POLITIKA FIZIČNE VARNOSTI

Kazalo

1. NAMEN

Namen te politike je zagotoviti ustrezno obvladovanje tveganj v povezavi z varovanjem prostorov in opreme, informacij v fizični obliki in nosilcev elektronskih informacij v prostorih TBP in izven tega območja. S politiko zagotavljamo zahtevano razpoložljivost in zaupnost.

Politika fizične varnosti 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. VARNOSTNA OBMOČJA

TBP ima določene tri vrste varnostnih območij:
- javna območja,
- interna območja ter
- varovana območja.

Javna območja so namenjena vsem, tudi zunanjim obiskovalcem. Po javnih območjih se lahko vsi gibljejo neomejeno.

Interna območja so namenjena izključno zaposlenim s potrebo po dostopu. Območja so varovana s pristopno kontrolo, so nedostopna neposredno od zunaj. Gibanje obiskovalcev in ostalih nepooblaščenih oseb se lahko izvaja le ob predhodni najavi in ob spremstvu pooblaščene osebe.
Poseben režim v okvirju internih območij velja za pogodbene partnerje:
- ki s svojim osebjem izvajajo prevoze blaga (šoferje);
- ki s svojim osebjem izvajajo poštarske in druge sorodne storitve pošiljanja pisemskih in paketnih pošiljk;
- serviserje opreme, katera se nahaja na območju TBP (kavni avtomati, avtomati s hrano in pijačo);

Osebju tovrstnih pogodbenih partnerjev TBP ob vstopu poda navodila (shemo) z označenimi dovoljenimi območji gibanja njihovega osebja, katero se omeji na nujno potrebne površine za opravljanje njihove dejavnosti ter dolžnostjo varovanja informacij. Lahko pa namesto tega tovrstnim pogodbenim partnerjem TBP posreduje pisno obvestilo, ki zajema prej navedeno.

Varovana območja so strožje varovana, s posebno pristopno kontrolo, protivlomnim alarmom in video nadzorom. Nepooblaščenim je vstop v varovana območja prepovedan, razen v primeru posebnih potreb. V tem primeru mora priti do potrditve s strani pristojne osebe. Ves čas mora biti taka oseba pod nadzorom. Vnos naprav, ki lahko zajemajo zvok in sliko (telefoni, kamere, foto aparati…) je prepovedan. V primeru potrebe po zajemu slikovnega materiala (npr. za potrebe promocij, marketinga…) mora dovoljenje izdati direktor TBP.
Vsi obiskovalci morajo v času vstopa v interna in varovana območja nositi jasne oznake, ki jih ločijo od zaposlenih.

Vsi zunanji obiskovalci morajo biti seznanjeni s pogoji vstopa, zabeležen mora biti datum in čas vstopa ter izstopa. V primeru vstopa vozil se evidentira tudi registrska številka vozila.

2.2. PRISTOPNA KONTROLA

Vsa interna in varovana območja so od javnih območij ločena s pristopno kontrolo. Upravljanje pravic dostopa za zaposlene poteka preko kadrovske službe po načelu minimalnih potrebnih pravic, pri čemer kadrovska služba določi krog oseb (po delovnem mestu ali vključenosti v posamezen oddelek), ki imajo posebne pravice in pogoje dostopa.
Pristopna kontrola se izvaja s pomočjo brezkontaktnih kartic in ključev. Kjer se za dostop uporabljajo ključi, mora odgovorna oseba voditi seznam izdanih ključev.
Za varovana območja je potrebno zagotoviti tudi evidenco vstopov in izstopov.

2.3. VAROVANJE PISARN IN OSTALIH POMEMBNIH PROSTOROV

Dostop do pomembnih prostorov mora biti ustrezno varovan. Varovana območja niso dostopna neposredno iz javnih površin. Oznake takih prostorov naj ne razkrivajo vsebine. Za večjo raven zaščite se smiselno uporabijo še sistemi mehanske zaščite (protivlomna stekla, ognjevarne blagajne, varnostne ključavnice itd)

2.4. FIZIČNI NADZOR

Prostori z vsebino morajo biti ustrezno tehnično varovani. V ta namen se uporablja alarmni sistem in video nadzor. Alarmi so povezani na varnostno službo. Video nadzor ločimo na živo sliko in posnetke. Živo sliko nenehno prikazujemo pri varnostni službi. Zajeto sliko se uporabi le v primeru suma incidenta skladno z zakonodajo.

