INFORMACIJSKA VARNOSTNA POLITIKA ZA PODROČJE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE (IKT)

1 Uvod

Dokument »Informacijska varnostna politika za področje informacijsko-komunikacijske tehnologije (IKT)« vsebuje informacije, ki so po klasifikaciji dokumentov opredeljeni kot interni in niso namenjen širši javnosti. Varnost informacijskega sistema je vitalna komponenta delovanja zavoda.
Informacijska varnostna politika temelji na treh varnostnih gradnikih: zaupnost (confidentiality), celovitost (integrity) in razpoložljivost (availability). Z njimi morajo biti seznanjeni vsi zaposleni in uporabniki informacijskega sistema zavoda. Trije gradniki so nerazdružljivo povezani z varnostjo informacijskega sistema, ki podpira in izvaja poslovne aktivnosti.
Zaščita zaupnosti, celovitosti in razpoložljivosti so osnovni trije cilji, ki morajo biti izpolnjeni za zmanjševanje tveganja pri varnosti informacijskega sistema in posledično poslovanja.

Zaupnost pomeni zaščito občutljivih poslovnih informacij pred nepooblaščenim dostopom ali protipravnim prestrezanjem. Zagotavlja, da je informacija dostopna samo tistim, ki imajo ustrezna pooblastila. V primeru izpada drugih varnostnih mehanizmov (npr. ukraden prenosni računalnik, ukradeni podatki s strežnika) nam zaupnost zagotavlja, da so vsi podatki neuporabni - zapisani v nerazumljivi/neuporabni obliki.

Celovitost obravnava zagotavljanje pravilnosti ter celovitosti informacij in programske opreme. Kontrola celovitosti se uporablja za zaščito podatkov in sistemov pred nepooblaščeno spremembo. Celovitost olajša ugotavljanje sprememb ter preprečuje, da bi spremenjeno kopijo obravnavali kot original.

Razpoložljivost zagotavlja, da so informacije in poslovno pomembne storitve, aplikacije in procesi na voljo pooblaščenim uporabnikom, ko jih le ti potrebujejo. Za podporo varovanja zaupnosti, celovitosti in razpoložljivosti informacijskih virov zavoda je izdelana informacijska varnostna politika zavoda. V tem dokumentu je opisana informacijska varnostna politika za področje upravljanja IKT. Dokument je sestavljen iz več nivojev, ki so definirani in opisani v nadaljevanju. Dokument se pregleduje letno. V primeru predlaganih sprememb dokumenta informacijski varnostni inženir opravi pregled vseh predlaganih sprememb in pripravi končni predlog sprememb dokumenta.

2 Elementi varnostnega nadzora

2.1 Upravljanje s sredstvi

Cilj upravljanja s sredstvi je doseči in vzdrževati ustrezno zaščito sredstev v zavodu.

Kontrola 1: Odgovorne osebe IKT in zavoda vsako leto preverijo in uskladijo seznam strojne in programske opreme, ki se uporablja v zavodu.
Kontrola 2: Vsa informacijska sredstva imajo določenega lastnika.
Kontrola 3: Vsa informacijska sredstva imajo določenega skrbnika.
Kontrola 4: Vse informacije so označene in urejene.

Kriterij usklajenosti

Upoštevanje kontrol, opisanih v razdelku »Natančen opis«, je obvezno.

- Odstopanja od kriterija morajo biti dokumentirana in potrjena s strani odgovorne osebe IKT in zavoda.

Implementacija

Vzpostavitev registra strežnikov, mrežnih naprav in ostalih produkcijskih sistemov.
Vzpostavitev registra poslovnih in informacijskih produkcijskih aplikacij.
Vzpostavitev preglednice »Povezave med poslovnimi procesi in informacijskimi sredstvi«.

Natančen opis

Kontrola 1: Odgovorne osebe IKT in zavoda vsako leto preverijo in uskladijo seznam strojne in programske opreme, ki se uporablja v zavodu.
Seznam sistemov (strežniki - fizični in virtualni, pomembne delovne postaje, omrežna komunikacijska oprema, ostala produkcijska oprema) se vodi v preglednici, za katero so odgovorni skrbniki sistemov. Vsi pomembni elementi informacijsko-komunikacijskega sistema se zabeležijo v preglednico »Povezave med poslovnimi procesi in informacijskimi sredstvi«. V preglednici so označeni procesi po prioritetah, ki so pomembne za določitev prioritet pri obnovi informacijsko-komunikacijskega sistema. Podrobnejši seznam s kratkimi opisi programske opreme, razvite v okviru zavoda, je voden s strani odgovorne osebe IKT. Vsi seznami se redno dopolnjujejo in vsaj enkrat letno pregledajo ter posodobijo, tako da odražajo trenutno stanje.

Kontrola 2: Vsa v registru zavedena informacijska sredstva imajo določenega lastnika.
Lastnik informacijskega sredstva je odgovoren za nadzor, razvoj, vzdrževanje in varovanje informacijskega sredstva zavoda. Naloge lastnika informacijskega sredstva so:

- potrjevanje upravičenosti dostopa za posamezne uporabnike,
- pregled varnostnih dogodkov v dnevniških zapisih in ukrepanje v primeru zaznanih nepravilnosti,
- pregled uporabnikov s pravicami za dostop do informacijskega vira (enkrat letno),
- pregled uporabnikov s posebnimi pravicami dostopa v rednih časovnih intervalih (vsakih 6 mesecev).

