POLITIKA ORGANIZACIJE INFORMACIJSKE VARNOSTI

Kazalo

1. NAMEN

Namen te politike je zagotoviti organiziran sistem varovanja informacij, skladen s strategijo in cilji TBP. S politiko zagotavljamo zahtevano celovitost, razpoložljivost in zaupnost informacij ter izvajamo ukrepe in kontrole za obvladovanje informacijskih varnostnih tveganj. Ti ukrepi in kontrole vključujejo politike, pravila, procese, postopke, organizacijsko strukturo in druge, za informacijsko varnost pomembne, elemente.

2. POLITIKA

2.1. NOTRANJA ORGANIZACIJA INFORMACIJSKE VARNOSTI

2.1.1. Vloge in odgovornosti

TBP ima za izvajanje, delovanje in upravljanje informacijske varnosti v varnostni politiki opredeljene in odobrene naslednje specifične vloge:

- Skrbnik SUVI, skrbništvo izvaja Predstavnik vodstva za kakovost
- Predstavnik vodstva za informacijsko varnost
- Pooblaščenec za upravljanje incidentov
- Skrbniki informacijskih virov

V obsegu SUVI se izvajajo še naslednje specifične naloge, ki so pomembne za izvajanje, delovanje in upravljanje informacijske varnosti:

- Upravljanje tveganj v sklopu posameznih procesov TBP oz. sistema vodenja kakovosti in
- Upravljanje fizične varnosti v sklopu Kadrovske službe.

2.1.2. Ločevanje vlog in odgovornosti

Z namenom zmanjševanja tveganj, povezanih z goljufijami, napakami in izogibanjem informacijskim varnostnim kontrolam, v TBP skrbimo, da se nasprotujoče si naloge dodeli različnim posameznikom. Na splošno smo predvsem pozorni, da en posameznik določene aktivnosti, ki jo izvaja, hkrati tudi ne nadzira. Nadalje pa ločevanje vlog in odgovornosti izvajamo pri naslednjih aktivnostih:

- predlog, odobritev in izvedba spremembe;
- zahtevanje, odobritev in izvajanje pravic dostopa;
- razvoj programske opreme in upravljanje produkcijskih sistemov;
- uporaba in upravljanje aplikacij;
- uporaba aplikacij in upravljanje podatkovnih zbirk;
- načrtovanje, revidiranje in zagotavljanje nadzora informacijske varnosti.

V primeru, da ločevanje vlog ni izvedljivo, mora TBP zagotoviti druge kompenzacijske kontrole, ki morajo biti dokumentirane.

2.1.3. Odgovornost vodstva

Za uspešno izvajanje procesov informacijske varnosti, vodstvo TBP s sklepom pooblašča in zadolžuje Predstavnika vodstva za informacijsko varnost. Njegova odgovornost je:

- zagotavljanje ozaveščenosti zaposlenih o varovanju informacij,
- zagotavljanje izobraževanja na področju varovanja informacij,
- zagotavljanje kvalitetnega izvajanja procesa varovanja informacij,
- koordinacijo med organizacijskimi enotami,
- obravnavanje varnostnih incidentov,
- medsebojno usklajenost in ustreznost varnostnih politik.

Nadalje pa lastniki procesov zagotavljajo:
- skrb za izvajanje varnostnih politik in vpeljanih kontrol,
- upravljanje tveganj v enoti in
- izvajanje vodstvenega nadzora v okviru svoje organizacijske enote.

Vodstvo zagotovi varno prijavo (zaščito) prijaviteljev/žvižgačev.

2.1.4. Stiki z organi oblasti

TBP vzdržuje ustrezne stike z organi oblasti. Predpisani so postopki, ki določajo, kdaj in kdo mora stopiti v stik z organi oblasti (npr. SI-CERT, organi pregona, gasilci, nadzorni organi) ter kako pravočasno poročati o ugotovljenih incidentih varovanja informacij, če obstaja sum, da je prišlo do kršitve zakonov.

2.1.5. Stiki z interesnimi skupinami

TBP vzdržuje tudi stike z različnimi zainteresiranimi skupinami in strokovnimi združenji z namenom izboljšanja znanja glede dobrih praks v zvezi z informacijsko varnostjo. Ravno tako na ta način izmenjujemo informacije o novih tehnologijah, grožnjah ali ranljivostih, hkrati pa nam je s tem omogočen dostop do strokovnega znanja in svetovanja v zvezi z informacijsko varnostjo.

2.1.6. Spremljanje in obveščanje o grožnjah (Threat intelligence)

Ustrezno zbiranje in obdelava obveščevalnih informacij o grožnjah TBP pomaga pri preprečevanju realizacije groženj oziroma pri pripravi odziva ob prvi pojavitvi z namenom zmanjšanja vpliva na delovanje TBP.