2.5. OKOLJSKA ZAŠČITA

Skladno z zakonodajo in potrebami TBP pomembne prostore ščitimo pred požari, poplavami in ostalimi naravnimi nesrečami. Uporabljamo ustrezne senzorje in alarmiranje. Podrobnejši opis varovanja ter sistemov aktivne in pasivne požarne zaščite se nahaja v Požarnem redu.
Zaradi varnosti kritične informacijske opreme ne nameščamo v prostore, kjer lahko pride do poplav, izliva vode ali požara.

2.6. DELO V VAROVANIH OBMOČJIH

Za delo v varovanih območjih veljajo posebne zahteve. Zunanji izvajalci se ne smejo sami nahajati v varovanih območjih. Njihovo delo mora biti ves čas nadzorovano. Prepovedan je vnos lastne IKT opreme. Prepovedan je vnos naprav za zajem slike in zvoka. TBP zagotavlja omarice pred vhodi v varovana območja, kjer zunanji obiskovalci lahko odložijo opremo, ki je ne smejo vnašati v varovano območje. Vsak obiskovalec mora biti seznanjen s pogoji dela v varovanih območjih in posledicami kršitve politike za delo v teh območjih.

2.7. ČISTA MIZA IN ZASLON

Pravilo prazne mize

Zaposleni ne smejo nenadzorovano puščati nosilcev podatkov z osebnimi podatki ali občutljivimi osebnimi podatki ter podatki, ki so klasificirani samo za interno rabo, na pisarniških mizah ali drugih mestih, kjer so dostopni nepooblaščenim osebam. Nosilce podatkov morajo uporabniki varno shraniti po končanem delovnem času oziroma, ko dlje časa niso fizično prisotni v prostoru. Izven delovnega časa mora biti vsa pisarniška oprema, kjer se hranijo nosilci podatkov z osebnimi podatki ali občutljivimi osebnimi podatki ter podatki, ki so klasificirani samo za interno rabo, zaklenjena ali drugače varovana. Enako velja tudi za računalniško in programsko opremo.

Pravilo praznega ekrana

Na računalniške zaslone mora biti onemogočen vpogled nepooblaščenim osebam. Vpogled lahko v posameznih primerih dovolijo zaposleni, če gre za obdelavo podatkov o uporabniku storitev, ki mora imeti vpogled v svoje osebne podatke ali poslovno skrivnost.
Ob odhodu s svojega delovnega mesta morajo zaposleni zakleniti računalnik. Računalnik mora imeti nastavljeno samodejno zaklepanje ekrana po 60 minutah neuporabe. Ob koncu delovnega časa se mora zaposleni odjaviti iz sistema.

2.8. NAMESTITEV IN ZAŠČITA OPREME

Vsa oprema je nameščena in zaščitena tako, da so kar najbolj odpravljena tveganja nepotrebnih okvar, nevarnosti iz okolja in priložnosti za nepooblaščen dostop. Pri namestitvi opreme se upoštevajo navodila proizvajalca oz. dobavitelja opreme, tehnične zahteve (temperatura, vlaga, električno napajanje …), ergonomske zakonitosti (svetloba, telesna drža …) in vpliv na druga delovna mesta.

Raven varovanja in zaščite je vedno odvisna od pomembnosti podatkov, glede na ocenjeno tveganje izgube ali poškodovanja podatkov.

V TBP se vzdržuje popis sredstev opreme računalniškega informacijskega sistema. Vsaka predaja ali sprejem opreme morata biti zabeležena. Uporabniki morajo izvajati ukrepe za preprečevanje kraje opreme. Vsa oprema ima identifikacijske oznake. Popis sredstev se preverja najmanj 1-krat letno. Za premeščanje računalniške opreme je zadolžena pooblaščena oseba, ki vodi evidenco o opremi računalniškega informacijskega sistema in beleži spremembe v računalniškem informacijskem sistemu.

