POLITIKA V POVEZAVI S ČLOVEŠKIMI VIRI

Kazalo

1. NAMEN

Namen te politike je zagotoviti ustrezno obvladovanje tveganj v povezavi s človeškimi viri za zagotavljanje ustrezne razpoložljivosti, kompetenc in pooblastil, upravljanje izvajanja varnostnih postopkov ter opredeljuje dolžnosti in pravice zaposlenih in uporabnikov informacijskega sistema v postopkih:

- pred zaposlitvijo,
- med zaposlitvijo ter
- ob prekinitvi oz. spremembi zaposlitve.

Politika v povezavi s človeškimi viri velja za redno zaposlene in tiste, ki delo opravljajo po kakršni koli drugi pogodbi (npr.: honorarno delo, študentsko delo, avtorska pogodba in podobno) in imajo dostop do informacij TBP.

2. POLITIKA

2.1. PREVERJANJE KANDIDATOV ZA ZAPOSLITEV

Pred zaposlitvijo mora kadrovsko-pravna služba ustrezno in v okviru zakonskih omejitev (glede na zahteve delovnega mesta) preveriti primernost kandidatov. Posebno pozornost je treba posvetiti pri vodilnih delovnih mestih ter delovnih mestih, kjer se obdelujejo zaupni poslovni podatki ter osebni podatki in posebne vrste osebnih podatkov. Kandidata za novo zaposlitev se predhodno seznani z možnostjo preverjanja podatkov in za to pridobiti njegovo pisno privolitev.

Ravno tako se preverjanje smiselno izvaja pri zunanjih partnerjih.

2.2. POGOJI ZAPOSLITVE

V pogodbi o zaposlitvi ali uporabi informacijskega sistema in informacij morajo biti jasno opredeljena načela varovanja informacij oziroma mora biti podan sklic na dokumentacijo SUVI in sankcije v primeru kršenja pravil krovne varnostne politike in njenih podrejenih dokumentov.

Varovanje informacij se začne že pred samo zaposlitvijo ali uporabo informacijskega sistema in informacij, traja ves čas zaposlitve ali uporabe informacijskega sistema in se mora zagotavljati tudi po koncu zaposlitve ali uporabe informacijskega sistema TBP in naših kupcev.

2.3. IZOBRAŽEVANJE IN OZAVEŠČANJE O INFORMACIJSKI VARNOSTI

Vsi zaposleni in uporabniki informacijskega sistema morajo biti ustrezno izobraženi glede določil dokumentacije SUVI. Izobraževanje se opravi ob prihodu novega zaposlenega in je vključeno v program usposabljanja novozaposlenega (Obr.IP B7a-01/01 ali Obr.IP B7a-01/02) ali uporabnika informacijskega sistema ter vsaj 1-krat na leto obnavlja v sklopu letnih izobraževanja »Kakovost & Mi« oziroma takrat, ko je to potrebno zaradi spremembe varnostnih politik, postopkov ali navodil. Izobraževanja so obvezna za vse zaposlene. Preverjanje uspešnosti izobraževanj oziroma usposabljanj se lahko izvaja z različnimi načini preverjanja znanja udeležencev izobraževanj oziroma usposabljanj, kar podrobneje določa interni predpis procesa Človeških virov (IP B7a-01.xx). Vsebina izobraževanj in usposabljanj je opredeljena v ločenem dokumentu, gradivu »Kakovost & Mi«.

Kadrovsko-pravna služba vodi evidenco planiranih in izvedenih izobraževanj. O uspešnosti izobraževanj redno poroča na vodstvenih pregledih.
Ustrezno ozaveščanje in izobraževanje o varovanju informacij se lahko zahteva tudi od zunanjih partnerjev.

2.4. DISCIPLINSKI POSTOPEK

V primeru kršitve krovne varnostne politike in njenih podrejenih dokumentov ima delodajalec možnost, glede na okoliščine posameznega primera, sprožiti postopek odpovedi pogodbe o zaposlitvi v skladu z zakonodajo. V primeru kršitve varnostnih politik, se v TBP izvaja disciplinski postopek, skladen z Zakonom o delovnih razmerjih.

Vsako neupoštevanje pravil krovne varnostne politike in njenih podrejenih dokumentov se šteje za kršitev pogodbe o zaposlitvi oziroma civilnopravne pogodbe, na podlagi katere se opravlja delo ali pogodbe o sodelovanju in se kot tako tudi sankcionira. Za kršitve pogodbe o zaposlitvi se izvede ustrezen disciplinski proces, ki je skladen z zahtevami *ZDR-1.*

V primerih suma kršitve ali zlorabe s strani zaposlenega ali uporabnika informacijskega sistema se lahko izvede postopek takojšnje ukinitve uporabniških pravic in dostopov. Takšen postopek lahko sproži samo vodstvo TBP ali od njega pooblaščena oseba.