Kontrola 3: Vsi v registru zavedeni informacijski viri imajo določenega skrbnika.
Skrbnik je zadolžen za vzpostavitev delovanja, nastavitve in vzdrževanje informacijskih virov in omrežne komunikacijske infrastrukture v zavodu. Naloge skrbnika so:

- preverjanje delovanja informacijskega vira ali omrežne komunikacijske infrastrukture,
- vpeljava in vzdrževanje informacijskih rešitev z namenom zagotavljanja nemotenega delovanja informacijskega vira ali omrežne komunikacijske infrastrukture,
- implementacija varnostnih nastavitev za informacijski vir ali omrežno komunikacijsko infrastrukturo,

- odprava napak v delovanju in analiza vzrokov za motnje v delovanju,
- stalno izobraževanje z namenom pridobivanja in osveževanja znanja na področju dela, ki ga opravlja skrbnik.

Kontrola 4: Vse informacije so označene in urejene.
Urejanje informacij je opredeljeno v Pravilniku o obdelavi osebnih podatkov vključno z zagotavljanjem varnosti osebnih podatkov in politiko varstva osebnih podatkov zaposlenih, ki ureja to področje in je v skladu z veljavno zakonodajo.

2.2 Fizična zaščita

Cilj fizične zaščite je preprečiti nepooblaščen fizični dostop, škodo in motnje v prostorih, ter preprečiti izgubo, škodo, krajo ali kompromitiranje informacijskih sredstev.

Kontrola 5: Kritične zmogljivosti za obdelavo informacij so nameščene na varovanih območjih.

Kontrola 6: Urejena je kontrola nadzora vstopa v območje, kjer se nahajajo informacijska sredstva (strežniki, komunikacijska oprema) – nadzorovano območje.

Kontrola 7: Mediji, ki se uporabljajo za arhiviranje in restavriranje podatkov, so fizično zavarovani pred nepooblaščenim dostopom, krajo in poškodovanjem.

Kontrola 8: Pred odstranitvijo opreme se pregledajo nosilci podatkov in odstranijo vsi podatki ter licenčna programska oprema.

Kriterij usklajenosti
Upoštevanje kontrol opisanih v razdelku »Natančen opis«, je obvezno.

- Odstopanja od kriterija morajo biti dokumentirana in potrjena s strani odgovorne osebe IKT in zavoda.

Implementacija
Vzpostavitev vseh zahtevanih kontrol za varovanje podatkovnega centra zavoda.

Natančen opis
Kontrola 5: Kritične zmogljivosti za obdelavo informacij so nameščene na varovanih območjih. V varovanih območjih je poskrbljeno za sistem neprekinjenega napajanja, zaznavanje in zaščito pred požarom, vlomom in ustrezno klimatizacijo.

Kontrola 6: Urejena kontrola nadzora vstopa v območje, kjer se nahajajo informacijska sredstva (strežniki, komunikacijska oprema) – nadzorovano območje.

V nadzorovanih območjih morajo veljati naslednje kontrole oz. elementi varovanja:

1. Območje mora biti zaklenjeno tudi, ko je pod nadzorom.
2. Odgovorne osebe so zadolžene za ugotavljanje poslovne potrebe za dostop do območja.
3. Vsi dostopi v nadzorovano območje se beležijo.
4. Osebe, ki se jim odvzame pravica dostopa, so takoj umaknjene z liste za dostop.

5. Izvaja se redni trimesečni pregled poročil o dostopih v nadzorovano območje za ugotavljanje neavtoriziranih poskusov dostopa.
6. Izvaja se redni letni pregled poslovne upravičenosti za dostop oseb na listi dostopa.
7. Alarmi morajo delovati z zasilnim napajanjem.
8. Ob alarmnem dogodku se izvede preiskava. Na podlagi ugotovitev je potrebno sprejeti korektivne ukrepe in po potrebi spremeniti način vstopa, da se prepreči ponovitev alarmnega dogodka.

Opombe: Postopki za odpravljanje ugotovljenih napak ali nepravilnosti se morajo izvajati redno, po izvedenih četrtletnih ali letnih pregledih.

Kontrola 7: Mediji, ki se uporabljajo za arhiviranje in restavriranje podatkov, so fizično zavarovani pred nepooblaščenim dostopom, krajo in poškodovanjem.
Upoštevati je potrebno naslednja navodila:

- Mediji morajo biti shranjeni v nadzorovanem območju v omari, ki je zaklenjena.
- Prostor, kjer so shranjeni mediji, mora biti ognjevaren.
- Dostop do medijev imajo samo pooblaščene osebe.

Kontrola 8: Pred odstranitvijo opreme se pregledajo nosilci podatkov in odstranijo vsi podatki in licenčna programska oprema.

Vse naprave, ki vsebujejo občutljive informacije (predvsem zaupni in osebni podatki), je potrebno fizično uničiti ali podatke izbrisati na način, ki onemogoča obnovitev izvirnih informacij (uporaba funkcij briši oz. formatiraj ni dovoljena).

2.3 Upravljanje s komunikacijo in produkcijo

Cilj upravljanja s komunikacijo in produkcijo je zagotoviti pravilno delovanje informacijsko-komunikacijskega sistema, zmanjšanje okvar sistema, zaščito programske opreme in informacij, vzdrževanje celovitosti in razpoložljivosti informacij, zaščito omrežij in podporne infrastrukture ter odkrivanje nepooblaščenega obdelovanja informacij.

Kontrola 9: Vsi delovni postopki so dokumentirani in na voljo vsem, ki jih potrebujejo.
Kontrola 10: Podatki se varnostno kopirajo in hranijo na dveh ločenih lokacijah. Zapisani podatki se v rednih intervalih preverjajo po zapisanih postopkih za obnovo.
Kontrola 11: Vzpostavljene so tehnične kontrole za preprečitev razširjanja in izvajanja škodljivih programov.
Kontrola 12: Informacije so med izmenjavo ustrezno zaščitene.
Kontrola 13: Pred objavo javno dostopnih informacij se vse informacije ustrezno preverijo, tako da se zagotovi pravilnost objavljenih podatkov.
Kontrola 14: Razvijalci programske opreme morajo v okviru priprave končne različice produkta izvesti tudi proti-virusno preverjanje.
Kontrola 15: Instalacija popravkov programske opreme mora biti izvedena v okviru odobrenega postopka upravljanja s spremembami (change management process).
Kontrola 16: Nadzorne zapise je potrebno kreirati za sisteme, programe in mrežno opremo, kjer je to tehnično izvedljivo.

