tento dokument uvádza v plnom znení syllabus pre modul Cyber Security (Bezpečnosť pri využívaní IKT). Syllabus podrobne popisuje znalosti a zručnosti (learning outcomes), ktoré by uchádzač o skúšku z tohto modulu mal mať. Syllabus je zároveň aj východiskom pre zostavenie teoretických a praktických testov na overenie znalostí a zručností z tohto modulu.

## Copyright © 2010 - 2019 ICDL Foundation

Všetky práva sú vyhradené. Žiadnu časť publikácie nemožno reprodukovat' v žiadnej forme, ak nebolo vydané povolenie od ICDL Foundation. Žiadosti o povolenie na reprodukciu materiálu treba zaslať do ICDL Foundation.

## PREHLÁSENIE (zrieknutie sa zodpovednosti)

Hoci príprave tejto publikácie bola v ICDL Foundation venovaná najvyššia pozornosť, ICDL Foundation nedáva ako vydavateľ žiadnu záruku na úplnosť informácií v tomto materiáli a ICDL Foundation nemá povinnosť ani zodpovednosť v spojení s akýmikoľvek chybami, omylmi, nepresnosťami, stratou alebo škodou, ktorá by kedykoľvek vznikla na základe informácií alebo inštrukcií obsiahnutých v tomto materiáli. ICDL Foundation si vyhradzuje právo vykonávať zmeny podľa vlastného uváženia a bez predchádzajúceho upozornenia.

Oficiálna originálna verzia tohto materiálu je verzia zverejnená na webovej stránke ICDL Foundation: [icdl.org](http://icdl.org), slovenská verzia na [www.icdl.sk](http://www.icdl.sk)

## Modul – Kybernetická bezpečnosť, M12

**Modul Kybernetická bezpečnosť (IT Security, syllabus verzia 2.0)**, vyžaduje od uchádzača pochopenie základných pojmov, ktoré podporujú bezpečné používanie IKT v každodennom živote a využívanie zodpovedajúcich techník a aplikácií na udržiavanie bezpečného pripojenia do počítačovej siete, spoľahlivé a bezpečné využívanie internetu a zodpovedajúce spracovanie údajov a informácií.

### Ciele modulu

Uchádzač bude schopný:

- rozumieť základným pojmom, ktoré sa týkajú dôležitosti zabezpečenia údajov a informácií, rozoznávať bežnú ochranu údajov/ súkromia a princípy regulácie prístupu k nim (retention and control principles),
- rozoznávať ohrozenie osobnej bezpečnosti formou krádeže identity a potenciálneho ohrozenia údajov z dôvodu využívania cloud computingu,
- využívať heslá a šifrovanie na zabezpečenie súborov a údajov,
- rozumieť hrozbám zo strany škodlivého softvéru a chrániť počítač, zariadenia a počítačovú sieť pred škodlivým softvérom a cieľným útokom škodlivého softvéru,
- rozoznávať bežné typy ochrany počítačových sietí a bezdrôtových počítačových sietí, využívať osobné firewally (personal firewalls) a osobné prístupové body (personal hotspots),
- chrániť počítač pred neautorizovaným prístupom a bezpečne spravovať a aktualizovať heslá,
- využívať vhodné nastavenia webového prehliadača a rozumieť ako autentifikovať (authenticate) webové sídla a bezpečne sa pohybovať po webe (prehliadať webové stránky),
- rozumieť bezpečnostným otázkam z oblasti elektronickej komunikácie, ktoré sa vynárajú z používania elektronickej pošty (e-mailu), sociálnych sietí, telefonovania cez internet (VoIP), komunikácie v sieti v reálnom čase (Instant Messaging) a využívania mobilných zariadení,
- zálohovať a obnovovať údaje na lokálne úložiská i úložiská v cloude a bezpečne spravovať údaje a príslušné zariadenia.

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
12.1 Pojmy z oblasti informačnej bezpečnosti	12.1.1 Ohrozenie údajov	12.1.1.1	Rozlišovať medzi údajom a informáciou.
		12.1.1.2	Rozumieť pojmu kyberzločin (cybercrime), hacking.
		12.1.1.3	Rozlišovať zlomyseľné a náhodné ohrozenia údajov zo strany jednotlivcov, poskytovateľov služieb ako aj externých organizácií.
		12.1.1.4	Rozlišovať ohrozenie údajov z vyššej moci (mimoriadnych situácií), ako sú: požiar, potopa, vojna, zemetrasenie.
		12.1.1.5	Rozlišovať ohrozenia údajov z dôvodu využívania cloud computingu ako: správa údajov (data control), potenciálna strata súkromia.
	12.1.2 Hodnota informácie	12.1.2.1	Rozumieť základným charakteristikám informačnej bezpečnosti, ako sú: dôvernosť, integrita (celistvosť), dostupnosť.
		12.1.2.2	Rozumieť dôvodom na ochranu osobných údajov/ informácií, ako sú predchádzanie: krádeži identity, získaniu údajov podvodom (fraud), narušeniu súkromia (maintain privacy).