V TBP pri zbiranju informacij o varnostnih grožnjah združujemo strateški (vrste napadov in napadalcev), taktični (metodologije, orodja in tehnologije napadov) in operativni nivo (podrobnosti o napadih, vključno s tehničnimi indikatorji) spremljanja in obveščanja o varnostnih grožnjah. Glavni namen spremljanja in analiziranja varnostnih groženj je:
- izvajanje postopkov za vključitev zbranih informacij v proces ocenjevanja informacijskih varnostnih tveganj,
- vzpostavitev dodatnega orodja pri uporabi tehničnih preventivnih in zaznavnih kontrol,
- zagotovitev vhodnih informacij pri izvajanju postopkov testiranja informacijske varnosti.

Za spremljanje obveščevalnih podatkov je odgovoren Predstavnik vodstva za informacijsko varnost.

2.2. VODENJE PROJEKTOV

2.2.1. Informacijska varnost pri vodenju projektov

Pomemben element vseh projektov z IT podporo, ki jih planiramo in izvajamo v TBP, je obravnavanje varovanja informacij. Na ta način zagotovimo, da tveganja informacijske varnosti prepoznamo ter da le-ta upoštevamo tako pri načrtovanju kot pri izvedbi posameznih projektov z IT podporo.

Vsak projekt z IT podporo vsebuje naslednje elemente:
- cilji projekta morajo biti skladni s cilji varovanja informacij;
- pri načrtovanju posameznega projekta izvedemo oceno operativnih tveganj (in znotraj tega informacijskih varnostnih tveganj);
- v večje projekte se vključuje Predstavnik vodstva za informacijsko varnost;
- z zunanjim dobaviteljem in odjemalcem dogovorimo potreben nivo zagotavljanja varovanja informacij;
- stanje informacijske varnosti se v sklopu projekta redno pregleduje in po potrebi usklajuje.

Izvajanje kontrol varovanja informacij v okviru projektov z IT podporo je opredeljeno z metodologijo projektnega vodenja in natančno opisano v vsakokratnem vzpostavitvenem dokumentu projekta (plan razvoja novega izdelka, projektna naloga, ponudba zunanjega izvajalca). Za manjše projekte, kjer vzpostavitveni dokument ni predviden, tveganja in pripadajoče kontrole izhajajo iz vzpostavljenega SUVI.

2.3. UPRAVLJANJE INFORMACIJ IN SREDSTEV

2.3.1. Popis informacij in drugih povezanih sredstev

V TBP je vzpostavljen popis informacijskih virov. Popis informacijskih virov, ki ga vodi IT, sestavljajo naslednje kategorije informacijskih virov:

- fizične lokacije,
- strojna oprema,
- virtualni in logični strežniki,
- programska oprema,
- računalniško omrežje in aktivna omrežna oprema,
- človeški viri ter,
- informacije.

Posamezen informacijski vir je opremljen z navedbo skrbnika in opredelitvijo kritičnosti. Skrbniki informacijskih virov:

- so dolžni popis informacijskih virov ažurno posodabljati,
- morajo biti vključeni v proces ocenjevanja tveganj.

Za popis informacij so zadolženi lastniki informacij.

2.3.2. Sprejemljiva uporaba informacij in drugih povezanih sredstev

Zaposleni in zunanji uporabniki, ki uporabljajo ali imajo dostop do informacij in informacijskih virov TBP morajo biti seznanjeni z odgovornostmi in zahtevami glede varovanja in ustreznega ravnanja z informacijami in informacijskimi viri. S tem namenom je TBP sprejela Predpis o sprejemljivi uporabi informacij in informacijskih virov Obr.IP A5a-01/04. S predpisom morajo biti seznanjeni vsi zaposleni in zunanji uporabniki, ki uporabljajo ali imajo dostop do informacij in informacijskih virov TBP.

Predpis o sprejemljivi uporabi informacij in informacijskih virov Obr.IP A5a-01/04 vključuje vsaj:
a) pričakovano in nesprejemljivo vedenje uporabnikov z vidika informacijske varnosti;
b) dovoljeno in prepovedano uporabo informacij in informacijskih virov TBP;
c) aktivnosti nadzora, ki ga izvaja TBP.

2.3.3. Vračilo sredstev

Postopki vračila informacijskih sredstev ob prenehanju ali spremembi zaposlitve ali pogodbe o sodelovanju za zaposlene in uporabnike informacijskega sistema in informacij se v TBP izvajajo skladno s točko 2.5. Politike v povezavi s človeškimi viri. Vračilo sredstev vključuje uporabnikove končne naprave, prenosne naprave za shranjevanje podatkov, morebitno drugo specifično opremo, fizična in logična avtentikacijska sredstva za informacijske sisteme in prostore ter fizične kopije informacij.