2.5. ODGOVORNOSTI OB PRENEHANJU ALI SPREMEMBI ZAPOSLITVE

Odgovornosti in obveznosti, ki veljajo tudi po koncu zaposlitve, morajo biti vključene v pogodbe o zaposlitvi ali pogodbi o sodelovanju oziroma ob dogovoru, sklenjenem ob prekinitvi zaposlitve – del t.i. razdolžne liste. Vsi zaposleni ter uporabniki informacijskega sistema in informacij morajo ob koncu zaposlitve ali pogodbe vrniti vsa informacijska sredstva TBP, ki so jih prejeli v uporabo, kar se navede na razdolžni listi ter s podpisom le-te potrdi vodja informatike. Vsem zaposlenim ter uporabnikom informacijskega sistema se ob koncu zaposlitve odvzame vse pravice fizičnega in logičnega dostopa do informacij.

V primeru potrebe po takojšnji ukinitvi pravic, zahtevek sproži vodstvo TBP ali od njega pooblaščena oseba.

V primeru spremembe delovnega mesta, kadrovsko-pravna služba ustrezno poda zahtevek za ukinitev pravic starega in dodajanje pravic novega delovnega mesta. Ravno tako poskrbi za ustrezen prenos opreme (vračilo, preknjiženje, dodelitev nove opreme).

2.6. ZAUPNOST IN DOGOVORI O NERAZKRIVANJU

Vsi zaposleni, ne glede na obliko zaposlitve, so dolžni varovati zaupne podatke vseh stopenj zaupnosti, za katere zvedo med trajanjem delovnega razmerja, tako v času trajanja delovnega ali drugega pogodbenega razmerja kot tudi po prenehanju delovnega ali drugega pogodbenega razmerja v ali izven prostorov podjetja. Pri tem upoštevajo določila Pravilnika o varovanju poslovne skrivnosti, zaupnih podatkov ter o varovanju dokumentiranega gradiva TBP d.d.

Vsi zaposleni in vsak, ki na novo sklene delovno razmerje, mora podpisati Izjavo o varovanju informacij. Podpis izjave je pogoj za začetek opravljanja dela.

Vsi, ki s podjetjem sodelujejo na podlagi drugačnega pogodbenega razmerja (študentsko delo, praksa, honorarno delo, avtorsko delo in podobno), se obravnavajo kot zaposleni in morajo podpisati enako Izjavo, s katero se dogovori zaupnost podatkov med TBP in izvajalcem. Zanje veljajo iste obveznosti varovanja informacij vseh stopenj zaupnosti. Upravljanje informacijske varnosti v razmerjih z zunanjimi partnerji je dodatno opredeljeno v Politiki organizacije informacijske varnosti.

Vse podpisane izjave se vodijo v kadrovski mapi ali mapi, kjer se hranijo pogodbe z zunanjimi partnerji.

2.7. DELO NA DALJAVO

Na delovnih mestih, kjer to delovni proces omogoča, lahko zaposleni izvajajo delo na daljavo. Zaposleni so pri delu na daljavo dolžni spoštovati enaka pravila varovanja informacij, kot veljajo pri delu v prostorih TBP. Pri tem so posebej pozorni na izvajanje pravil:

- uporabe odobrenih naprav / prepoved uporabe zasebnih naprav,
- uporabe varne povezave za dostop do IT okolja TBP,
- politike čiste mize in čistega zaslona,
- fizične varnosti naprav (v zasebnih in javnih prostorih ter med prenosom),
- preprečevanja nepooblaščenega dostopa do naprav in informacij in
- uporabe naprav v zasebnih in javnih omrežjih.

Zunanji partnerji, ki potrebujejo dostop do virov v omrežju TBP, dostopajo do le-teh skladno z dokumentom Navodilo za VPN dostop Obr.IP A5a-01/05. Ostale zahteve glede varovanja informacij, vključno s sporočanjem zaznanih informacijskih varnostnih dogodkov in incidentov, so s posameznim zunanjim partnerjem dogovorjene v pogodbi.

2.8. POROČANJE O INFORMACIJSKIH VARNOSTNIH DOGODKIH

TBP zagotavlja ustrezne mehanizme, s pomočjo katerih lahko vsi uporabniki javljajo zaznane informacijske varnostne dogodke in incidente. Kjer je to smiselno, mora TBP zagotoviti tudi anonimnost prijav. Ostale določbe so opredeljene v postopku upravljanja incidentov.

Lenart, 13.12.2023

Uprava TBP d.d.
Direktor družbe

Danilo ROJKO