Osrednje območne knjižnice

mariborska knjižnica
Mariborska knjižnica, Rotovški trg 2, 2000 Maribor
tel.: +386 2 23 52 100, fax: +386 2 23 52 127, www.knjiznica-mb.si, info@mb.sik.si

Organizacija upravljanja informacijske varnosti v splošni knjižnici

Vir: https://onlinedegrees.sandiego.edu/cyber-security-information-security-network-security/

Maribor, december 2024

Organizacija upravljanja informacijske varnosti v splošni knjižnici

Besedilo: **Irena Sirk** in **Anka Rogina,** Mariborska knjižnica

Ta dokument je nastal kot rezultat izvajanja kompetenčnih vsebin, v okviru delovanja Mariborske knjižnice kot osrednje območne knjižnice. Nastanek dokumenta je finančno podprlo Ministrstvo za kulturo RS.

Maribor, december 2024

Organizacija upravljanja informacijske varnosti v splošni knjižnici

Uvod

Krovna informacijska varnostna politika splošni knjižnici določa, da je treba zaščititi informacije in informacijska sredstva knjižnice ter ohranjati zaupnost, celovitost in razpoložljivost informacij, da bi tako zagotovili njeno nemoteno in varno poslovanje ter preprečili škodo oz. zmanjšali posledice varnostnih incidentov na najmanjšo možno mero.

Ta dokument je podrejeni dokument Krovne informacijske varnostne politike splošne knjižnice. Natančneje obravnava informacijsko varnost v knjižnici glede na organizacijo dela, obnašanje ljudi, fizično in tehnološko varovanje.

Dokument je nastal na osnovi standarda ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*, ki v Prilogi A navaja 93 varnostnih kontrol. Za ta dokument smo izbrali 25 varnostnih kontrol in na njihovi osnovi izpeljali 42 zahtev za knjižnice. Vsebina dokumenta je razdeljena na štiri tematske sklope, v okviru teh pa še na podsklope. Pri vsakem je najprej navedena varnostna kontrola (ena ali več) po standardu ISO/IEC 27001:2022, tej sledijo zahteve za knjižnice, potrebni oz. priporočeni dokumenti ter navedba odgovornosti za izvajanje kontrole oz. zahteve. Kot Priloga je dokumentu dodan še kontrolni seznam.

Dokument lahko splošne knjižnice prosto uporabijo kot vzorec svojega internega dokumenta. Pri tem pa mora vsaka knjižnica sama določiti velikost svojega sistema upravljanja informacijske varnosti. Oceniti mora lastne zmožnosti za doseganje informacijske varnosti, upoštevati vse dejavnike, ki vplivajo na njeno informacijsko varnost ter upoštevati notranje in zunanje deležnike, ki delujejo v njenem informacijskem sistemu. Kontrolni seznam v prilogi lahko uporabijo za hiter pregled stanja, za ozaveščanje pomanjkljivosti in za določanje prioritet.

Pomembno

Varnostne kontrole smo iz angleščine prevedli sami in na tem mestu poudarjamo, da ne gre za uradni, ampak delovni prevod standarda. Varnostne kontrole smo izbrali na osnovi lastne presoje. Menimo, da tako postavljene zahteve za splošne knjižnice predstavljajo solidno

osnovo za začetno vzpostavitev dokumentov informacijske varnostne politike. Po svoji presoji lahko knjižnice upoštevajo tudi več kontrol, ki so navedene v standardu in so jih prepoznale kot koristne za spremljanje varnosti svojega informacijskega sistema. Knjižnice, ki se bodo želele certificirati v skladu s standardom ISO/IEC 27001:2022, bodo seveda morale izpolniti zahteve vseh 93 varnostnih kontrol.

Varnostne kontrole in zahteve za knjižnice

Organizacijski vidik

1. Odgovornosti vodstva

Kontrola po standardu ISO/IEC 27001, Annex A

5.4 Odgovornosti vodstva

Vodstvo mora od vseh zaposlenih zahtevati informacijsko varnostno ravnanje v skladu z vzpostavljeno politiko informacijske varnosti, področnimi politikami in postopki organizacije.

Zahteve v knjižnici:

Z1: Vodstvo je odgovorno za učinkovito upravljanje z informacijsko varnostjo. V ta namen izvaja vodstvene preglede učinkovitosti sistema za upravljanje z varnostjo.

Z2: Vodstvo knjižnice mora zagotoviti, da zaposleni izpolnjujejo zahteve informacijske varnostne politike. Odgovorno je za zavrnitev neupravičenih ali nepotrebnih zahtev po dostopu do informacijskih virov ter za zagotavljanje ukinitve dostopa do informacijskih virov, ko ga zaposleni ne potrebujejo več.

Z3: Vsi zaposleni morajo pri svojem delu upoštevati dokument, ki opisuje politiko informacijske varnosti.