Za izvajanje postopkov vračila informacijskih sredstev s strani zaposlenih (tudi specializanti, študentsko delo, praksa, honorarno delo, avtorsko delo in podobno) je odgovorna kadrovska služba. Za izvajanje postopkov vračila sredstev zunanjih izvajalcev je odgovoren posamezni skrbnik pogodbe zunanjega izvajanja.

2.3.4. Klasifikacija informacij

TBP ima vzpostavljen sistem klasifikacije informacij, ki upošteva zahteve glede zaupnosti, celovitosti in razpoložljivosti informacij. Klasifikacija in z njo povezane kontrole varovanja informacij, upošteva poslovne potrebe glede:

- izmenjave in/ali omejevanja dostopnosti informacij,
- varovanja celovitosti informacij,
- zagotavljanja razpoložljivosti ter
- pogodbenih in zakonskih zahtev glede zaupnosti, celovitosti ali razpoložljivosti informacij.

Sistem klasifikacije vključuje pravila za razvrščanje in merila za pregled razvrščanja v daljšem časovnem obdobju. Pravila za razvrščanje se posodablja v skladu s spremembami, ki vplivajo na vrednost, občutljivost in kritičnost informacij v njihovem življenjskem ciklu. Informacijska sredstva, s katerimi se obdelujejo informacije, se razvrstijo v skladu z razvrstitvijo informacij, ki so shranjene na sredstvu, obdelane ali zaščitene s sredstvom.

Za klasifikacijo informacij v TBP so zadolženi lastniki informacij.
Informacije v TBP delimo na:

- javne; namenjene vsem, tudi zunanjim javnostim,

- interne; namenjene vsem zaposlenim,
- zaupne; namenjene ozkemu krogu zaposlenih s potrebo po vedenju.

V primeru izmenjave dokumentov z drugimi organizacijami, ki imajo različno klasifikacijsko shemo, se je potrebno predhodno dogovoriti o označevanju informacij.

2.3.5. Označevanje sredstev

Glede na vzpostavljen sistem klasifikacije informacij se vse informacije in sredstva s katerimi se obdelujejo informacije ustrezno označuje. Glede na obliko informacij, je TBP kot ustrezne, prepoznala naslednje tehnike označevanja stopenj zaupnosti informacij:

- fizične nalepke,
- glava in noga dokumenta,
- metapodatki,
- vodni znak in
- žig.

Lastniki informacij posebej obravnavajo in določijo postopke:

- za primere, ko se označevanje lahko izpusti,
- za primere, ko zaradi tehničnih omejitev označevanje ni mogoče.

2.3.6. Prenos informacij

Za izmenjavo in prenos informacij v TBP uporabljamo različne komunikacijske zmogljivosti, od elektronske pošte, nalaganja vsebin z interneta, uporabe telefonov, do uporabe različnih nosilcev podatkov. Pri prenosu in izmenjavi informacij TBP zagotavlja zaščito informacij pred prestrezanjem, kopiranjem, spreminjanjem, napačnim usmerjanjem in uničenjem. Za zaščito zaupnosti in celovitosti zaupnih informacij uporabljamo kriptografske tehnike.

Zaposleni lahko izven omrežja TBP dostopajo do informacij, shranjenih na internih sistemih, samo ob uporabi varne povezave, ob upoštevanju dostopnih pravic do posameznih informacij oz. informacijskih sredstev.

Zaposlene redno opominjamo, naj se o zaupnih temah ne pogovarja na javnih mestih in ob prisotnosti nepooblaščenih oseb.

2.4. NADZOR DOSTOPA

2.4.1. Nadzor dostopa

V skladu s potrebami delovnih procesov so posameznemu uporabniku v TBP dodeljene pravice za dostop do prostorov in informacijskega sistema oziroma posameznih delov (dostop do strežnika, dostop do uporabniške aplikacije, podatkovne zbirke itd.).

Uporabnik dostopa do informacijskega sistema in pomembnih virov s pomočjo enega ali kombinacije naslednjih načinov:

- Uveljavljanje pravice dostopa na osnovi tega, kaj uporabnik ve (npr. uporabniško ime in pripadajoče geslo).
- Uveljavljanje uporabniške pravice na osnovi tega, kaj uporabnik ima (npr. identifikacijska kartica, ključ).
- Uveljavljanje pravice dostopa na podlagi tega, kje smo (npr. preprečitev dostopa s pomočjo varovanja in zaščite prostorov, omejevanje dostopa glede na lokacijo).

Uporabnik, ki pridobi pristopno pravico na podlagi enolično razpoznavnega uporabniškega imena ali na podlagi drugega ustreznega načina nedvoumnega razpoznavanja uporabnika, je odgovoren za vse dejavnosti, ki so registrirane (revizijska sled) z njegovim uporabniškim imenom. Svoje metode razpoznavanja uporabnik ne sme zaupati drugi osebi. V primeru upravičenega razkritja gesla uporabnik poskrbi za takojšnjo menjavo gesla.