Kontrola 17: Nadzorne zapise je potrebno kreirati za vse uspešne in neuspešne poskuse dostopa do informacijskih sredstev zavoda iz zunanjih lokacij.
Kontrola 18: Podatki o aktivnosti morajo vsebovati vsaj naslednje parametre: datum, čas, tip poskusa dostopa, identifikacija uporabnika.
Kontrola 19: Ure na vseh informacijskih sistemih so usklajene z dogovorjenim časovnim virom.

Kriterij usklajenosti
Upoštevanje kontrol opisanih v razdelku »Natančen opis«, je obvezno.

- Odstopanja od kriterija morajo biti dokumentirana in potrjena s strani odgovorne osebe IKT in zavoda.

Implementacija
Zapis vseh nastavitev komunikacijske opreme – konfiguracija za posamezne elemente komunikacijske opreme.

Natančen opis
Kontrola 9: Vsi delovni postopki so dokumentirani in na voljo vsem, ki jih potrebujejo.
Postopki za sistemske dejavnosti so dokumentirani v delovnih navodilih za posamezne aktivnosti kot so postopki za:

- zagon in zaustavitev strežnikov,
- izvajanje arhiviranja in restavriranja podatkov,
- vzdrževanje opreme,
- ravnanje z nosilci podatkov,
- dejavnosti povezane s komunikacijsko infrastrukturo,
- vzdrževanje varnostne infrastrukture.

Kontrola 10: Podatki se varnostno kopirajo in hranijo na dveh ločenih lokacijah. Zapisani podatki se v rednih intervalih preverjajo po zapisanih postopkih za obnovo.
Zaradi zagotavljanja neprekinjenega poslovanja in zaščite podatkov ob nepredvidenih dogodkih se na informacijskih virih izvajajo postopki varnostnega kopiranja in arhiviranja opisani v nadaljevanju tega dokumenta. Magnetni trakovi in drugi mediji za shranjevanje podatkov so shranjeni v ognjevarni omari.

Strežniki
Osebe ali zunanji izvajalci, zadolženi za izvajanje arhiviranja, skrbijo tudi za arhiv podatkov. Arhiviranje podatkov se izvaja po vnaprej določenem načrtu za vsak strežnik. Arhiviranje se izvaja avtomatsko s pomočjo avtomatsko nastavljenih pravil vsakodnevno ob v naprej določenih urah.

Delovne postaje
Za ključne uporabnike je urejena sistemska centralna hramba podatkov in dokumentov. Uporabniki shranjujejo vse poslovne podatke in dokumente v mapo na omrežnem disku, ki je povezana v centralni sistem hrambe podatkov in dokumentov. Varovanje je urejeno z arhiviranjem v centralnem arhivskem sistemu. Uporabniki morajo za vse lokalno shranjene dokumente in podatke skrbeti sami z arhiviranjem na prenosljive medije (CD, DVD, USB, ipd.), ki jih primerno zaščitijo pred nedovoljenim dostopom. Za tako ustvarjen arhiv odgovarja uporabnik sam.

Mrežna infrastruktura

Konfiguracije komunikacijskih naprav so shranjene na centralnem mestu. Ob vsaki spremembi parametrov na komunikacijski opremi se naredi nova verzija varnostne kopije konfiguracijskih parametrov, s pomočjo katerih je mogoče ponovno vzpostaviti delovanje komunikacijskega omrežja.

Kontrola 11: Vzpostavljene so tehnične kontrole za preprečitev razširjanja in izvajanja škodljivih programov.

Preprečitev razširjanja in izvajanja škodljivih programov je izvedena z naslednjimi ukrepi:

- Dovoljena je uporaba le odobrene rešitve za zaščito pred virusi.
- Sprotno posodabljanje proti-virusnega programa:

  Konfiguracija proti-virusnega programa za avtomatsko obnavljanje varnostnih definicij se izvaja vsaj enkrat dnevno. Če avtomatska obnova preko mreže ni mogoča, je potrebno vzpostaviti postopek za ročno obnovo virusnih definicij vsaj enkrat tedensko.

  Konfiguracija proti-virusnega programa, da izvede preverjanje, se izvaja vsaj enkrat dnevno po obnovitvi varnostnih definicij in preverjanje celotnega sistema vsaj enkrat tedensko.

  Opombe: Če obstaja sum, da je na kateremkoli delu informacijsko-komunikacijskega sistema nameščena škodljiva programska oprema, je potrebno takoj obvestiti informacijskega varnostnega inženirja ali skrbnika, da pomaga zmanjšati škodo.

Kontrola 12: Informacije so med izmenjavo ustrezno zaščitene.

V internem omrežju so vzpostavljene kontrole, ki preprečujejo prestrezanje in spreminjanje podatkov na komunikacijski poti. Pri izmenjavi podatkov s tretjimi strankami je potrebno vedno uporabiti zaščitene komunikacijske poti (šifriranje, digitalni podpisi, …).

Kontrola 13: Pred objavo javno dostopnih informacij se vse informacije ustrezno preverijo, tako da se zagotovi pravilnost objavljenih podatkov.

Pred objavo informacij na spletni strani je potrebno informacije preveriti. V okviru rednega preverjanja ranljivosti omrežja se izvaja tudi pregled ranljivosti javno dostopnih strežnikov.