Potrebni / Priporočeni dokumenti

Dokument, ki opisuje politiko informacijske varnosti, npr. Krovna informacijska varnostna politika

Odgovoren za izvajanje

Vodstvo

2. Vloge in odgovornosti na področju informacijske varnosti

Kontrola po standardu ISO/IEC 27001, Annex A

5.2 Vloge in odgovornosti na področju informacijske varnosti

Določiti in dodeliti je treba vloge in odgovornosti za informacijsko varnost v skladu s potrebami organizacije.

Zahteve v knjižnici:

Z4: V knjižnici so določene osebe, ki so odgovorne za nadzor, razvoj, vzdrževanje in varovanje informacijskih sredstev knjižnice (»lastniki«).

Z5: V knjižnici so določene osebe, ki so zadolžene za vzpostavitev delovanja, nastavitve in vzdrževanje informacijskih virov in komunikacijske infrastrukture knjižnice. Te osebe so navadno strokovnjaki s področja informacijske tehnologije (IT). Lahko so zaposlene v knjižnici ali pa so zunanji izvajalci (»skrbniki«, »upravitelji«).

Z6: V knjižnici je določena pooblaščena oseba za zagotavljanje informacijske varnosti, ki je zadolžena za učinkovito izvajanje informacijske varnosti v knjižnici.

Z7: Vsi zaposleni, obiskovalci in drugi uporabniki informacijskega sistema, vključno z zunanjimi izvajalci, morajo upoštevati informacijsko varnostno politiko.

Pojasnila vlog v knjižnici:

- praviloma so direktorji odgovorne osebe za nadzor, razvoj in vzdrževanje, ti. »lastniki«;
- pooblaščene osebe za zagotavljanje informacijske varnosti so navadno vodje razvoja ali vodje IT službe, če jih knjižnica ima;
- osebe, zadolžene za delovanje, nastavitve in vzdrževanje informacijskih virov in komunikacijske infrastrukture knjižnice (»upravitelj« ali »skrbnik«) so navadno strokovnjaki s področja IT (»informatiki« ali »sistemci«). Lahko so zaposleni v knjižnici ali pa so zunanji izvajalci.
- včasih je lahko pooblaščena oseba in upravitelj tudi funkcija, združena v eni osebi.

Potrebni / Priporočeni dokumenti

Pravilnik ali navodila o odgovornostih na področju informacijske varnosti

Odgovoren za izvajanje

Vodstvo; odgovorni za IT področje.

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

3. Zasebnost in zaščita osebnih podatkov

Kontrola po standardu ISO/IEC 27001, Annex A

5.34 Zasebnost in zaščita osebno določljivih podatkov

Organizacija mora določiti in izpolniti zahteve v zvezi z ohranjanjem zasebnosti in zaščito osebnih podatkov v skladu z veljavnimi zakoni in predpisi ter pogodbenimi zahtevami.

Zahteve v knjižnici:

Z8: Knjižnica mora imeti pripravljen dokument, ki opredeljuje zasebnost in zaščito osebnih podatkov skladno z GDPR in ZVOP-2.

Z9: Vsi deležniki, tako zaposleni kot zunanji izvajalci, morajo podpisati dokument o varovanju vseh podatkov in še zlasti osebnih podatkov, kot to določa GDPR in ZVOP-2.

Potrebni / Priporočeni dokumenti

GDPR, ZVOP-2, Izjava o varstvu osebnih podatkov, dokumenti kot npr. Aneks k pogodbam z obdelovalci podatkov (vzorec pripravilo ZSK) in ostali dokumenti, predvideni pri informacijskem pooblaščencu, ipd.

Odgovoren za izvajanje

Vodstvo

4. Dostopi do informacijskih virov

Kontrole po standardu ISO/IEC 27001, Annex A

5.15 Nadzor dostopa

Pravila za nadzor fizičnega in logičnega dostopa do informacij in drugih povezanih sredstev se oblikujejo in izvajajo na podlagi poslovnih zahtev in zahtev informacijske varnosti.

5.17 Informacije o preverjanju pristnosti

Dodeljevanje in upravljanje informacij o avtentikaciji se nadzorujeta s postopkom upravljanja, vključno s svetovanjem osebju glede ustreznega ravnanja z informacijami o avtentikaciji.

5.18 Pravice dostopa

Pravice dostopa do informacij in drugih povezanih sredstev se zagotavljajo, pregledujejo, spreminjajo in odstranjujejo v skladu s področno politiko organizacije in pravili za nadzor dostopa.

Zahteve v knjižnici:

Z10: Dostopi do informacijskih virov (v knjižnici ali zunaj nje) morajo biti zavarovani z avtentikacijo (preverjanjem pristnosti uporabnika). Določen mora biti postopek dodeljevanja avtentikacij.