Vsi posebni dostopi se obravnavajo kot izredni dostopi. Posebne dostope dobijo uporabniki, ki prevzamejo naloge upravljanja posameznega sistema. Vsi posebni dostopi morajo biti jasno vezani na posameznega uporabnika. Določitev nivoja posebnega dostopa je v pristojnosti neposrednega vodje zaposlenega.

Dostopi zunanjih izvajalcev, ki za izvajanje storitev potrebujejo dostop do omrežja TBP, se izvajajo in upravljajo skladno z Navodilom za VPN dostop Obr.IP A5a-01/05.

Za vzdrževanje učinkovitega nadzora dostopa do informacijskega sistema se izvajajo redne kontrole uporabniških dostopnih pravic.

2.4.2. Upravljanje identitet

Uporabniško ime za posameznega uporabnika, ki je v delovnem razmerju in je zaveden v kadrovski evidenci je kreiran na naslednji način:

- Uporabniška imena se tvorijo po sistemu ime in prva črka priimka.

Izjeme, kjer uporabniško ime ni sestavljeno na tak način, so:

- Uporabniška imena, ki imajo posebne pravice (privilegirani računi),
- glavno administrativno geslo,
- neimenska uporabniška imena, ki so potrebna za komunikacijo med različnimi aplikacijami in sistemi,
- uporabniška imena zaposlenih pri zunanjih izvajalcih.

2.4.3. Informacije za avtentikacijo (preverjanje pristnosti)

Z namenom zmanjševanja tveganja zlorabe gesel, nepooblaščenega dostopa, ogrožanja ali kraje informacij, so v TBP predpisana pravila za varno ravnanje z gesli, redno menjavo in izbiro kvalitetnih gesel. Ločujemo:

- Administratorska gesla - uporabljajo skrbniki za dostop do sistemov in aplikacij in jim omogočajo izvajanje skrbniških opravil, ki vključujejo tudi dodeljevanje in ukinitev pravic dostopa uporabnikom do sistemov, podatkov in aplikacij
- Uporabniška gesla - uporabljajo uporabniki za prijavo v računalniško omrežje in za dostop do aplikacij in informacij.

Geslo uporabnika sistema je namenjeno samo njegovi uporabi, zato so uporabniki sistemov odgovorni za vse akcije, ki se zgodijo z uporabo njihove identitete. Uporabniki s svojimi osebnimi gesli ravnajo kot s strogo zaupnimi informacijami in jih ne smejo razkrivati oziroma posojati drugim osebam. Če zaposleni zasledi malomarno ali zlonamerno ravnanje z gesli, to takoj sporočiti nadrejenemu. Geslo mora uporabnik spremeniti takoj, če obstaja sum na razkritje gesla, in o tem obvesti pooblaščeno osebo.

Sistemski skrbnik, ki je odgovoren za dodelitev začasnega gesla, zaposlenim posreduje začasno geslo na varen način. Uporabnik začasno geslo spremeni ob prvi prijavi. Gesla zaposleni ne smejo zapisovati na papir ali shranjevati na kakršenkoli drug način, ki bi drugi osebi lahko omogočil dostop do gesla.

Pri izbiri in menjavi uporabniških gesel se upoštevajo naslednja pravila:

- izbirati je potrebno gesla z najmanj 8 znakov ustrezne kompleksnosti
- znaki gesla naj vsebujejo eno malo in eno veliko črko ter vsaj eno številko
- gesla ne vsebujejo šumnikov
- gesla je potrebno menjati vsakih 12 mesecev
- vsaj 5 zaporednih gesel je neponovljivih
- geslo se zaklene za deset minut po petih nepravilnih poizkusih vnosa.

Enaka pravila veljajo za administratorska gesla.

Izjeme od pravila se beležijo.

2.4.4. Dostopne pravice

Pri dodeljevanju dostopnih pravic TBP upošteva naslednja temeljna načela upravljanja uporabniških dostopov:

- poslovne zahteve;
- varnostne zahteve;
- »potreba vedeti« (ang. need to know);
- klasifikacija posameznih informacij;
- prepovedi dostopa do vsega, kar ni posebej dovoljeno.

Pravice dostopa do informacij, aplikacij in sistemov, ki jih posameznik potrebuje glede na dodeljeno delovno mesto, so določena v sistemizaciji delovnega mesta. Dodatne oziroma posebne pravice določi in odobri lastnik posameznega vira. Odobreno zahtevo za dodelitev dostopa se posreduje odgovornim osebam - sistemskim skrbnikom, ki so zadolžene za dodeljevanje in ukinjanje pravic dostopa. Sistemski skrbniki dodelijo zahtevane pravice dostopa, nato pa obvestijo vlagatelja zahteve, da so bile pravice urejene. Sistemski skrbnik določi začetno geslo uporabniku, ki ga mora uporabnik ob prvi prijavo spremeniti v skladu s politiko gesel.