Kontrola 14: Razvijalci programske opreme morajo v okviru priprave končne različice produkta izvesti tudi proti-virusno preverjanje.

V implementaciji te zahteve mora biti vključeno naslednje:

- Pred prenosom aplikacije v produkcijsko okolje mora biti aplikacija varnostno preverjena.
- Varnostno preverjanje mora biti izvedeno tudi za popravke in nove različice že vpeljanih aplikacij.

Kontrola 15: Namestitev popravkov programske opreme mora biti izvedena v okviru odobrenega postopka upravljanja s spremembami (change management process).

Sprememba podatkov in programov ni dovoljena brez vnaprej načrtovane spremembe v skladu s postopkom upravljanja s spremembami, razen v primeru izrednega postopka za spremembe s strani pooblaščene osebe.

Kontrola 16: Nadzorne zapise je potrebno kreirati za sisteme, programe in mrežno opremo, kjer je to tehnično izvedljivo. V nadzornih zapisih je potrebno beležiti naslednje aktivnosti:

- Uspešni in neuspešni poskusi prijave.
- Uspešni in neuspešni poskusi dostopa do nastavitev operacijskega sistema (spreminjanje in/ali branje), ki odstopajo od splošno dovoljenih.
- Aktivnosti, ki jih izvaja administrator (npr. sprememba varnostne konfiguracije). Zbiranje teh zapisov mora biti vedno vključeno.
- Uspešne dodelitve in razrešitve IP naslovov na ustreznih mrežnih servisih.

Kontrola 17: Nadzorne zapise je potrebno kreirati za vse uspešne in neuspešne poskuse dostopa do informacijskih sredstev zavoda iz zunanjih lokacij.
Vsi zapisi morajo biti shranjeni na ločenem sistemu v omrežju zavoda. Izjeme za zbiranje nadzornih zapisov niso dovoljene. Zapise je potrebno tedensko (avtomatsko ali ročno) preveriti zaradi odkrivanja sistematičnih napadov.

Kontrola 18: Podatki o aktivnosti morajo vsebovati vsaj naslednje parametre: datum, čas, tip poskusa dostopa in identifikacijo uporabnika. Različni informacijski viri hranijo informacije v različnih formatih z različnimi parametri. Vsi informacijsko-komunikacijski sistemi hranijo najmanj zgoraj naštete parametre.

Kontrola 19: Ure na vseh informacijsko-komunikacijskih sistemih so usklajene z dogovorjenim časovnim virom.
Ure informacijskih virov znotraj zavoda se morajo sinhronizirati s centralno določenim časovnim virom na strežnikih v zavodu, ki se sinhronizira z zunanjimi strežniki.

2.4 Dostop do informacijskih sredstev

Cilj kontrol za dostop do informacijskih sredstev je zagotoviti dostop do informacij, zmogljivosti za obdelavo informacij in poslovnih procesov na podlagi poslovnih in varnostnih zahtev ter potreb.

Kontrola 20: Vsakemu uporabniku informacijsko-komunikacijske tehnologije v zavodu (zaposleni, udeleženci izobraževanja, zunanji sodelavci, zunanji izvajalci) je dodeljena unikatna oznaka.

Kontrola 21: Vzpostavljen je proces za dodeljevanje, spremembe in brisanje identifikacije uporabnikov.

Kontrola 22: Pooblastitev za skrbniški dostop do informacij temelji na poslovni potrebi ter jo določi lastnik informacijskega vira ali sistema.

Kontrola 23: Vzpostavljen je proces za redno letno preverjanje upravičenosti uporabnikov in drugih oseb , ki jim je dodeljena identifikacija za dostop do produkcijskih sistemov.

Kontrola 24: Identiteta uporabnika je overjena, preden uporabnik prične z uporabo informacijsko-komunikacijskega sistema ali aplikacije.

Kontrola 25: Gesla za privilegiran dostop so dostopna samo osebam, ki jih potrebujejo pri svojem delu in so vezana na osebo, če je to možno.

Kontrola 26: Gesla za večkratno uporabo, ki se uporabljajo za preverjanje identitete upoštevajo definirana navodila, če tehnologija to omogoča.

Kontrola 27: Gesla za večkratno uporabo, ki se uporabljajo za preverjanje identitete, so zaščitena.

Kontrola 28: Sistemi ali aplikacije, ki uporabljajo gesla za neposredno komunikacijo z drugimi sistemi ali aplikacijami, lahko uporabljajo gesla, ki ne zastarajo.

Kontrola 29: Vse nedejavne seje se po določenem času neaktivnosti prekinejo.

Kontrola 30: Dostop zunanjim sodelavcem in poslovnim partnerjem do internih informacijskih sredstev zavoda mora biti odobren s strani odgovorne osebe ter tehnično omejen na najmanjšo možno mero za izvedbo dogovorjenih opravil.

Kontrola 31: Dobavitelj ali odgovorna služba mora poskrbeti za varnostno nastavitev uporabniških virov, ki dovoli dostop le pooblaščenim uporabnikom, potrjenim s strani lastnika informacijskega vira.

Kontrola 32: Vzpostavljen je tehnični nadzor za preprečevanje nedovoljenega dostopa do zaupnih podatkov zavoda in osebnih podatkov zaposlenih na zavodu, poslovnih partnerjev, strank ter drugih zaupnih podatkov.

Kriterij usklajenosti

Upoštevanje kontrol, opisanih v razdelku »Natančen opis«, je obvezno.

- Odstopanja od kriterija morajo biti dokumentirana in potrjena s strani odgovorne osebe IKT in zavoda.

