ICDL
The Digital Skills Standard

ICDL Workforce

IT SIGURNOST

Syllabus 2.0

Nastavni plan

Svrha

U ovom dokumentu je detaljno opisan nastavni plan za ICDL modul IT Sigurnost. Nastavni plan kroz ishode opisuje znanja i veštine koje kandidat treba da poseduje da bi položio test za ovaj modul. Nastavni plan predstavlja osnov za teorijski i praktični deo testa za ovaj modul.

Odricanje od odgovornosti

Iako je ICDL Fondacija pažljivo pripremala ovaj dokument, ICDL Fondacija, kao izdavač, i Regionalna ICDL kancelarija u Beogradu, ne garantuju apsolutnu tačnost informacija sadržanih u nastavnom planu niti snose odgovornost za bilo koju grešku, propust, netačnost, gubitke niti štete koje mogu nastati na osnovu sadržanih informacija ili bilo kog uputstva ili saveta iz ovog teksta. ICDL Fondacija zadržava pravo da vrši izmene, po sopstvenom nahođenju u bilo koje vreme bez prethodne najave.

Modul IT Sigurnost

U modulu IT sigurnost su navedeni koncepti i veštine koje se odnose na razumevanje bezbednog korišćenja IKT u svakodnevnom životu. Nastavni plan obuhvata korišćenje relevantnih tehnika i aplikacija za održavanje bezbedne konekcije na mrežu, bezbedno i sigurno korišćenje interneta, kao i upravljanje podacima i informacijama na odgovarajući način.

Ciljevi modula

Kandidat bi trebalo da:

- Razume ključne koncepte čuvanja informacija i podataka sigurnim, da identifikuje zajedničke principe zaštite podataka, privatnosti i kontrole.
- Prepozna pretnje ličnoj bezbednosti od krađe identiteta i potencijalne pretnje podacima korišćenjem računarstva u oblaku.
- Bude u mogućnosti da koristiti lozinke i šifriranje za zaštitu fajlova i podataka.
- Shvati pretnju zlonamernog softvera; da bude u mogućnosti da zaštiti računar, uređaj ili mrežu od napada zlonamernih softvera.
- Prepozna zajedničke mrežne i bežične vrste sigurnosti kao i da bude u mogućnosti da koristi lični zaštitni zid i ličnu pristupnu tačku.
- Zaštiti računar ili uređaj od neovlašćenog pristupa i da bude u mogućnosti da sigurno upravlja i ažurira lozinke.
- Koristi odgovarajuća podešavanja veb pregledača i razume kako da autentifikuje veb stranice i pretražuje internet bezbedno.
- Razume bezbednosne probleme koji mogu nastati upotrebom e-mejla, društvenih mreža, VoIP-a, instant poruka i mobilnih uređaja.
- Pravi sigurnosne kopije i vraća podatke na lokalni ili prostor za skladištenje u oblaku kao i da raspolaže i obriše podatake bezbedno.

POGLAVLJE	*OBLAST*	OZNAKA	CILJEVI
1 Koncepti bezbednosti	*1.1 Podaci*	1.1.1	Praviti razliku između podataka i informacija
		1.1.2	Razumeti pojam sajber kriminal, hakovanje.
		1.1.3	Prepoznati zlonamerne, slučajne pretnje podacima od strane pojedinaca, servis provajdera, eksternim organizacija.
		1.1.4	Prepoznati pretnje podacima kao što su: vatra, poplava, rat i zemljotres.
		1.1.5	Prepoznati pretnje podacima korišćenjem računarstva u oblaku kao što su: kontrola podataka, potencijalni gubitak privatnosti.
	1.2 Vrednost informacija	1.2.1	Razumeti osvnovne karakteristike o bezbednosti informacija kao što su: poverljivost, integritet, dostupnost.