Pojasnilo:

Avtentikacija (angleško authentication) je preverjanje pristnosti; kadar gre za dodatno varnost, kjer se zahteva več kot en dejavnik preverjanja, govorimo o večfaktorski avtentikaciji (angl. MFA, Multifactor authentication) (vir: https://www.mipi.si/teme/informacijska-pismenost/kaj-je-avtentikacija-ki-nas-sciti-pred-zlorabami-gesel-in-uporabniskih-racunov)

V uporabi so različni načini avtentikacij, najbolj pogosto je to prijava z uporabniškim imenom in geslom ter enojna ali dvojna potrditev na predpisani način.

Potrebni / Priporočeni dokumenti

Pravilnik, ki vsebuje popis avtentikacij, ki jih knjižnica uporablja (način avtentikacije, kdo, komu in kako jih dodeljuje, pravila prijav ipd.)

Pravila o kontroli dostopa

Pravila upravljanja gesel

Odgovoren za izvajanje

Vodstvo; zaposleni, ki dodeljujejo dostope do informacijskih virov

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

5. Storitve v oblaku

Kontrola po standardu ISO/IEC 27001, Annex A

5.23 Informacijska varnost pri uporabi storitev v oblaku

Postopki za pridobitev, uporabo, upravljanje in izstop iz storitev v oblaku se vzpostavijo v skladu z zahtevami organizacije glede informacijske varnosti.

Zahteve v knjižnici:

Z11: Potrebno je upoštevati določila GDPR in ZVOP-2.

Z12: Kadar je le mogoče, mora zaposleni za shranjevanje podatkov knjižnice uporabiti shrambo v oblaku, ki jo je zagotovila knjižnica (npr. OneDrive). Uporaba storitev v oblaku za shranjevanje podatkov (npr. Dropbox) je dovoljena samo, če ima knjižnica takšen način

predviden in opisan v svojih dokumentih za to področje, kot je npr. Pravilnik ali navodila za uporabo storitev v oblaku.

Z13: Pri uporabi shrambe v oblaku jo mora zaposleni, če je le tehnično mogoče, nastaviti tako, da bodo podatki shranjeni le v oblaku in ne na nosilcu podatkov v (zasebni) napravi zaposlenega.

Potrebni / Priporočeni dokumenti

GDPR, ZVOP-2, Pogodba o gostovanju v oblaku, Pravilnik ali navodila za uporabo storitev v oblaku

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

6. Pripravljenost IKT za neprekinjeno poslovanje

Kontrola po standardu ISO/IEC 27001, Annex A

5.30 Pripravljenost IKT za neprekinjeno poslovanje

Pripravljenost IKT se načrtuje, izvaja, vzdržuje in preizkuša na podlagi ciljev neprekinjenega poslovanja in zahtev za neprekinjeno delovanje IKT.

Zahteve v knjižnici:

Z14: Pripraviti in vzdrževati je treba Načrt neprekinjenega poslovanja, ki vsebuje načine ravnanja ob prekinitvi delovanja IKT tehnologije, sistem prioritet in popis potrebnih aktivnosti.

Potrebni / Priporočeni dokumenti

Načrt neprekinjenega poslovanja knjižnice

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

7. Pravice intelektualne lastnine

Kontrola po standardu ISO/IEC 27001, Annex A

5.32 Pravice intelektualne lastnine

Organizacija izvaja ustrezne postopke za zaščito pravic intelektualne lastnine.

Zahteve v knjižnici:

Z15: Posebna skrb mora biti posvečena uporabi programske opreme, ki je kot intelektualna lastnina zaščitena z avtorskimi pravicami. Pred nameščanjem programske opreme za ustrezno licenco poskrbijo odgovorne osebe (lastniki informacijskih sredstev). Uporaba programske opreme, pridobljene na nelegalen način, je prepovedana.

Z16: Če zaposleni potrebuje programsko opremo, ki ni del standardne, se za nakup in nameščanje opreme dogovori s predpostavljenim in odgovorno osebo (lastnikom informacijskega sredstva).

Z17: Večina informacij in programske opreme (glasba, video, programi, filmi, dokumenti, ...), ki so dostopni v javni domeni (vključno z internetom), je zaščitena z avtorskimi pravicami ali drugo obliko zaščite intelektualne lastnine. S kršenjem avtorskih pravic in intelektualne lastnine zaposleni prevzame vso materialno in kazensko odgovornost. V primeru dvomov o možnosti uporabe programske opreme se je treba posvetovati z odgovorno osebo za IT področje.

Potrebni / Priporočeni dokumenti

Navodila o upoštevanju pravic intelektualne lastnine

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje, zaposleni

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

8. Skladnost s politikami, pravili in standardi za informacijsko varnost

Kontrola po standardu ISO/IEC 27001, Annex A

5.36 Skladnost s politikami, pravili in standardi za informacijsko varnost

Redno je treba preverjati skladnost z informacijsko varnostno politiko organizacije, področnimi politikami, pravili in standardi.

Zahteve v knjižnici:

Z18: Pripraviti je treba načrt časovnih pregledov s poročili stanja na področju informacijske varnosti. Preglede organizira in vodi oseba, ki je zadolžena za informacijsko varnost.