Implementacija

Vzpostavitev registra uporabniških identifikacij. Vzpostavitev postopka rednega letnega preverjanja uporabniških identifikacij.

Natančen opis

Kontrola 20: Vsakemu uporabniku informacijsko-komunikacijske tehnologije zavoda (zaposleni, udeleženci izobraževanja, zunanji sodelavci, zunanji izvajalci) je dodeljena unikatna oznaka. Sistemi avtentikacije v zavodu se upravljajo ločeno. Posamezen uporabnik ima lahko na različnih virih različno unikatno oznako. Dodeljevanje pravic temelji na zahtevkih odgovornih oseb.

Kontrola 21: Vzpostavljen je proces za dodeljevanje, spremembe in brisanje identifikacije uporabnikov. Dodeljevanje, spremembe in brisanje identifikacije uporabnikov poteka po postopku, ki je predpisan za posamezne sisteme oziroma vire. O dodeljevanju, spremembi in brisanju identifikacije uporabnikov odločajo lastniki informacijskih virov.

Postopki za zaposlene

Dodeljevanje uporabniškega računa:

- Kadrovska služba vnese osnovne podatke v kadrovski informacijski sistem za novo zaposlenega.
- Odgovorna oseba na članici za zaposlenega na podlagi poslovne potrebe in v okviru svojih pooblastil sestavi informacijske zahteve glede na delovno mesto, zadolžitve, funkcije in mandate in jih posreduje skrbniku sistema.
- Skrbnik sistema ustrezno uredi uporabniške pravice in dostope za uporabniški račun ter obvesti o izvršeni akciji kadrovsko službo in vodjo zaposlenega.

Brisanje uporabniškega računa:

- Vodja zaposlenega posreduje podatke za zaprtje uporabniškega računa skrbniku sistema.
- Poleg zahteve vodje zaposlenega lahko skrbnik preverja aktivnost zaposlenih v kadrovskem informacijskem sistemu ter v primeru prenehanja delovnega razmerja ali delovne vloge uporabniku odvzame pravice dostopa do informacijskih sistemov.
- Skrbnik sistema onemogoči dostop do uporabniškega računa in sproži postopke za ukinitev.

Sprememba uporabniškega računa:

- Vodja zaposlenega posreduje zahteve za spremembe skrbniku sistema.
- Skrbnik sistema ustrezno uredi uporabniške pravice in dostope za uporabniški račun in obvesti o izvršeni akciji vodjo zaposlenega.

Kontrola 22: Pooblastitev za skrbniški dostop do informacij temelji na poslovni potrebi ter jo določi lastnik informacijskega vira ali sistema.
Dodeljevanje pooblastila za skrbnika se izvaja po v naprej določenem procesu, ki vključuje:

- preverjanje potrebe,
- preverjanje nekaznovanosti,
- preverjanje potrebne izobrazbe in delovnih izkušenj.

Vsa pooblastila mora potrditi odgovorna oseba za informacijsko varnost. Pregled poslovnih potreb za ohranjanje pooblastil se izvaja vsaj enkrat letno. Odstranitev pooblastil se izvede v treh delovnih dneh po odkritju, da ni več poslovnih potreb ali prejemu ustreznega obvestila.

Kontrola 23: Vzpostavljen je proces za redno letno preverjanje upravičenosti uporabnikov in drugih oseb, ki jim je dodeljena identifikacija za dostop do produkcijskih sistemov.
Preverjanje upravičenosti dostopa do posameznega informacijskega vira se izvaja za vsak informacijski vir posebej. Za pregled podatkov so odgovorni lastniki informacijskih sredstev.

Kontrola 24: Identiteta uporabnika je overjena preden uporabnik prične z uporabo informacijsko-komunikacijskega sistema ali aplikacije.

V zavodu obstajajo naslednji načini overjanja:

- Digitalni certifikati (kvalificirano digitalno potrdilo) za uporabnike informacijsko-komunikacijskega sistema.

- Overjanje, ki je izvedeno v posameznih informacijskih rešitvah (npr. Eduroam, eAsistent ipd.).
- Overjanje za dostop do zunanjih aplikacij kot so npr. ZZZV, elektronsko bančništvo.

Avtentikacija uporabnika predstavlja samo začetno preverjanje. Na informacijskem viru se po osnovni avtentikaciji v imeniku LDAP izvaja avtorizacija dostopa do posameznih delov ali sklopov v okviru informacijskega vira.
Dostop do nekaterih informacijskih virov je lahko izveden z dodatno avtentikacijo in avtorizacijo.
V primeru neupravičenega dostopa lahko skrbnik onemogoči dostop do informacijskega vira ali ustrezno spremeni avtorizacijske pravice na informacijskem viru.
V primeru uporabe zunanjih aplikacij je potrebno varnostne pristope, avtentikacijo in nastavitve uporabniških profilov nastaviti v skladu s ponudnikom/skrbnikom aplikacije.

Kontrola 25: Gesla za privilegiran dostop so dostopna samo osebam, ki jih potrebujejo pri svojem delu in so vezana na osebo, če je to možno. Gesla za privilegiran dostop v informacijsko-komunikacijski sistem so dostopna samo osebam, ki jih potrebujejo pri svojem delu in so shranjena na varnem mestu (zapečatena kuverta). Vsak dostop do gesla je zabeležen.

Kontrola 26: Gesla za večkratno uporabo, ki se uporabljajo za preverjanje identitete, upoštevajo definirana navodila, če tehnologija to omogoča.