POGLAVLJE	*OBLAST*	OZNAKA	CILJEVI
		1.2.2	Razumeti razloge za zaštitu ličnih informacija: izbegavanje krađe identiteta, prevare, održavanje privatnosti.
		1.2.3	Razumeti razloge za zaštitu poslovnih informacija na računarima i uređajima kao što su: sprečavanje krađe, lažna upotreba, slučajni gubitak podataka, sabotaža
		1.2.4	Identifikovati zajedničke principe zaštite podataka, privatnosti i kontrole kao što su: transparentnost, zakonite svrhe, proporcionalnost.
		1.2.5	Shvatiti pojmove subjekti podataka i kontroleri podataka i kako se na njih primjenjuju principi zaštite podataka, privatnosti i kontrole.
		1.2.6	Shvatiti važnost pridržavanja smernica i politika za upotrebu IKT-a i kako im pristupiti.
	1.3 Lična sigurnost	1.3.1	Razumeti pojam socijalno inženjerstvo i posledice kao što su: prikupljanje informacija, prevare, pristup sistemu računara.
		1.3.2	Identifikovati metode socijalnog inženjerstva kao što su: telefonski poziv, navlačenje, surfovanje preko ramena
		1.3.3	Razumeti pojam Krađa identiteta i njegove posledice: lične, finansijske, poslovne, zakonske.
		1.3.4	Identifikovati metode krađe identiteta: "ronjenjem", skimming, pretexting.
	1.4 Bezbednost fajlova	1.4.1	Razumeti uticaj uključivanja/isključivanja makro sigurnosnih naredbi.
		1.4.2	Razumeti prednosti, ograničenja šifriranja. Biti svestan važnosti ne otkrivanja lozinke za šifriranje, ključa ili sertifikata.
		1.4.3	Šifrirati fajl, folder, drajv.
		1.4.4	Postaviti lozinku za fajlove kao što su: dokumenta, tabelarni proračuni, kompresovani fajlovi.

POGLAVLJE	*OBLAST*	OZNAKA	CILJEVI
2 Zlonamerni programi	*2.1 Vrste i metode*	2.1.1	Razumeti pojam Zlonamerni program. Prepoznati različite načine na koji se zlonamerni program može sakriti na računarima i uređajima: Trojanski konj, rutkit, bekdor.
		2.1.2	Prepoznati vrste zlonamernih programa i shvatiti kako oni funkcionišu: virusi, crvi
		2.1.3	Prepoznati vrste zlonamernih programa za krađu podataka, novčanu dobit i razumeti kako oni rade: adware, ransomware, spyware, botnets, keystroke logging, diallers.
	2.2 Zaštita	2.2.1	Razumeti kako radi antivirusni softver i njegova ograničenja.
		2.2.2	Razumeti da antivirusni softver treba biti instaliran na računarima i uređajima.
		2.2.3	Razumeti važnost redovnog ažuriranja softvera kao što su: anti-virus, internet pretraživača, plug-in, aplikacija, operativnih sistema.
		2.2.4	Skenirati specifične fajlove, foldere upotrebom anti-virus softvera. Zakazati skeniranje upotrebom anti-virus softvera.
		2.2.5	Razumeti rizike pri korišćenju nepodržanih i zastarelih softvera kao što su: povećanje pretnje od zlonamernih programa, nekompatibilnost.
	2.3 Rešavanje i uklanjanje	2.3.1	Razumeti termin Karantin i efekte zaraženih/sumnjivih fajlova u karantinu.
		2.3.2	Staviti u karantin, obrisati sumnjive/zaražene fajlove.
		2.3.3	Razumeti da napad zlonamernog programa može biti dijagnostikovan i rešen korišćenjem onlajn izvora kao što su: veb stranice operativnog sistema, anti-virus, provajderi softvera veb pretraživača.
3 Bezbednost mreže	*3.1 Mreže i konekcije*	3.1.1	Razumeti termin Mreža i prepoznati zajedničke vrste mreža kao što su: lokalna mreža (LAN), bežična lokalna mreža (WLAN), širokopojasna mreža (WAN), virtuelna privatna mreža (VPN).