Dostopne pravice se zaposlenemu lahko spremenijo, ko je zaposleni prerazporejen na drugo delovno mesto ali je dobil v okviru obstoječega delovnega mesta nove zadolžitve. V tem primeru se zaposlenemu obstoječe pravice odvzame, nato pa se mu dodeli nove dostopne pravice, skladno s postopkom dodeljevanja pravic dostopa.

Pravice dostopa se uporabniku ukinejo:
- ob prekinitvi delovnega razmerja,
- v primeru zlorabe pravic,
- v primeru, da posameznik pri zunanjem izvajalcu ne opravlja več storitev vzdrževanja,
- ob poteku vzdrževalne pogodbe, če gre za zaposlene pri pogodbenih izvajalcih.
- Pri spremembi delovnega mesta (delovnih nalog)

Kadrovska služba, ki skrbi za dodeljevanje in odvzem pravic periodično (vsaj na 3 mesece), preverja, ali so bili za vse zaposlene, ki jim je prenehalo delovno razmerje, odvzete pravice. V primeru poteka pogodbe je skrbnik pogodbe odgovoren, da preveri, če so bili odvzete pravice zaposlenih pri pogodbenem partnerju.

Dostopne pravice do kritičnih informacijskih sistemov se za vse uporabnike pregledujejo letno. Skrbniki sistemov izpišejo aktivne uporabniške dostope v informacijske sisteme ali aktivne dostopne pravice za prostore. Sezname dostopnih pravic dobijo v pregled lastniki informacij, ki potrdijo ustreznost dostopov oziroma uredijo morebitna odstopanja (odvzamejo nepotrebna pooblastila). Skrbnik sistema na podlagi pregleda pripravi seznam za brisanje neaktivnih uporabnikov. Aktivnosti odobri posamezni lastnik tveganja na viru.

Za izvedbo rednih pregledov dostopnih pravic je odgovoren Predstavnik vodstva za informacijsko varnost.

2.5. UPRAVLJANJE DOBAVITELJEV

2.5.1. Informacijska varnost v odnosih z dobavitelji

TBP zagotavlja zaščito virov, ki so dostopni dobaviteljem, ter vzdrževanje dogovorjene ravni informacijske varnosti in izvajanja storitev. Pri tem se upošteva in zagotavlja:
- ugotavljanje potrebe po dobaviteljih in njihovo izbiro,
- vključitev dobaviteljev v sisteme upravljanja (kriteriji),
- spremljanje dogovorov o ravni storitve z dobavitelji,
- ocenjevanje in preverjanje ter
- urejanje razmerij z dobavitelji.

Kjer določenih vprašanj ta politika ne ureja, se zanje uporabljajo ustrezne določbe drugih informacijskih varnostnih politik in veljavne področne zakonodaje.

2.5.2. Informacijska varnost v pogodbah z dobavitelji

Dogovor o spoštovanju varnostnih zahtev za dobavitelje, ki jih določajo informacijske varnostne politike ter morebitne druge pravne podlage, se vključi v pogodbo, ki predstavlja pravno podlago za dostop dobavitelja storitev do podatkov oziroma informacijskih sistemov podjetja.

Zaradi zaupnosti podatkov, do katerih ima dostop dobavitelj, se določba o zaupnosti tako pridobljenih podatkov vključi v pogodbo o zunanjem izvajanju storitev oziroma, če se ta potreba pojavi naknadno, se sklene dogovor o zaupnosti pridobljenih podatkov – pogodba o vzajemnem varovanju poslovne skrivnosti (NDA). S takim dogovorom se dobavitelj storitev zaveže, da bo pridobljene podatke o organiziranosti podjetja, njegovi strojni, programski in drugi opremi, sistemih, omrežjih in druge podatke, katerih razkritje tretjim osebam bi lahko kakorkoli ogrozilo ali škodovalo podjetju ali drugim organizacijam ali osebam, s katerimi podjetje sodeluje, varoval kot poslovno skrivnost ter jih ne bo uporabljal na kakršenkoli način izven načina, dogovorjenega s pogodbo, v času trajanja te pogodbe in v določenem roku po njenem preteku.

Posamezne osebe dobavitelja, ki bodo izvajale storitev, morajo biti seznanjene s potrebnimi varnostnimi politikami naročnika, kar potrdijo s podpisom izjave o zaupnosti.

TBP vzdržuje register podpisanih NDA, ter register informacij, ki se izmenjujejo. Za vzdrževanje registrov je odgovorna nabava.

2.5.3. Upravljanje informacijske varnosti v IKT dobavni verigi

TBP daje posebno pozornost upravljanju informacijske varnosti v odnosih z dobavitelji IKT. Glavni namen je vzdrževanje dogovorjene ravni informacijske varnosti in zagotavljanje jasnega razumevanja obveznosti in odgovornosti glede izpolnjevanja relevantnih zahtev informacijske varnosti.