Kontrola 27: Gesla za večkratno uporabo, ki se uporabljajo za preverjanje identitete, so zaščitena.
Navodila za preverjanje identitete gesel so:

- Geslo je šifrirano; če šifriranje ni mogoče, je dostop do gesel omejen le na avtorizirane skrbnike sistemov.
- Gesla ne sme uporabljati več uporabnikov, razen če je zagotovljen nadzor in evidenca uporabe po uporabnikih.
- Za ponastavitev gesla je zagotovljen varen proces, ki vključuje preverjanje zahtevka za ponastavitev gesla.
- Privzeto uporabniško geslo, ki je nastavljeno ob namestitvi operacijskega sistema ali aplikacije, je potrebno spremeniti med ali takoj po namestitvi.
- Prenašanje gesla preko interneta, javnih omrežij ali brezžičnih omrežij je dovoljeno le v varnem načinu v šifrirani obliki.

Kontrola 28: Sistemi ali aplikacije, ki uporabljajo gesla za neposredno komunikacijo z drugimi sistemi ali aplikacijami, lahko uporabljajo gesla, ki ne zastarajo (non-expiring).
Neposredna komunikacija z drugimi sistemi ali aplikacijami poteka preko odobrenih komunikacijskih poti. Vsako novo komunikacijsko povezavo med informacijskimi sistemi mora odobriti varnostni inženir oz. skrbniki informacijsko-komunikacijskih sistemov, ki se povezujejo.

Kontrola 29: Vse nedejavne seje se po določenem času neaktivnosti prekinejo.
Nedejavne seje se po določenem času prekinejo. Čas je odvisen od kritičnosti sistema in ga določi lastnik vira. Uporabnik se mora po prekinitvi ponovno prijaviti.

Kontrola 30: Dostop do internih informacijskih sredstev mora biti odobren s strani odgovorne osebe ter tehnično omejen na najmanjšo možno mero za izvedbo dogovorjenih opravil.

Najmanj enkrat letno se opravi pregled vseh pravic in dostopov. Vsi nepotrebni dostopi do informacijskih sredstev zavoda se onemogočijo ali trajno izbrišejo. Pregled izvede lastnik informacijskega vira in rezultate posreduje odgovorna oseba za informacijsko varnost.

Kontrola 31: Dobavitelj ali odgovorna služba mora poskrbeti za varnostno nastavitev uporabniških virov, ki dovoli dostop le pooblaščenim uporabnikom, potrjenim s strani lastnika informacijskega vira. Pred prehodom v produkcijsko okolje je potrebno onemogočiti vsa privzeta uporabniška imena in spremeniti privzeta gesla na vseh sistemih. Dostop do informacijsko-komunikacijskega sistema je omogočen samo uporabnikom, ki dostop potrebujejo za opravljanje svojega dela.

Kontrola 32: Vzpostavljen je tehnični nadzor za preprečevanje nedovoljenega dostopa do zaupnih podatkov zavoda in osebnih podatkov zaposlenih na zavodu, poslovnih partnerjev, strank ter drugih zaupnih podatkov.
Dostop do zaupnih podatkov zavoda je dovoljen le tistim, ki ga potrebujejo in je izrecno odobren s strani odgovorne osebe zavoda. Dostop skupini je dovoljeno odobriti le, če vsi člani skupine potrebujejo dostop; če je le mogoče naj bo dostop urejen za posameznega člana. V primeru, da ni mogoče vzpostaviti tehničnega nadzora, je vzpostavljen proceduralni nadzor, vključno z dnevnikom sprememb in dostopa do podatkov.

2.5 Upravljanje incidentov

Cilj upravljanja incidentov je zagotoviti, da se dogodki in slabosti informacijsko-komunikacijskih sistemov sporočajo na centralno mesto. Na podlagi tako zbranih dogodkov se sprejemajo vse aktivnosti za hiter, učinkovit in urejen odziv na incidente pri varovanju informacij.

Kontrola 33: Vse incidente je potrebno prijaviti odgovorni osebi zavoda in skrbniku na predpisan način.

Kontrola 34: V primeru resnega varnostnega incidenta, kakor je: nedovoljen dostop do zaupnih ali občutljivih podatkov, sprememba ali ogrožanje celovitosti sistemov/strežnikov, odpovedovanje dostopnosti storitev (npr. DOS/DDOS), sprememba ali kvarjenje spletnih strani ali strežnikov, vdor ali poizkus vdora v sistem, uničenje podatkov, prevara, in podobno; je potrebno izvesti predpisane varnostne aktivnosti.

Kontrola 35: Če se pri varnostnem pregledu odkrije zlorabo pooblastil, morata biti o tem obveščena odgovorna oseba za informacijsko varnost in lastnik informacijsko-komunikacijskega sredstva.

<u>Kriterij usklajenosti</u>
Upoštevanje kontrol, opisanih v razdelku »Natančen opis«, je obvezno.

- Odstopanja od kriterija morajo biti dokumentirana in potrjena s strani odgovorne osebe IKT in zavoda.

Implementacija

Ažuren, natančen in verodostojen zapis incidentov, ki je dostopen le pooblaščenim osebam.

Natančen opis

Izvor varnostnega incidenta je lahko notranji ali zunanji. Varnostni incidenti se razlikujejo po obsegu, cilju in učinkih na poslovanje zavoda.

Kontrola 33: Vse incidente je potrebno prijaviti odgovorni osebi zavoda, varnostnemu inženirju in skrbniku na predpisan način. Uporabnik prijavi varnostni incident odgovorni osebi zavoda, ki preda prijavo skrbniku. Skrbnik odpravi napako in zabeleži intervencijo v dnevnik aktivnosti. Uporabnik po končani aktivnosti skrbnika potrdi odpravo incidenta. Vsi varnostni incidenti se beležijo v centralni register, ki ga vodi informacijski varnostni inženir.