POGLAVLJE	*OBLAST*	OZNAKA	CILJEVI
		3.1.2	Razumeti implikacije povezivanja na mrežu kao što su: zlonamerni programi, neautorizovan pristup podacima, održavanje privatnosti.
		3.1.3	Razumeti ulogu mrežnog administratora u upravljanju autentifikacijom, autorizacijom i nalozima, praćenju i instaliranju relevantnih sigurnosnih zakrpa, praćenju mrežnog saobraćaja, i radu sa pronađenim zlonamernim programima unutar mreže.
		3.1.4	Razumeti funkciju, ograničenja zaštitnog zida u ličnom i poslovnom okruženju.
		3.1.5	Uključiti/Isključiti lični zaštitni zid. Dozvoliti, blokirati aplikaciju, uslugu kroz lični zaštitni zid.
	3.2 Bezbednost bežičnih mreža	3.2.1	Prepoznati različite opcije za bežičnu bezbednost i njena ograničenja: Wired Equivalent Privacy (WEP), Zaštićen Wi-Fi pristup (WPA) / Zaštićen Wi-Fi pristup 2 (WPA2), Kontrola pristupa medijima (MAC), Identifikator skupa usluga (SSID).
		3.2.2	Razumeti da korišćenjem nebezbednosne bežične mreže može doći do napada kao što su: Prisluškivači , otmica mreže, "čovek u sredini"
		3.2.3	Razumeti termin Lična pristupna tačka.
		3.2.4	Omogućiti, onemogućiti ličnu pristupnu tačku, kao i bezbedno konektovanje/ diskonektovanje uređaja.
4 Kontrola pristupa	*4.1 Metode*	4.1.1	Identifikovati mere za prevenciju neovlašćenog pristupa podacima kao što su: korisničko ime, lozinka,PIN, šifriranje, višestepena identifikacija korisnika
		4.1.2	Razumeti šta je jednokratna lozinka i njenu tipičnu upotrebu.
		4.1.3	Razumeti svrhu naloga na mreži.
		4.1.4	Razumeti da nalozima na mreži treba pristupiti upotrebom korisničkog imena i lozinke kao i da tokom odsustva nalog treba zaključati.

POGLAVLJE	*OBLAST*	OZNAKA	CILJEVI
		4.1.5	Identifikovati uobičajene biometrijske sigurnosne tehnike koje se koriste u kontroli pristupa poput: otisak prsta, skeniranje zenice oka, prepoznavanje lica, geometrija ruku.
	4.2 Upravljanje lozinkama	4.2.1	Prepoznati dobru praksu za upotrebu lozinki: adekvatna dužina lozinke, adekvatna kombinacija slova, brojeva i specijalnih karaktera, ne deliti lozinke, povremeno ih menjati, koristiti različite lozinke za različite naloge.
		4.2.2	Razumeti funkcije, ograničenja programa za upravljanje lozinkama.
5 Sigurno korišćenje VEB-a	*5.1 Podešavanje veb čitača*	5.1.1	Odabrati odgovarajuća podešavanja za omogućavanje, onemogućavanje automatskog dovršavanja, čuvanja pri popunjavanju obrazaca.
		5.1.2	Obrisati privatne podatke iz veb čitača kao što su: istorije pretraživanja, istorije preuzimanja, lozinke, kolačići, automatsko popunjene podatke.
	5.2 Bezbedno pretraživanje	5.2.1	Biti svestan da se određene onlajn aktivnosti (kupovina, plaćanje računa) trebaju vršiti samo na bezbednim stranicama korišćenjem bezbedne mreže.
		5.2.2	Identifikovati načine za potvrdu autentičnosti vebsajta kao što su: kvalitet sadržaja, starost, validnost URL-a, informacije o kompaniji ili vlasniku, kontakt informacije, bezbednosni sertifikat, provera vlasnika domena.
		5.2.3	Razumeti termin Pharming.
		5.2.4	Razumeti funkcije i vrste softvera za kontrolu sadržaja: softver za filtriranje interneta, softver za roditeljski nadzor.
6 Komunikacije	*6.1 E-Mail*	6.1.1	Razumeti svrhu šifrovanja, dešifrovanja e-mejla.
		6.1.2	Razumeti termin Digitalni potpis.
		6.1.3	Identifikovati moguć lažni, neželjeni e-mail.