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
		12.1.2.3	Rozumieť dôvodom na ochranu obchodne citlivých informácií umiestnených na počítačoch a zariadeniach, ako sú: predchádzanie ich krádeži alebo ich podvodnému zneužívaniu, predchádzanie náhodnej strate údajov resp. sabotáži.
		12.1.2.4	Poznať bežnú ochranu údajov/ súkromia a princípy regulácie prístupu k údajom, ako sú: transparentnosť, legitímne účely, proporionalita.
		12.1.2.5	Rozumieť pojmom dotknutá osoba (data subject), prevádzkovateľ /sprostredkovateľ (data controller) a ako aplikovať princípy ochrany, regulácie prístupu k údajom/ súkromiu (pozri zákon č. 18/2018 Z. z).
		12.1.2.6	Rozumieť významu dodržiavania bezpečnostných zásad a politik, ktoré sa týkajú využívania informačných a komunikačných technológií, a spôsobu ako k týmto zásadám pristupovať.
	12.1.3 Osobná bezpečnosť	12.1.3.1	Rozumieť pojmu sociálne inžinierstvo a jeho následkom, ako sú: neoprávnený prístup k počítačovým systémom, neoprávnené zhromažďovanie informácií, podvodné konanie.
		12.1.3.2	Poznať metódy sociálneho inžinierstva, ako sú: telefonáty vrátane napodobenín automatických telefonických hlások, podvodné získavanie prístupových údajov (phishing), odpozorovanie displeja (shoulder surfing).
		12.1.3.3	Chápať pojem krádež identity a jeho osobné, finančné obchodné a právne dôsledky.
		12.1.3.4	Rozlišovať metódy krádeže identity, ako sú: information diving <sup>1</sup> , skimming <sup>2</sup> , pretexting <sup>3</sup> .
	12.1.4 Bezpečnosť súborov	12.1.4.1	Rozumieť bezpečnostným dôsledkom spojeným s povolením / zakázaním makier.
		12.1.4.2	Rozumieť výhodám a obmedzeniam pri uplatňovaní šifrovania. Byť si vedomý, aké je dôležité neodkryť a nestratiť šifrovacie heslo, kľúč, certifikát.
		12.1.4.3	Šifrovať súbor, priečinok, dátový nosič (drive).
		12.1.4.4	Zabezpečiť heslom súbory, ako sú: dokumenty, výpočtové tabuľky (spreadsheets), zabezpečiť heslom súbor, priečinok pri jeho kompresii / archivácii, zabezpečiť heslom už skomprimovaný súbor.
12.2 Škodlivý softvér (malware)	12.2.1 Typy a metodiky	12.2.1.1	Rozumieť pojmu škodlivý softvér (malware). Rozlišovať rôzne spôsoby skrývania sa škodlivého softvéru, ako sú: trójske kone, maskujúce sa aplikácie (rootkit), zadné dverka (back door).
		12.2.1.2	Poznať rôzne typy nákazlivého škodlivého softvéru, ako sú: vírusy alebo červy, a rozumieť ich pôsobeniu.

<sup>1</sup> neoprávnené obnovovanie vymazaných dôverných informácií

<sup>2</sup> používanie technických prostriedkov na krádež údajov z identifikačných prvkov, napr. z platobných kariet

<sup>3</sup> využívanie naoko dôveryhodných scenárov za účelom získavania citlivých informácií