Kontrola 34: V primeru resnega varnostnega incidenta, kakor so nedovoljen dostop do zaupnih ali občutljivih podatkov, sprememba ali ogrožanje celovitosti sistemov/strežnikov, odpovedovanje dostopnosti storitev (npr. DOS/DDOS), sprememba ali kvarjenje spletnih strani ali strežnikov, vdor ali poizkus vdora v sistem, uničenje podatkov, prevara, in podobno, je potrebno izvesti predpisane aktivnosti.

V primeru varnostnega incidenta se izvedejo naslednje aktivnosti:

- Odgovorna oseba zavoda obvesti informacijskega varnostnega inženirja, ki izvede preiskavo incidenta in izvede postopek za odpravo posledic incidenta.
- Z nastankom varnostnega incidenta se začne voditi dnevnik, ki vsebuje vse informacije in akcije, povezane z varnostnim incidentom. Za vsak vnos v dnevnik je potrebno dodati datum, čas in vir informacije.
- Če ni mogoče oceniti predvidenega časa izpada in se oceni, da je tveganje za zavod visoko, mora pooblaščeno osebje takoj pričeti z nadzorovanimi ukrepi za obvladovanje in zmanjšanje škode na poslovno informacijsko-komunikacijskem sistemu zavoda.
- Varnostne incidente, povezane s fizično varnostjo je potrebno javiti pristojni varnostni službi.

V primeru suma varnostnega incidenta ni dovoljeno:

- Nepooblaščeno izvajati preiskave, saj bi to lahko imelo za posledico uničenje sledi in ogrožanje preiskave.
- Obvestiti posameznike, pri katerih bi lahko bil izvor varnostnega incidenta. Vse aktivnosti je potrebno uskladiti z informacijskim varnostnim inženirjem.
- Poskusiti izvesti protinapad proti napadalcu. Tak postopek je nevaren in je lahko v nasprotju z zakonom.
- Poskusiti odstraniti ogroženost brez odobritve informacijskega varnostnega inženirja, kar bi lahko imelo za posledico uničenje sledi in ogrožanje preiskave.

Informacije o preiskavi varnostnih incidentov so dostopne le tistim, ki so do njih upravičeni. Zato ni dovoljeno razkrivati podatkov o preiskavi, njenega namena, podrobnosti ali rezultatov nikomur, razen v primeru, da informacijski varnostni inženir oz. odgovorna oseba odloči drugače. Prav tako ni dovoljeno brez odobritve odgovorne osebe zavoda razkriti nobene informacije komurkoli izven zavoda.

Kontrola 35: Če se pri pregledu varnosti odkrije zlorabo pooblastil, morata biti o tem obveščena informacijski varnostni inženir in lastnik informacijskega sredstva.

2.6 Upravljanje neprekinjenega poslovanja

Cilj upravljanja neprekinjenega poslovanja je zaščita kritičnih poslovnih procesov pred posledicami večjih okvar informacijsko-komunikacijskih sistemov ali nesreč ter zagotovitev pravočasnega ponovnega delovanja.

Kontrola 36: Lastniki informacijskih virov in vodstvo na osnovi tveganj, verjetnosti in pomembnosti posameznega informacijskega vira določijo prioritete, ki določajo čas ponovne vzpostavitve delovanja za posamezne dele informacijsko-komunikacijskega sistema.

Kontrola 37: Podrobni postopki za ponovno vzpostavitev delovanja informacijsko-komunikacijskega sistema so zapisani v posebnem dokumentu, ki je dostopen pooblaščenim osebam za njegovo kontrolo in izvajanje.

Kontrola 38: Predpisani postopki za ponovno vzpostavitev delovanja informacijsko-komunikacijskega sistema se testirajo ob vsaki večji spremembi informacijsko-komunikacijskega sistema ali vsaj enkrat letno.

Kriterij usklajenosti

Upoštevanje kontrol opisanih v razdelku »Natančen opis«, je obvezno.

- Odstopanja od kriterija morajo biti dokumentirana in potrjena s strani odgovorne osebe IKT in zavoda.

Implementacija

Dokument o predpisanih postopkih za ponovno vzpostavitev delovanja informacijsko-komunikacijskega sistema.

Natančen opis

Kontrola 36: Lastniki informacijskih virov in vodstvo na osnovi tveganj, verjetnosti in pomembnosti posameznega informacijskega vira določijo prioritete, ki določajo čas ponovne vzpostavitve delovanja za posamezne dele informacijsko-komunikacijskega sistema.
Prioritete posameznih kritičnih aplikacij glede na procese so določene v posebni preglednici. Vsebina preglednice se posodablja skladno z razvojem informacijsko-komunikacijskega sistema.

Kontrola 37: Podrobni postopki za ponovno vzpostavitev delovanja informacijsko-komunikacijskega sistema so zapisani v dokumentu o predpisanih postopkih za ponovno vzpostavitev delovanja informacijsko-komunikacijskega sistema, ki je dostopen pooblaščenim osebam za njegovo kontrolo in izvajanje.
Dokument o predpisanih postopkih za ponovno vzpostavitev delovanja informacijsko-komunikacijskega sistema vsebuje vse tehnične podrobnosti, potrebne za obnovo sistemov, vključno s kontaktnimi podatki vseh oseb, ki so potrebne za izvedbo aktivnosti za ponovno vzpostavitev informacijsko-komunikacijskega sistema.
Dokument o predpisanih postopkih za ponovno vzpostavitev delovanja informacijsko-komunikacijskega sistema se posodablja ob vsaki spremembi okolja na zavodu. Primeri sprememb, pri katerih je potrebno posodobiti dokument, so nakup nove opreme, nadgradnja sistemov, vpeljava novih funkcionalnosti v sisteme in spremembe tveganj.