POGLAVLJE	*OBLAST*	OZNAKA	CILJEVI
		6.1.4	Identifikovati zajedničke karakteristike "navlačenja" kao što su: upotreba imena tuđe organizacije, ljudi, lažnih veb linkova, logoa i brenda, podsticanje otkrivanja ličnih informacija.
		6.1.5	Biti svestan da možete prijaviti pokušaj "navlačenja" legitimnim organizacijama, relevantnim organima vlasti.
		6.1.6	Biti svestan da se uređaj ili računar mogu zaraziti zlonamernim programom otvaranjem priloga iz e-maila koji sadrži marko ili izvršni fajl.
	6.2 Društvene mreže	6.2.1	Shvatiti važnost ne otkrivanja poverljivih ili ličnih informacija na veb lokacijama društvenih mreža.
		6.2.2	Biti svestan potrebe za primenom i povremenim pregledanjem podešavanja naloga za društvene mreže kao što su: privatnost naloga, lokacija.
		6.2.3	Primeniti podešavanja naloga na društvenim medijima: privatnost naloga, lokacija.
		6.2.4	Razumeti potencijalne opasnosti kod korišćenja društvenih mreža: zlostavljanje putem interneta, grooming, zlonamerno otkrivanje ličnih informacija, lažni ili zlonamerni linkovi, sadržaji i poruke.
		6.2.5	Biti svestan da se neprikladno ponašanje na sajtovima društvenih mreža može prijaviti servis provajderu i relevantnim državnim organima.
	6.3 VoIP i Instant poruke	6.3.1	Razumeti sigurnosne propuste kod upotrebe instant poruka i VoIP-a kao što su: zlonamerni programi, bekdor pristup, pristup fajlovima, prisluškivanje.
		6.3.2	Prepoznati metode za obezbeđivanje poverljivosti prilikom korišćenja instant poruka i VoIP-a: šifrovanje, ne otkrivanje važnih informacija, ograničavanje deljenja fajlova.
	6.4 Mobilni uređaji	6.4.1	Razumeti moguće implikacije kod korišćenja aplikacija koje nisu iz zvaničnih izvora: zlonamerni programi za mobilne uređaje, pristup ličnim podacima, lošiji kvalitet, skriveni troškovi.

POGLAVLJE	*OBLAST*	OZNAKA	CILJEVI
		6.4.2	Razumeti termin Application permissions.
		6.4.3	Imati na umu da mobilne aplikacije mogu izvući privatne informacije sa mobilnog uređaja kao što su: podaci za kontakt, istorija lokacija, slike.
		6.4.4	Buditi svestan hitnih i mera predostrožnosti ako se izgubi uređaj kao što su: daljinsko isključivanje, daljinsko brisanje, lociranje uređaja.
7 Upravljanje sigurnošću podataka	*7.1 Sigurnost i pravljenje sigurnosnih kopija podataka*	7.1.1	Prepoznati načine obezbeđivanja fizičke sigurnosti računara i uređaja kao što su: ne ostavljanje uređaja bez nadzora, snimanje detalja i lokacije opreme, korišćenje bravice za kablove, kontrolisanje pristupa.
		7.1.2	Razumeti važnost pravljenja sigurnosnih kopija podataka kao prevenciju gubitaka podataka sa uređaja i računara. devices.
		7.1.3	Identifikovati karakteristike procedure pravljenja kopije podataka kao što su: redovnost, zakazivanje, lokacija, kompresija.
		7.1.4	Napraviti sigurnosne kopije na lokacijama kao što su: lokalni disk, eksterni disk, u oblaku.
		7.1.5	Povratiti dokumenta sa lokacije: lokalni disk, eksterni disk, u oblaku.
	7.2 Brisanje i trajno uništavanje podataka	7.2.1	Napraviti razliku između brisanja i trajnog uništavanja podataka.
		7.2.2	Razumeti razloge za trajno brisanje podataka sa svih diskova i uređaja.
		7.2.3	Biti svestan da se podaci ne brišu trajno sa nekih naloga kao što su: sajtovi društvenih mreža, blog, internet forumi, usluge u oblacima.
		7.2.4	Identifikovati zajedničke metode trajnog brisanja podataka kao što su: sekači papira, uništavanje medija i diskova, , demagnetizacija, korišćenje uslužnih programa za uništavanje podataka.