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
		12.2.1.3	Rozlišovať formy odcudzenia údajov, typy škodlivého softvéru zameraného na dosiahnutie zisku / predražovanie a rozumieť ako pracujú, a to: adware <sup>4</sup> , ransomware <sup>5</sup> , spyware <sup>6</sup> , botnets <sup>7</sup> , keylogger <sup>8</sup> (keystroke logging), diallers <sup>9</sup> , a chápať na akom princípe fungujú.
	12.2.2 Ochrana	12.2.2.1	Rozumieť princípom fungovania antivírusového softvéru a poznať jeho obmedzenia.
		12.2.2.2	Rozumieť, že antivírusový softvér má byť nainštalovaný na počítači a zariadeniach.
		12.2.2.3	Rozumieť dôležitosti pravidelnej aktualizácie softvéru ako: antivírusový program, webový prehliadač, zásuvné aplikácie (plug-in), štandardné aplikácie, operačný systém.
		12.2.2.4	Vedieť pomocou antivírusového softvéru skontrolovať (skenovať) konkrétnu pamäťovú jednotku, priečinok alebo súbory. Vedieť napláňovať uskutočnenie kontroly (skenovania) s využitím antivírusového programu.
		12.2.2.5	Rozumieť rizikám pri využívaní zastaraného a nepodporovaného softvéru, ako: zvýšené ohrozenie škodlivým softvérom, nekompatibilita.
	12.2.3 Vyriešenie a odstránenie	12.2.3.1	Rozumieť pojmu karantény a chápať účinok umiestnenia infikovaných alebo podozrivých súborov do karantény.
		12.2.3.2	Umiestniť do karantény, vymazať infikované /podozrivé súbory.
		12.2.3.3	Rozumieť, že útok škodlivým softvérom je možné diagnostikovať a vyriešiť pomocou využitia informácií z online zdrojov, ako sú: webové stránky operačného systému, antivírusového programu, poskytovateľov webového prehliadača a webové sídla zodpovedajúcich autorít.
<b>12.3 Bezpečnosť počítačových sietí</b>	12.3.1 Počítačové siete a pripojenia	12.3.1.1	Rozumieť pojmu počítačová sieť a rozlišovať jednotlivé typy počítačových sietí, ako sú: lokálne siete (LAN), bezdrôtové lokálne siete (WLAN), rozľahlé siete (WAN), virtuálne prívätne siete (VPN).
		12.3.1.2	Chápať, aký vplyv na bezpečnosť môže mať pripojenie sa do siete: škodlivý softvér, neoprávnený prístup k údajom, narušenie súkromia (maintaining privacy).
		12.3.1.3	Chápať úlohu správcu počítačovej siete v procese riadenia autentifikácie <sup>10</sup> , autorizácie <sup>11</sup> , pri správe používateľských účtov, pri monitorovaní a inštalovaní relevantných bezpečnostných záplat a aktualizácií, pri monitorovaní sieťovej komunikácie, pri riešení nájdeného škodlivého softvéru, všetko v rámci spravovanej siete.

<sup>4</sup> škodlivý reklamný softvér

<sup>5</sup> škodlivý softvér, ktorý zabráňuje prístupu k infikovanému počítaču. Na obnovenie prístupu vyžaduje zaplatenie výkupného (ransom)

<sup>6</sup> "špehovací" softvér na zisťovanie a odosielanie citlivých údajov v počítači bez vedomia používateľa

<sup>7</sup> škodlivý softvér, ktorý vybrané počítače (pripojené k internetu) v pozadí podriadi tretej osobe a vytvorí z nich svoju sieť

<sup>8</sup> softvér na odchyťovanie stlačených kláves

<sup>9</sup> Softvér, ktorý uskutočňuje drahé telefonické hovory na účet používateľa bez jeho vedomia