Kontrola 38: Predpisani postopki dokumenta o predpisanih postopkih za ponovno vzpostavitev delovanja informacijsko-komunikacijskega sistema se testirajo ob vsaki večji spremembi informacijsko-komunikacijskega sistema ali vsaj enkrat letno. Testiranje se izvede s pomočjo vzpostavljenega testnega okolja za posamezne sklope ali v celoti, če to dopuščajo viri, ki so na voljo.

2.7 Združljivost

Cilj združljivosti je preprečiti kršitve zakonov in drugih zakonskih ali pogodbenih obveznosti in vsakršnih varnostnih zahtev.

Kontrola 39: Vsi osebni podatki so obravnavani kot to predvideva zakonodaja s področja varovanja osebnih podatkov.

Kontrola 40: Dostopi do zmogljivosti zavoda so opremljeni z opozorilom o dovoljeni uporabi in nedovoljenem dostopu oseb brez pooblastila.

Kontrola 41: Varnostni pregled informacijsko-komunikacijskih sistemov se mora izvajati redno v predpisanih intervalih.

Kontrola 42: Pregled varnostnih procesov mora biti izveden letno na reprezentativnem vzorcu različnih sistemov in lokacij.

Kriterij usklajenosti Upoštevanje kontrol, opisanih v razdelku »Natančen opis«, je obvezno.

- Odstopanja od kriterija morajo biti dokumentirana in potrjena s strani odgovorne osebe IKT in zavoda.

Implementacija
Izvedba neodvisnega varnostnega testiranja.

Natančen opis

Kontrola 39: Vsi osebni podatki so obravnavani kot to predvideva zakonodaja s področja varovanja osebnih podatkov.
Vse zbirke osebnih podatkov zavoda so prijavljene v registru zbirk osebnih podatkov. Pri varovanju se upoštevajo predpisane kontrole. Podrobneje je sistem varovanja osebnih podatkov opredeljen v Pravilniku o obdelavi osebnih podatkov vključno z zagotavljanjem varnosti osebnih podatkov in politiko varstva osebnih podatkov zaposlenih.
Kontrola 40: Dostopi zmogljivosti zavoda so opremljeni z opozorilom o dovoljeni uporabi in nedovoljenem dostopu oseb brez pooblastila.
Nepooblaščena uporaba zmogljivosti zavoda za neposlovne potrebe je brez posebne odobritve vodstva prepovedana. Vsako nepooblaščeno dejavnost je potrebno sporočiti nadrejenemu, ki je zadolžen za izvajanje nadaljnjih postopkov.

Kontrola 41: Varnostni pregled informacijsko-komunikacijskih sistemov se mora izvajati redno v predpisanih intervalih.

Varnostni pregledi se morajo izvajati v rednih časovnih intervalih v odvisnosti od strežnika:

Tip strežnika	**Varnostni pregled**
Spletni strežniki, splošno dostopni strežniki	vsake 3 mesece
Produkcijski interni strežniki	vsakih 6 mesecev
Ostali interni strežniki in mrežna oprema	vsako leto

Preverjanje mora vključevati najmanj naslednje elemente:

- Vse zahtevane kontrole morajo biti nastavljene in izvedene v skladu s tehničnimi navodili.
- Skrbniška pooblastila imajo le odobreni uporabniki.
- Dostop do virov operacijskega sistema imajo le odobreni uporabniki.
- Vsi zahtevani programi za zaščito pred zlonamernimi programi in kodo so nameščeni in delujoči.
- Zahtevano zbiranje nadzornih zapisov je vzpostavljeno.

Vsa ugotovljena odstopanja/nepravilnosti obravnava informacijski varnostni inženir in lastnik podatkov. Odgovorna oseba zavoda je o vseh nepravilnostih obveščena takoj.

Opombe: Internetni strežniki, za katere je odkrita ranljivost in le-ta ni odpravljena v definiranem časovnem okvirju, se morajo umakniti iz uporabe, dokler se ranljivost ne odpravi. Uporaba orodij za preverjanje ranljivosti s strani nepooblaščenih oseb, je prepovedana.

Kontrola 42: Pregled varnostnih procesov mora biti izveden letno na reprezentativnem vzorcu različnih sistemov in lokacij.

Pri pregledu varnostnih procesov je potrebno zajeti:

- Upravljanje uporabniških sredstev.
- Fizično kontrolo dostopa.
- Dostop do informacijskih sredstev:
  - administracijo uporabniških identifikacij in gesel (odobritev, odvzem, redni pregledi, ponastavitev gesel),
  - pooblastila za skrbniški dostop do informacij in sistemov.
- Zajem in pregled nadzornih zapisov:
  - hramba zahtevanih nadzornih zapisov.
- Integriteta informacijskih storitev in razpoložljivost:
  - upravljanje administracijskih in varnostnih pooblastil,
  - testiranje ranljivosti,
  - upravljanje nameščanja varnostnih popravkov,
  - nadzor in detekcija napačnih priklopov na sistem in sistematičnih napadov,
  - aktivacija neodobrenih sistemov in storitev.

Prehodne in končne določbe

Informacijska varnostna politika za področje IKT velja za vse zaposlene zavoda, ki skrbijo za informacijsko infrastrukturo.
Vsaka kršitev navodil v dokumentu se obravnava kot kršitev delovnih oziroma pogodbenih obveznosti.
Skrbniki informacijsko-komunikacijske tehnologije so dolžni v roku 18 mesecev po sprejemu varnostne politike zagotoviti spoštovanje pravil iz tega dokumenta.
Dokument prične veljati teden dni po objavi na spletni strani in oglasnih deskah zavoda.

Andrej Šušmelj, ravnatelj

Digitally signed by ANDREJ ŠUŠMELJ
Date: 2022.08.17 13:54:30 +02'00'

Številka delovodnika: 386-1/2022-2

Nova Gorica, 17.8.2022