Potrebni / Priporočeni dokumenti

Načrt izvajanja pregledov, poročila

Odgovoren za izvajanje

Vodstvo;

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

Nadzor nad ljudmi

1. Ozaveščenost, izobraževanje in usposabljanje o informacijski varnosti

Kontrola po standardu ISO/IEC 27001, Annex A

6.3 Ozaveščenost, izobraževanje in usposabljanje o informacijski varnosti

Vsi zaposleni v organizaciji in zainteresirane stranke (pogodbeniki) morajo biti ustrezno ozaveščeni o informacijski varnosti, ustrezno izobraženi in usposobljeni ter seznanjeni z rednimi posodobitvami politike informacijske varnosti organizacije, področnih politik in postopkov, ki so pomembni za njihovo delovno mesto.

Zahteve v knjižnici:

Z19: Za zaposlene je potrebno organizirati izobraževanja s področja informacijske varnosti ob spremembah zakonodaje, vpeljavi novosti ali vsaj enkrat letno. Pri izvedbi izobraževanja morajo biti kot gradiva uporabljene zadnje različice varnostnih politik, navodil, predpisov in drugih virov, na katere se nanaša izobraževanje.

Z20: Odgovorna oseba, ki koordinira delo z zunanjimi izvajalci, je zadolžena, da se zunanji izvajalec seznani z varnostno politiko in upošteva njena določila. Zunanji izvajalec mora pred pričetkom del podpisati izjavo o seznanitvi in izpolnjevanju določil informacijske varnostne politike. Zapis o zahtevah s področja informacijske varnosti v knjižnici mora biti (npr. v obliki člena) v pogodbah in dogovorih o sodelovanju, ki posegajo tudi na področje informacijske varnosti.

Z21: Dokumente, ki vplivajo na informacijsko varnostno politiko, je treba redno posodabljati glede na spremembe s področja poslovanja in zakonodaje ter o spremembah obveščati vse deležnike oz. pripraviti posodobljene verzije dokumentov.

Potrebni / Priporočeni dokumenti

Zapis o zahtevah informacijske varnosti v knjižnici (posebni dokument, del pogodbe ipd.), Dokument (npr. v obliki obrazca) o varovanju osebnih podatkov

Odgovoren za izvajanje

Vodstvo; oseba, odgovorna za informacijsko varnost; zaposleni, ki urejajo dokumente (pogodbe, dogovore ipd.) za posamezno področje

2. Odgovornosti po prenehanju ali spremembi zaposlitve

Kontrola po standardu ISO/IEC 27001, Annex A

6.5 Odgovornosti po prenehanju ali spremembi zaposlitve

Treba je opredeliti, uveljaviti in ustreznim osebam in drugim zainteresiranim stranem sporočiti odgovornosti in dolžnosti informacijske varnosti, ki ostanejo v veljavi po prenehanju ali spremembi zaposlitve.

Zahteve v knjižnici:

Z22: Ob prenehanju ali spremembi zaposlitve je treba pripraviti zapisnik o primopredaji dokumentacije, ki jo je zaposleni uporabljal pri svojem delu, če le ta obstaja.

Z23: Ob odhodu zaposlenega iz knjižnice je treba ukiniti gesla, elektronske naslove in vse ostale možnosti dostopov.

Z24: Prav tako je treba spremeniti, ukiniti in onemogočiti vse vrste dostopov zaposlenemu ob menjavi delovnega mesta, če jih le ta na novem delovnem mestu ne potrebuje več.

Potrebni / Priporočeni dokumenti

Navodila o predaji dokumentacije in prenehanju pooblastil v elektronski obliki

(Pravilnik o delovnih razmerjih)

Odgovoren za izvajanje

Vodstvo

3. Delo na daljavo

Kontrola po standardu ISO/IEC 27001, Annex A

6.7 Delo na daljavo

Kadar osebje dela na daljavo, je treba izvajati varnostne ukrepe za zaščito informacij, do katerih se dostopa, ki se obdelujejo ali shranjujejo zunaj prostorov organizacije.

Zahteve v knjižnici:

Z25: Na lastni računalniški napravi, ki jo uporablja za delo na daljavo, mora zaposleni vključiti požarni zid, še posebej, če je bil izklopljen ali so bile spremenjene njegove nastavitve. Če je zaposleni spreminjal njegove nastavitve, jih mora ponovno preveriti in se prepričati, da izbrane nastavitve zagotavljajo zadostno raven varnosti. Če zaposleni ni prepričan, katere nastavitve so ustrezne, naj uporabi privzete nastavitve.

Z26: Vzpostavitev navideznega zasebnega omrežja (VPN povezave) zagotavlja šifriranje podatkov med napravo, ki jo uporablja zaposleni in omrežjem knjižnice in je zato praviloma ustrezna in varna rešitev za delo na daljavo. Če je to tehnično mogoče, ga mora zaposleni uporabiti.