Pri upravljanju dobaviteljev IKT se upošteva predvsem:
- opredelitev zahtev za informacijsko varnost, ki se uporabijo v postopku nabave opreme ali storitev IKT;
- zahteve, da dobavitelji zagotavljajo varnostne zahteve tudi do morebitnih podizvajalcev;
- zahteve, da dobavitelji predložijo opis izvedenih varnostnih funkcij strojne ali programske opreme;
- zagotavljanje dokazil, da je dobavljena oprema skladna z navedenimi varnostnimi zahtevami;
- zagotavljanje sledljivosti za kritične sestavne dele in njihovo poreklo v celotni dobavni v verigi;
- zagotavljanje, da dobavljena oprema deluje v skladu s specifikacijo, brez kakršnih koli nepričakovanih ali neželenih funkcionalnosti;
- zagotavljanje pristnosti opreme;
- zagotavljanje, da oprema dosega zahtevane ravni varnosti
- opredelitev pravil za izmenjavo informacij v celotni dobavni verigi;
- izvajanje posebnih postopkov za upravljanje življenjskega cikla opreme in komponent, njihova razpoložljivost ter povezana varnostna tveganja.

Informatika TBP vodi evidenco dobaviteljev IKT. Evidenca se redno pregleduje, da se zagotovi posodabljanje pogodb v primeru sprememb, ki vplivajo na zagotavljanje ustrezne ravni varovanja informacij.

2.5.4. Spremljanje, pregledovanje in upravljanje sprememb storitev dobaviteljev

V medsebojne pogodbe z dobavitelji se smiselno vključi zahteve o nivoju zagotavljanja storitev (SLA). Določi se metriko in sprejemljiva odstopanja, kakor tudi ukrepe v primeru neizpolnjevanja dogovorjenih nivojev. Za spremljanje in merjenje je odgovorna kontaktna oseba, navedena v pogodbi.

Preverjanje dobaviteljev se izvaja preko merjenj SLA. V primeru, da gre v pogodbenem odnosu za večja tveganja zaupnosti, celovitosti in razpoložljivosti, je potrebno v pogodbo z dobaviteljem vključiti tudi dogovore o pravici do pregleda na lokaciji dobavitelja, kakor tudi pogoje, način in obseg le-teh.

Kadar TBP menja dobavitelja oziroma dobavitelj spremeni storitev ali nivo zagotavljanja storitev, je treba izvesti oceno tveganja spremembe. Zagotoviti je treba ustrezne kontrole, da se tveganja zmanjša na sprejemljiv nivo.

2.5.5. Informacijska varnost uporabe storitev v oblaku

V TBP so vzpostavljeni postopki za pridobitev, uporabo, upravljanje in izhod iz storitev v oblaku v skladu z zahtevami glede informacijske varnosti.

Na področju pridobivanja storitev v oblaku mora TBP:
- Opredeliti varnostne zahteve v povezavi z varovanjem informacij pri rabi storitev v oblaku.
- Opredeliti potreben obseg uporabe oblačnih storitev in vzpostaviti kriterije na podlagi katerih se izvaja izbiro ustreznega ponudnika storitev v oblaku.
- Določiti vloge in odgovornosti pri upravljanju storitev v oblaku.
- Opredeliti katere kontrole varovanja informacij morajo biti upravljane s strani ponudnika oblačnih storitev.

Rešitve storitev v oblaku morajo temeljiti na standardih za računalniško arhitekturo in infrastrukturo, poleg tega pa je potrebno s strani posameznega ponudnika pridobiti ustrezna zagotovila o izpolnjevanju vseh zahtev v povezavi z varovanjem informacij. Ponudnik naj se obveže tudi do zgodnjega obveščanja v primeru večjih tehničnih ali infrastrukturnih sprememb, geografskih in pravnih pristojnosti ter sprememb na strani pogodbenih izvajalcev. Določene morajo biti obveznosti ponudnika ob izstopu, še zlasti razpoložljivost in podpora.

Zagotovljena mora biti kontrola nad upravljanjem dostopnih pravic ter spremljanje in zaščita pred zlonamerno programsko opremo. Opredeljena mora biti tudi odgovornost ponudnika za upravljanje varnostnih kopij ter zagotavljanje in vračanje informacij na zahtevo (v sklopu zagotavljanja storitev), kot tudi ob izstopu.

Zagotoviti je potrebno neposredno podporo ponudnika storitev v oblaku v primeru incidentov na področju varovanja informacij, z možnostjo pridobivanja dokaznega gradiva.

Hranjenje in vsakršna oblika obdelave osebnih podatkov se mora izvajati znotraj zakonsko določenih geografskih območij.