<sup>10</sup> overovanie identity používateľov

<sup>11</sup> poskytovanie oprávnení

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
		12.3.1.4	Rozumieť pojmu firewall, chápať jeho funkciu a poznať jeho obmedzenia v súkromnom i pracovnom prostredí.
		12.3.1.5	Zapnúť, vypnúť firewall. Povolit', blokovať prístup aplikácie, služby/funkcie k údajom pomocou osobného firewallu.
	12.3.2 <i>Bezpečnosť bezdrôtovej siete</i>	12.3.2.1	Rozlišovať jednotlivé typy zabezpečenia bezdrôtovej siete a ich obmedzenia, a to u: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC) filtrovanie, Service Set Identifier (SSID) skrývanie.
		12.3.2.2	Uvedomovať si, že používanie nezabezpečenej počítačovej siete môže umožniť útoky ako: odpočúvanie komunikácie(eavesdropping) <sup>12</sup> , prevzatie sieťového spojenia (network hijacking) <sup>13</sup> , odpočúvanie a pozmeňovanie komunikácie metódou „človek uprostred“ (Man in the Middle, MitM) <sup>14</sup> .
		12.3.2.3	Rozumieť pojmu osobný prípojný bod (personal hotspot).
		12.3.2.4	Povolit', zakázať bezpečný osobný hotspot, bezpečne pripojiť, odpojiť zodpovedajúce zariadenia.
12.4. Riadenie prístupu	12.4.1 <i>Metodika</i>	12.4.1.1	Poznať opatrenia na zamedzenie neautorizovaného prístupu k údajom, ako sú: používateľské meno, heslo, PIN, šifrovanie, viacfaktorová autentifikácia (multifactor authentication).
		12.4.1.2	Rozumieť pojmu jednorazové (one-time) heslo a jeho typické využitie.
		12.4.1.3	Rozumieť účelu sieťového účtu.
		12.4.1.4	Rozumieť, že k používateľskému účtu v počítačovej sieti sa pristupuje cez používateľské meno a heslo a účet má byť zamknutý (locked) alebo používateľ má byť odpojený (logged off), keď sa na účte nepracuje.
		12.4.1.5	Poznať bežné bezpečnostné techniky, ktoré sa využívajú na riadenie prístupu k sieti na základe biometrických údajov, ako sú: odtlačky prstov, obraz (sken) dúhovky oka, rozpoznávanie tváre, geometria dlane.
	12.4.2 <i>Správa hesiel</i>	12.4.2.1	Poznať odporúčané politiky pre výber hesiel, ako sú: primeraná dĺžka hesla, vhodná štruktúra hesla s využitím kombinácie písmen, číslíc a špeciálnych znakov, nezdieľanie hesla, pravidelná zmena hesla, rozdielne heslá pre rozdielne služby.
		12.4.2.2	Rozumieť funkcii, obmedzeniam softvéru na správu hesiel.
12.5 Bezpečná práca s webom	12.5.1 <i>Nastavenie webového prehliadača</i>	12.5.1.1	Dokázať zvolit' vhodné nastavenia pri vyplňaní formulárov a to: povoliť, zakázať automatické dokončovanie formulára (autocomplete), povoliť, zakázať automatické ukladanie hesiel (autosave).

<sup>12</sup> odpočúvania komunikácie osôb/ zariadení, existuje viacero metód, jednou z nich je „man in the middle“

<sup>13</sup> preberať ovládanie aktívnej aplikácie/zariadenia cez sieť na diaľku

<sup>14</sup> Metóda odpočúvania komunikácie medzi osobami/ zariadeniami, pri ktorej osoba „uprostred“ ju môže skryto pozmeňovať

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
		12.5.1.2	Odstrániť z webového prehliadača súkromné údaje, ako sú: história prehliadania, história stiahnutých súborov, uložené dočasné súbory (vyrovnávacia pamäť, cache), heslá, cookies, údaje pre automatické dokončovanie <sup>15</sup> .
	12.5.2 <i>Bezpečné prehliadanie webu</i>	12.5.2.1	Uvedomovať si, že niektoré činnosti na webe (online nákupy, finančné transakcie) by sa mali uskutočňovať iba na zabezpečených webových stránkach a pri bezpečnom pripojení do siete.
		12.5.2.2	Poznať spôsoby ako si potvrdiť autenticitu /hodnovernosť/ pravosť web stránky, ako: kvalitný obsah, všeobecné uznávaný zdroj (currency), platné URL, prítomné informácie o spoločnosti alebo vlastníkovi stránky, kontaktné informácie, bezpečnostný certifikát stránky, overený vlastník domény.
		12.5.2.3	Rozumieť pojmu pharming (presmerovanie na podvrhnuté webové stránky).
		12.5.2.4	Chápať účel, funkciu a poznať druhy softvéru na kontrolu obsahu webových stránok, ako sú: softvér na filtrovanie internetového obsahu, softvér na účely rodičovskej kontroly.
12.6 Komunikácia	12.6.1 <i>Elektronická pošta (E-mail)</i>	12.6.1.1	Rozumieť účelu šifrovania / dešifrovania pri používaní elektronickej pošty.
		12.6.1.2	Rozumieť pojmu digitálny podpis.
		12.6.1.3	Rozpoznávať možnú podvodnú, nevyžiadajú správu elektronickej pošty.
		12.6.1.4	Poznať charakteristické znaky podvodnej techniky phishing, ako sú: zneužívanie oficiálnych názvov firiem, osôb; používanie falošných odkazov na webové stránky; zneužívanie zavedených log a značiek, povzbudzovanie k odkrytiu osobných informácií.
		12.6.1.5	Byť si vedomý, že môžem pokusy o phishing ohlásiť organizáciám, v ktorých mene útočník pôsobí, resp. príslušným úradom.
		12.6.1.6	Uvedomovať si nebezpečenstvo nákazy počítača alebo zariadenia škodlivým softvérom pri otvorení prílohy elektronickej pošty, ktorá obsahuje makro alebo spustiteľný súbor.
	12.6.2 <i>Sociálne siete</i>	12.6.2.1	Chápať, že je dôležité neuvádzať dôverné alebo osobné identifikačné informácie na stránkach sociálnych sietí.
		12.6.2.2	Uvedomovať si, že je nutné používať a pravidelne preskúmať, či je nastavená vhodná úroveň súkromia účtu na sociálnej sieti a či je vhodné nastavenie lokality.
		12.6.2.3	Vedieť na účte sociálnej siete nastaviť úroveň súkromia a lokalitu.