Z27: Če zaposleni za delo na daljavo uporablja oddaljeno namizje (npr. vgrajeno v Microsoft Windows, TeamViewer ali podobne rešitve), se mora zaradi varne nastavitve požarnega zidu in povezljivosti z oddaljenim računalnikom posvetovati s skrbnikom informacijskega vira v knjižnici in tega na službenem računalniku ne sme vzpostavljati sam, če ni za to pooblaščen.

Z28: Podatkov informacijskega sistema knjižnice zaposleni praviloma ne sme shranjevati na lastnih napravah.

Za delo na daljavo knjižnica izbere tisti način, ki ga je zmožna ustrezno varnostno obvladovati.

Potrebni / Priporočeni dokumenti

Pravilnik / Navodila za delo na daljavo.

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje, zaposleni

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

4. Poročanje o dogodkih informacijske varnosti

Kontrola po standardu ISO/IEC 27001, Annex A

6.8 Poročanje o dogodkih informacijske varnosti

Organizacija mora zagotoviti mehanizem, s katerim lahko zaposleni po ustreznih kanalih pravočasno poročajo o opaženih ali domnevnih dogodkih informacijske varnosti.

Zahteve v knjižnici:

Z29: Vsak uporabnik (zaposleni ali zunanji) informacijskega sistema je dolžan vsak dogodek, ki lahko vpliva na varnost informacij, sporočiti odgovorni osebi za informacijsko varnost, ki ugotovi ali dogodek predstavlja varnostni incident.

Z30: V primeru neobičajnega obnašanja informacijskega sistema je uporabnik dolžan obvestiti odgovorno osebo za informacijsko varnost in ravnati po njenih navodilih.

Z31: Knjižnica vodi evidenco varnostnih incidentov, ki jo redno pregleduje odgovorna oseba za informacijsko varnost in izvaja ustrezne varnostne ukrepe.

Pojasnilo: V skladu z **Zakonom o informacijski varnosti (ZInfV)** (https://pisrs.si/pregledPredpisa?id=ZAKO7707) je **varnostni incident** vsak dogodek, ki ima dejanski negativen učinek na varnost omrežij in informacijskih sistemov.

Tudi izguba elektronske naprave (npr. telefon, tablica) ali nosilca podatkov (npr. zgoščenka, USB ključek) je varnostni incident.

Potrebni / Priporočeni dokumenti

Dokument, v katerem so definirani varnostni incidenti in v katerem je opisana pot za javljanje posameznih incidentov, kot npr. področje IKT, ostala dokumentacija, področje Cobiss itd.

Evidenca informacijskih incidentov

Odgovoren za izvajanje

Vodstvo; odgovorna oseba za informacijsko varnost; vodje na posameznih področjih dela; zaposleni; zunanji deležniki

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

Fizični nadzor

1. Območja fizičnega varovanja

Kontrola po standardu ISO/IEC 27001, Annex A

7.1 Območja fizičnega varovanja

Določiti in upoštevati je treba meje varnostnih območij, da se zaščitijo območja, ki vsebujejo informacije in druga povezana sredstva (npr. naprave za obdelavo informacij).

Zahteve v knjižnici:

Z32: V knjižnici so določeni varovani prostori, ki so posebej opremljeni v ta namen. To so strežniški prostori, drugi računalniški prostori, pisarne ipd., v katerih so nameščena sredstva za obdelavo informacij (strežniki, komunikacijska oprema - routerji, modemi, stikala ipd.). Varovan mora biti dostop v te prostore (npr. zaklenjeni prostori, omejen dostop, dostop z vstopno kodo, pravila dostopanja ipd.).

Potrebni / Priporočeni dokumenti

Seznam varovanih prostorov
Navodila za uporabo ključev

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje, vzdrževalno osebje v knjižnici

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

2. Čista miza in čisti zaslon

Kontrola po standardu ISO/IEC 27001, Annex A

7.7 Čista miza in čisti zaslon

Pravila o čistih pisalnih mizah za papirje in izmenljive nosilce podatkov ter pravila o čistih zaslonih za prostore za obdelavo informacij morajo biti opredeljena in ustrezno uveljavljena.

Zahteve v knjižnici:

Z33: Zaposleni morajo upoštevati načelo čiste mize. To določa, da ni dovoljeno puščati informacij in materialov z unikatnimi podatki ter strateško zaupnih podatkov na mizi oz. na zaslonu v času svoje odsotnosti. Priporočeno je, da je miza v tem času prazna, računalniški zaslon pa zaklenjen ali ugasnjen. Te materiale je potrebno hraniti v zaklenjenih predalih, omarah ali sobi.

Informacije z unikatnimi podatki so informacije, ki omogočajo identifikacijo uporabnika, posameznika ali podjetja (predvsem uporabniška imena in gesla, pametne kartice, ključki za ustvarjanje enkratnih gesel ipd.); materiali z unikatnimi podatki so predvsem žigi in strateško zaupni podatki, predvsem pogodbe, ponudbe, poročila in drugi dokumenti z zaupnimi podatki o cenah in stroških ter nosilci podatkov, ki vsebujejo večjo količino zaupnih informacij.