Izvaja se upravljanje, spremljanje in nadzor nad storitvami v oblaku:

- TBP mora, zlasti v primeru večjega števila storitev (ponudnikov), zagotoviti procese za nadzor kontrol, vmesnikov in sprememb storitev v oblaku.
- Zagotoviti je potrebno procese za upravljanje incidentov v povezavi z varovanjem informacij.
- Storitve v oblaku morajo biti obravnavane v oceni tveganja.
- Storitve v oblaku morajo biti redno spremljane, obravnavane med presojami in ustrezno ocenjevane.

Potrebno je zapisati jasno izhodno strategijo v primeru večjih sprememb in prekinitev izvajanja oblačnih storitev. Strategija mora upoštevati običajno splošnost in togost pogodb na področju storitev v oblaku, ki ob izhodu ne dopuščajo pogajalskih principov.

2.6. UPRAVLJANJE VARNOSTNIH DOGODKOV IN INCIDENTOV

TBP je s Politiko upravljanja incidentov vzpostavila proces upravljanja informacijskih varnostnih dogodkov in incidentov. Poleg upoštevanja dobrih praks standardov informacijske varnosti, se s Politiko upravljanja incidentov upošteva tudi zakonodajne zahteve glede informacijske varnosti, s poudarkom na odzivanju na varnostne incidente.

2.7. NEPREKINJENO VAROVANJE INFORMACIJ

2.7.1. Informacijska varnost med prekinitvami

TBP je vzpostavila Politiko neprekinjenega poslovanja. Pri načrtovanju neprekinjenega poslovanja upošteva tudi zagotavljanje neprekinjene informacijske varnosti med prekinitvami, kjer izvaja in vzdržuje:

- kontrole informacijske varnosti, podporne sisteme in orodja v okviru neprekinjenega poslovanja in IKT načrtih neprekinjenega delovanja;
- postopke za ohranjanje obstoječih kontrol informacijske varnosti med prekinitvami;
- nadomestne ukrepe informacijske varnosti, za tiste ukrepe, ki jih ni mogoče ohraniti med motnjami.

2.7.2. IKT pripravljenost za neprekinjeno poslovanje

Okrevalni načrt storitev IKT se podrejajo in so neločljivi del načrtov neprekinjenega poslovanja, opredeljenega v Politiki neprekinjeno poslovanje. Zahteve glede okrevalnih načrtov za storitve IKT so opredeljene s pomočjo rezultatov analize vpliva na poslovanje (BIA). Z izvedbo analize vpliva na poslovanje so določene ključne potrebe, ki so pomembne za vzpostavljanje in zagotavljanje nemotenega delovanja:

- Določi se finančne in druge podatke o posledicah na poslovanje v primeru nepredvidenih dogodkov, ki vplivajo na delovanje informatike
- Določi se pomembnost informacijskih procesov, aplikacij in podatkov
- Določi se prednostne dejavnosti s pripadajočima RTO – ciljni čas vzpostavitve delovanja sistema in RPO – ciljna točka obnavljanja podatkov
- Zagotovi se seznam oz. popis informacijskih sredstev z določeno kritičnostjo.

Okrevalni načrt storitev IKT je potrjen s strani vodstva in kot neločljivi del sledi strategiji ter zagotavlja neprekinjenost poslovanja procesov po prioritetah, določenih v Politiki neprekinjenega poslovanja.

Okrevalni načrti so izdelani za vse kritične IKT storitve.

V TBP je vzpostavljena organizacijska struktura oz. enota za pripravo na motnjo, ublažitev in odziv na motnjo, ki je podprta z osebjem s potrebnimi odgovornostmi in usposobljenostmi.

2.8. SKLADNOST

2.8.1. Zakonske in pogodbene zahteve

Politika TBP, kot tudi celotno njeno delovanje, se izvaja v skladu s sprejetimi zakonskimi in podzakonskimi akti ter s primarno in sekundarno zakonodajo EU. Vodstvo se zavezuje in zagotavlja, da je poslovanje v skladu z vso veljavno zakonodajo in ostalo relevantno regulativo. V zvezi z varovanjem informacij še posebej upoštevamo:

- Zakon o informacijski varnosti
- Zakon o varstvu osebnih podatkov
- Zakon o delovnih razmerjih
- Zakon o avtorskih in sorodnih pravicah
- Zakon o kritični infrastrukturi

V primeru sprememb zakonodaje, preverimo in uskladimo dokumentirani sistem upravljanja varovanja informacij.

Vsa pogodbena razmerja TBP morajo biti pripravljena skladno z zakonodajo in dobrimi praksami poslovanja. Kadar pogodbene zahteve posredno ali neposredno vplivajo na varnost informacij, mora pogodbo pred podpisom pregledati tudi Predstavnik vodstva za kakovost. Upravljanje odnosov z dobavitelji se izvaja skladno s poglavjem 2.5. tega dokumenta.

2.8.2. Pravice intelektualne lastnine

Pri uporabi in upravljanju strojne in programske opreme TBP spoštuje pravice intelektualne lastnine, kot jih zahteva nacionalna regulativa in mednarodna dobra praksa.