<sup>15</sup> Údaje získané pri vyplňovaní formulára na web stránke a uložené na neskoršie použitie

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
		12.6.2.4	Rozumieť potenciálnym nebezpečenstvám spojeným s používaním sociálnych sietí, ako sú: internetové šikanovanie (cyber bullying); vytváranie dôverného vzťahu za účelom zneužitia neplnoletej osoby (grooming); podvodným spôsobom odhalenie osobného obsahu; falošná totožnosť; zavádzajúce alebo škodlivé internetové odkazy, informácie, správy.
		12.6.2.5	Byť si vedomý, že nevhodné využívanie sociálnej siete alebo nevhodné správanie sa môžeme ohlásiť poskytovateľovi služby alebo zodpovedajúcim úradom.
	12.6.3 VoIP a komunikácia v sieti v reálnom čase (Instant Messaging, IM)	12.6.3.1	Rozumieť bezpečnostným hrozbám pri komunikácii v sieti v reálnom čase (instant messaging, IM) a komunikácii Voice over IP (VoIP), ako sú: škodlivý softvér, prístup prostredníctvom "zadných dvierok", neoprávnený prístup k súborom, odpočúvanie komunikácie osôb/zariadení (eavesdropping).
		12.6.3.2	Rozlišovať spôsoby zabezpečenia dôverných informácií pri komunikácii v sieti v reálnom čase a pri VoIP, ako sú: šifrovanie, nezverejňovanie dôležitých informácií, obmedzenie zdieľania súborov.
	12.6.4 Mobilné zariadenia	12.6.4.1	Rozumieť možným dôsledkom, ak používam aplikácie z neoficiálnych obchodov, ako sú: mobilný škodlivý softvér, zbytočné vyťažovanie zdrojov (resource utilization), neoprávnený prístup k osobným údajom, nízka kvalita produktu, skryté náklady počas využívania produktu.
		12.6.4.2	Rozumieť pojmu oprávnenia aplikácií (application permissions).
		12.6.4.3	Byť si vedomý, že mobilné aplikácie môžu z mobilného zariadenia získavať osobné informácie ako sú: kontaktné detaily, históriu pohybu v lokalitách, obrázky.
		12.6.4.4	Byť si vedomý, že ak sa mobilné zariadenie stratí, je potrebné uplatniť núdzové a bezpečnostné opatrenia, ako: deaktiváciu zariadenia na diaľku, vymazanie údajov zo zariadenia na diaľku, lokalizovať zariadenie.
<b>12.7 Bezpečná správa údajov</b>	12.7.1 Bezpečnosť a zálohovanie	12.7.1.1	Poznať spôsoby zabezpečenia fyzickej bezpečnosti počítačov a zariadení, ktoré obsahujú údaje, ako: nenechávať bez dozoru, zaznamenávať umiestnenie zariadení a ďalšie detaily, používať káblové zámky, používať prostriedky na riadenie prístupu.
		12.7.1.2	Chápať dôležitosť existencie záložných postupov v prípade straty údajov z počítača alebo zariadenia.
		12.7.1.3	Poznať zásady správneho zálohovania, ako sú: pravidelnosť a frekvencia zálohovania, plán zálohovania, umiestnenie dátového úložiska, kompresia dát.
		12.7.1.4	Vedieť zálohovať údaje na určené miesto ako: lokálne pamäťové médium, externé pamäťové médium, cloud služba.
		12.7.1.5	Vedieť obnoviť údaje zo zálohy na pôvodné alebo určené miesto, z lokálneho pamäťového média, externého pamäťového média, cloud služby.



KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
	12.7.2 <i>Bezpečné vymazanie a likvidácia</i>	12.7.2.1	Odlišovať vymazanie údajov od ich trvalého odstránenia.
		12.7.2.2	Rozumieť dôvodom, kvôli ktorým je potrebné trvalé odstránenie údajov z pamäťových médií a zariadení.
		12.7.2.3	Byť si vedomý, že vymazanie obsahu nemusí byť trvalé, ak je obsah spravovaný službami ako: sociálne siete, blog, internetové fórum, cloud služby.
		12.7.2.4	Poznať bežné metódy na trvalú likvidáciu údajov, ako: skartácia, fyzická likvidácia zariadení a médií, demagnetizácia (degaussing), používanie softvérových prostriedkov na likvidáciu údajov.