Potrebni / Priporočeni dokumenti

Navodila o shranjevanju dokumentov in informacij

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje, zaposleni

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

3. Infrastruktura

Kontrola po standardu ISO/IEC 27001, Annex A

7.11 Podporne storitve

Objekti za obdelavo informacij morajo biti zaščiteni pred izpadi električne energije in drugimi motnjami, ki jih povzročijo izpadi podpornih komunalnih storitev.

7.12 Varnost ožičenja

Kabli za prenos električne energije, podatkov ali podpornih informacijskih storitev morajo biti zaščiteni pred prestrezanjem, motnjami ali poškodbami.

Zahteve v knjižnici:

Z34: Oprema, ki zagotavlja delovanje informacijskega sistema ali se uporablja v poslovnih prostorih, kot je električno napajanje, telekomunikacije, vodovod, plin, kanalizacija, prezračevanje in klimatizacija, morajo biti nameščeni skladno z zahtevami proizvajalca.

Z35: V varovanih prostorih, v katerih so nameščena sredstva za obdelavo informacij (strežniki, komunikacijska oprema - routerji, modemi, stikala ipd.) mora biti poskrbljeno za sistem neprekinjenega napajanja (UPS naprave) vsaj za varni izklop naprav, zaznavanje in zaščito pred požarom, vlomom in ustrezno klimatizacijo.

Z36: Kadar je le mogoče, morajo biti kabli položeni podometno ali v zemlji. Kadar so položeni nadometno ali drugače izpostavljeni okolju in fizičnemu dostopu, morajo biti zaščiteni z ustreznim ohišjem oziroma zaščito, glede na potrebe prostora in namen uporabe.

Potrebni / Priporočeni dokumenti

Popis UPS in ostalih podpornih naprav ter njihova avtonomnost

Požarni red

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje, vzdrževalno osebje v knjižnici

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

4. Vzdrževanje opreme

Kontrola po standardu ISO/IEC 27001, Annex A

7.13 Vzdrževanje opreme

Opremo je treba pravilno vzdrževati, da se zagotovijo razpoložljivost, celovitost in zaupnost informacij.

Zahteve v knjižnici:

Z37: Za opremo, za katero proizvajalec zahteva redne preglede, morajo biti pregledi dokumentirani in izvedeni skladno z navodili proizvajalca.
V pravilno vzdrževanje opreme se šteje tudi redno posodabljanje (operacijskih sistemov, itd.).

Potrebni / Priporočeni dokumenti

Navodilo za ravnanje z računalniško in komunikacijsko opremo

Odgovoren za izvajanje

Odgovorni za IT področje, zaposleni

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

5. Varna odstranitev ali ponovna uporaba opreme

Kontrola po standardu ISO/IEC 27001, Annex A

7.14 Varna odstranitev ali ponovna uporaba opreme

Pred odstranitvijo ali ponovno uporabo je treba preveriti, ali so bili vsi občutljivi podatki in licenčna programska oprema odstranjeni ali varno prepisani.

Zahteve v knjižnici:

Z38: Preden se zastarela oprema zavrže ali preden se oprema pripravi za ponovno uporabo (npr. prenos računalnika na drugega zaposlenega), je treba trajno izbrisati podatke in licenčno programsko opremo oz. tisto licenčno programsko opremo, ki je drugi zaposleni ne potrebuje za svoje delo. To velja tudi za prenosne medije za shranjevanje podatkov (CD-ji, USB ključki, zunanji pomnilniki, ipd.).

Potrebni / Priporočeni dokumenti

Navodilo za ravnanje z računalniško in komunikacijsko opremo

Odgovoren za izvajanje

Odgovorni za IT področje

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

Tehnološki nadzor

1. Dostop do informacij

Kontrola po standardu ISO/IEC 27001, Annex A

8.2 Pravice privilegiranega dostopa

Dodeljevanje in uporaba privilegiranih pravic dostopa morata biti omejena in upravljana.

8.3 Omejitev dostopa do informacij

Dostop do informacij in drugih povezanih sredstev mora biti omejen v skladu z vzpostavljeno področno politiko nadzora dostopa.

Zahteve v knjižnici:

Z39: V knjižnici je treba določiti osebe, ki so zadolžene za dodeljevanje privilegiranih pravic. Prav tako morajo biti določene osebe, ki smejo te privilegirane pravice (npr. administratorski dostop do strežnikov in ostale komunikacijske opreme) uporabljati.

Privilegirani dostop do strežnikov za namen upravljanja s strežniki mora izhajati iz potreb tovrstnega dela in je dodeljen zaposlenim v IT službi, ki te naloge opravljajo.

Potrebni / Priporočeni dokumenti

Pravilnik, ki predpisuje dostop do informacij

Pravilnik, ki vsebuje popis avtentikacij, ki jih knjižnica uporablja (način avtentikacije, kdo jih dodeljuje, pravila prijav ipd.)