2.8.3. Zaščita zapisov

TBP ščiti zapise pred izgubo, uničenjem, ponarejanjem, nepooblaščenim dostopom in nepooblaščenim izdaje. Vsi opredeljeni zapisi morajo biti in ostati čitljivi ter prepoznavni. Dostop do zapisov v elektronski obliki je urejen skladno z določili za upravljanje nadzora dostopa v točki 2.4.1. tega dokumenta.

Evidenco in izločanje iz hranjenja izvaja lastnik zapisa. Vsi zapisi, ki se nahajajo v papirni obliki, se uničujejo z nadzorovanim razrezom. Izločanje iz arhiva in uničenje zapisov se popiše v zapisniku izločanja dokumentacije iz arhiva.

Zapisi se hranijo, dokler obstaja zakonska zahteva oziroma je dosežen namen hranjenja le-teh. Za določanje roka hrambe je odgovoren lastnik informacij.

2.8.4. Zasebnost in zaščita osebnih podatkov

TBP ima imenovano Pooblaščeno osebo za varstvo podatkov.

TBP se pri svojem poslovanju srečuje z osebnimi podatki zaposlenih, podatki strank in posebnimi vrstami osebnih podatkov. Vsi osebni podatki so obravnavani kot zaupni, ne glede na to, ali je stopnja zaupnosti označena ali ne. Pri tem se vedno spoštujejo določila relevantne zakonodaje (ZVOP) kot tudi načela pričakovane zasebnosti komuniciranja in pričakovane zasebnosti na delovnem mestu skladno z zahtevami Ustave RS in evropsko regulativo.

2.8.5. Neodvisni pregledi informacijske varnosti

Neodvisni pregledi informacijske varnosti v TBP, ne glede na način izvajanja (notranji ali zunanji), morajo biti natančno planirani, ne smejo motiti delovnih procesov bolj, kot to zahteva skrbno zbiranje podatkov in preverjanje izvajanja politike. Pregledi informacijske varnosti so nujni, morajo se uveljaviti in ponavljati. Rezultati pregledov morajo biti predstavljeni v okviru vodstvenih pregledov.

Notranji pregledi se praviloma izvajajo v sklopu notranje presoje sistemov vodenja. Zunanje preglede izvajajo predvsem inšpekcijske službe. Poleg z zakonom določenih nadzorstev, lahko zunanje preglede izvajajo tudi zunanji revizorji po naročilu vodstva TBP oziroma iz drugih poslovnih razlogov, kot so na primer zahteve kupcev.

2.8.6. Skladnost s politikami, pravili in standardi informacijske varnosti

TBP se je zavezala, da bo poslovala skladno s priporočili standarda sistema upravljanja varovanja informacij TISAX oz. ISO/IEC 27001. S tem namenom je v varnostnih politikah, delovnih postopkih in navodilih dokumentirala pravila upravljanja informacijske varnosti, da se zagotavlja zaupnost, celovitost in razpoložljivost informacij.

V ta namen predstavnik vodstva za SUVI in predstavnik vodstva za kakovost redno spremljata ustreznost poslovanja glede na zahteve standarda ter po potrebi predlagajo spremembe politik. Odgovorne osebe redno poročajo o stanju na področju skladnosti na vodstvenih pregledih ter v primeru, da so stopnje tveganja zaradi zaznanih neskladij nesprejemljive, takoj neposredno poročajo vodstvu TBP.

2.9. DOKUMENTIRANOST OPERATIVNIH POSTOPKOV

V TBP so vzpostavljeni in dokumentirani postopki za nameščanje, zaklepanje, zagon in zaustavitev računalnikov, varnostno kopiranje, vzdrževanje opreme, ravnanje z nosilci podatkov, upravljanje računalniških sob, ravnanje z elektronsko pošto in podobno.

V delovnih postopkih smo podrobno definirali poteke izvajanja vsakega dela, vključno:
- z obdelavo in ravnanjem z informacijami;
- z varnostnim shranjevanjem podatkov,
- z navodili za ravnanje v primeru napak, izpadov ali drugih izrednih razmer, ki se lahko pojavijo med delovanjem,
- z iskanjem pomoči v primeru nepričakovanih tehničnih težav,
- s posebnimi navodili za ravnanje z izpisi in nosilci podatkov,
- s postopki za ponovni zagon in reševanje sistema po zastoju,
- z upravljanjem s presojnimi sledmi in informacijami iz dnevnika o delovanju sistema.

Delovne postopke obvladujemo po postopku za obvladovanje dokumentov, katerih izdajo in spremembe odobrijo pristojne osebe.

Za pripravo in posodabljanje delovnih postopkov so odgovorni neposredni izvajalci oziroma lastniki virov.

Lenart, 13.12.2023

Uprava TBP d.d.
Direktor družbe

Danilo ROJKO