Pravila o kontroli dostopa za delo na IT področju

Pravila upravljanja gesel

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

2. Upravljanje tehničnih ranljivosti

Kontrola po standardu ISO/IEC 27001, Annex A

8.8 Upravljanje tehničnih ranljivosti

Pridobiti je treba informacije o tehničnih ranljivostih informacijskih sistemov v uporabi, oceniti je treba izpostavljenost organizacije tem ranljivostim in sprejeti ustrezne ukrepe.

Zahteve v knjižnici:

Z40: Pripraviti je treba popis prepoznanih tehničnih ranljivosti, kot so npr. dostopi do mapiranih pogonov, omrežnih mest, skupna raba posameznih dokumentov, delo na daljavo ipd. ter redno revidirati dokument. Spremljati je treba varnostne incidente in sprejemati ukrepe za njihovo preprečevanje.

Potrebni / Priporočeni dokumenti

Popis prepoznanih tehničnih ranljivosti

Navodila zaposlenim o ravnanju pri uporabi informacijskega sistema in ozaveščanje o potencialnih ranljivostih sistema.

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje, zaposleni

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

3. Varnostno kopiranje informacij

Kontrola po standardu ISO/IEC 27001, Annex A

8.13 Varnostno kopiranje informacij

Varnostne kopije informacij, programske opreme in sistemov je treba vzdrževati in redno preizkušati v skladu z dogovorjeno področno politiko varnostnega kopiranja.

Zahteve v knjižnici:

Z41: Varnostno kopiranje pomembnih poslovnih informacij mora biti izvedeno vsaj enkrat dnevno, če je le mogoče, samodejno. Varnostno kopiranje mora biti arhitekturno zasnovano tako, da škodljiva programska koda ne more hkrati z delovno kopijo podatkov šifrirati, izbrisati ali drugače poškodovati ali narediti nedostopnih tudi varnostnih kopij podatkov. Obstajati mora varnostna kopija pomembnih informacij vsaj za prejšnji dan. Za varnostno

kopiranje knjižnica izbere način, ki ustreza razvitosti njene opreme IKT in hkrati zagotavlja varnost.

Potrebni / Priporočeni dokumenti

Navodila o varnostnem kopiranju informacij

Odgovoren za izvajanje

Odgovorni za IT področje, zaposleni

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

4. Upravljanje sprememb

Kontrola po standardu ISO/IEC 27001, Annex A

8.32 Upravljanje sprememb

Postopki ob spremembah naprav za obdelavo informacij in informacijskih sistemov morajo biti vključeni v postopke upravljanja sprememb.

Zahteve v knjižnici:

Z42: Pripraviti je treba popis opreme, na kateri se obdelujejo informacije in voditi seznam fizičnih in programskih sprememb za posamezno napravo.

Potrebni / Priporočeni dokumenti

Navodila za pripravo popisa

Odgovoren za izvajanje

Vodstvo, odgovorni za IT področje

V primeru, da ima knjižnica zunanjega izvajalca, mora ta upoštevati in zadostiti predpisanim zahtevam zakonodaje in pravilniku/navodilom knjižnice.

PRILOGA

Organizacija upravljanja informacijske varnosti v splošni knjižnici

Kontrolni seznam

Naziv knjižnice:
Datum:

Oznaka zahteve	Besedilo zahteve	Knjižnica: Ima /Nima Izvaja/ Ne izvaja	Dokument: Knjižnica Ima /Nima /Potrebuje /Ne potrebuje	Odgovorna oseba (poimensko)
Z1	Vodstvo je odgovorno za učinkovito upravljanje z informacijsko varnostjo.			
Z2	Vodstvo knjižnice mora zagotoviti, da zaposleni izpolnjujejo zahteve informacijske varnostne politike.			
Z3	Vsi zaposleni morajo upoštevati dokument Politika informacijske varnosti.			
Z4	Določene so osebe, ki so odgovorne za nadzor, razvoj, vzdrževanje in varovanje informacijskih sredstev knjižnice (»lastniki«).			
Z5	V knjižnici so določene osebe, ki so zadolžene za vzpostavitev delovanja, nastavitve in vzdrževanje informacijskih virov in komunikacijske infrastrukture (»skrbniki«, »upravitelji«).			
Z6	V knjižnici je določena pooblaščena oseba za zagotavljanje informacijske varnosti.			
Z7	Vsi uporabniki informacijskega sistema morajo upoštevati informacijsko varnostno politiko.			
Z8	Knjižnica mora imeti pripravljen dokument, ki opredeljuje zasebnost in zaščito osebnih podatkov skladno z GDPR in ZVOP-2.			
Z9	Vsi deležniki morajo podpisati dokument o varovanju podatkov.			
Z10	Dostopi do informacijskih virov morajo biti zavarovani z avtentikacijo.			
Z11	Pri storitvah v oblaku je treba upoštevati določila GDPR in ZVOP-2.			
Z12	Zaposleni mora za shranjevanje podatkov knjižnice uporabiti shrambo v oblaku, ki jo je zagotovila knjižnica.			

Oznaka zahteve	Besedilo zahteve	Knjižnica: Ima /Nima Izvaja/ Ne izvaja	Dokument: Knjižnica Ima /Nima /Potrebuje /Ne potrebuje	Odgovorna oseba (poimensko)
Z13	Pri uporabi shrambe v oblaku mora zaposleni podatke shraniti le v oblaku in ne na nosilcu podatkov v napravi zaposlenega.			
Z14	Pripraviti in vzdrževati je treba Načrt neprekinjenega poslovanja IKT.			
Z15	Nameščati je treba le programsko opremo z licenco.			
Z16	Nameščanje nestandardne opreme v soglasju s predpostavljenim.			
Z17	S kršenjem avtorskih pravic in intelektualne lastnine zaposleni prevzame vso materialno in kazensko odgovornost.			
Z18	Pripraviti je treba načrt časovnih pregledov s poročili stanja na področju informacijske varnosti.			
Z19	Za zaposlene je potrebno organizirati izobraževanja s področja informacijske varnosti.			
Z20	Odgovorna oseba, ki koordinira delo z zunanjimi izvajalci, je zadolžena, da se zunanji izvajalec seznani z varnostno politiko in upošteva njena določila.			
Z21	Dokumente, ki vplivajo na informacijsko varnostno politiko, je treba redno posodabljati.			
Z22	Ob prenehanju ali spremembi zaposlitve je treba pripraviti zapisnik o primopredaji dokumentacije.			
Z23	Ob odhodu zaposlenega iz knjižnice je treba ukiniti gesla, elektronske naslove in vse ostale možnosti dostopov.			
Z24	Zaposlenemu je ob menjavi delovnega mesta treba spremeniti, ukiniti in onemogočiti vse vrste dostopov, ki jih na novem delovnem mestu ne potrebuje več.			
Z25	Na lastni računalniški napravi, ki jo uporablja za delo na daljavo, mora zaposleni vključiti požarni zid.			
Z26	Če je to tehnično mogoče, mora zaposleni uporabljati VPN povezavo.			
Z27	Če zaposleni za delo na daljavo uporablja oddaljeno namizje, se mora zaradi varne nastavitve požarnega zidu in povezljivosti z oddaljenim računalnikom posvetovati s skrbnikom informacijskega vira v knjižnici.			

Oznaka zahteve	Besedilo zahteve	Knjižnica: Ima /Nima Izvaja/ Ne izvaja	Dokument: Knjižnica Ima /Nima /Potrebuje /Ne potrebuje	Odgovorna oseba (poimensko)
Z28	Podatkov informacijskega sistema knjižnice zaposleni ne sme shranjevati na lastnih napravah.			
Z29	Vsak uporabnik (zaposleni ali zunanji) informacijskega sistema je dolžan vsak dogodek, ki lahko vpliva na varnost informacij, sporočiti odgovorni osebi za informacijsko varnost.			
Z30	V primeru neobičajnega obnašanja informacijskega sistema je uporabnik dolžan obvestiti odgovorno osebo za informacijsko varnost in ravnati po njenih navodilih.			
Z31	Knjižnica vodi evidenco varnostnih incidentov.			
Z32	V knjižnici so določeni varovani prostori, ki so posebej opremljeni v ta namen.			
Z33	Zaposleni morajo upoštevati načelo čiste mize.			
Z34	Infrastrukturna oprema mora biti nameščena skladno z zahtevami proizvajalca.			
Z35	V varovanih prostorih mora biti poskrbljeno za sistem neprekinjenega napajanja (UPS naprave), zaznavanje in zaščito pred požarom, vlomom in ustrezno klimatizacijo.			
Z36	Kabli morajo biti položeni podometno ali v zemlji. Kadar so izpostavljeni okolju in fizičnemu dostopu, morajo biti ustrezno zaščiteni.			
Z37	Za opremo, za katero proizvajalec zahteva redne preglede, morajo biti pregledi dokumentirani in izvedeni skladno z navodili proizvajalca.			
Z38	Preden se zastarela oprema zavrže ali preden se oprema pripravi za ponovno uporabo, je treba trajno izbrisati podatke in licenčno programsko opremo.			
Z39	V knjižnici je treba določiti osebe, ki so zadolžene za dodeljevanje privilegiranih pravic. Prav tako morajo biti določene osebe, ki smejo te privilegirane pravice uporabljati.			
Z40	Pripraviti je treba popis prepoznanih tehničnih ranljivosti.			
Z41	Izvajati je treba varnostno kopiranje pomembnih poslovnih informacij.			
Z42	Pripraviti je treba popis opreme, na kateri se obdelujejo informacije in voditi seznam fizičnih in programskih sprememb za posamezno napravo.			