2.9. ZAŠČITA OPREME IZVEN PROSTOROV TBP

Opreme, informacij ali programske opreme ni dovoljeno odnašati iz območja TBP brez predhodnega formalnega dovoljenja, ki ga izda vodstvo. Navedeno velja tudi za prenosne računalnike in ostale mobilne naprave, ki vsebujejo informacije službenega značaja.

Zahteva ne velja za kakršne koli izpise ali informacije na medijih, ki jih pripravimo za prenos na zahtevo pogodbenih partnerjev.

Vodimo evidenco pooblaščenih zaposlenih oseb za iznos opreme, informacij ali programske opreme, s katero so določeni tudi časovni roki iznosa in vračila.

Posameznih iznosov in vračil opreme ne evidentiramo, razen v posameznih primerih, ko bi se tako odločilo vodstvo.

Pri uporabi opreme na domu ali drugih lokacijah izven poslovnih prostorov TBP, morajo uporabniki upoštevati enaka varnostna pravila, kot veljajo na delovnem mestu.

Opreme in nosilcev podatkov, ki jih odnašamo iz prostorov TBP, nikoli ne puščamo brez nadzora. Prenosne računalnike prenašamo v primernih zaščitnih torbah ter jih, kjer je to mogoče, med potovanjem zakrivamo. Izven območja TBP ves čas upoštevamo proizvajalčeva navodila za zaščito.

Oprema, ki jo uporabljamo izven prostorov podjetja, je zavarovana z ustrezno zavarovalno polico.

Kadar uporabnik izgubi napravo, ki mu je bila dodeljena, mora o tem nemudoma obvestiti pristojnega vodjo in pooblaščenca za upravljanje incidentov. Če uporabnik izgubi prenosni telefon, mora poskrbeti za varnostno blokado aparata oz. številke pri ponudniku omenjenih storitev. Izgubo oz. krajo naprave izven podjetja mora potrditi policija.

2.10. ZAŠČITA MEDIJEV ZA SHRANJEVANJE

Uporabniki morajo zagotoviti ustrezno varovanje in zaščito pri upravljanju z nosilci podatkov. Le-ti morajo biti shranjeni tako, da nepooblaščena oseba nima vpogleda vanje in z njimi ne more prosto razpolagati.

Rokovanje z nosilci podatkov poteka v skladu s postopki rokovanja s podatki najvišje stopnje zaupnosti, kot so podatki na nosilcu.
V primeru izgube ali kraje izmenljivih nosilcev podatkov z zaupnimi podatki je treba to prijaviti skladno s Politiko organizacije informacijske varnosti, poglavje o upravljanju incidentov.

Preden se vsebina izmenljivega nosilca podatkov naloži na opremo, se mora vselej preveriti morebitna okuženost z virusi. Z nosilcev podatkov neznanega izvora se ne sme presnemavati datotek in ne nameščati preizkusnih programov (ali računalniških iger), če ni poznana njihova uporabnost. Za preverjanje je odgovorna informatika.

Z nosilcev podatkov, ki so predvideni za odstranjevanje in uničenje ter vsebujejo podatke z določeno stopnjo zaupnosti oz. druge občutljive podatke, se mora podatke predhodno varno uničiti. Uničenje podatkov mora biti izvedeno tako, da jih ni mogoče več obnoviti v celoti ali v najmanjšem delu. V ta namen se lahko uporabijo različni postopki:

- fizično uničenje nosilcev podatkov po postopku komisijskega uničenja,
- uporaba programske opreme za varni izbris podatkov,
- brisanje in formatiranje diskov,
- razmagnetenje nosilcev podatkov s posebno strojno opremo.

Če je potrebno in mogoče, se mora podatke pred izbrisom najprej uspešno prenesti na drug sistem oz. nosilce. Kadar uničevanje nosilcev opravlja zunanja organizacija, mora biti postopek pod nadzorom podjetja.
Zagotoviti je potrebno revizijske sledi o uničenju nosilcev.

2.11. NADZOR PODPORNIH ZMOGLJIVOSTI

Podporne zmogljivosti (napajanje, klima, gretje, prezračevanje…) morajo biti ustrezno nameščene, konfigurirane in redno vzdrževane skladno z navodili proizvajalca. V primeru oddaljenega nadzora podpornih zmogljivosti je potrebno zagotoviti ustrezno varnost (varne povezave na zahtevo, krmilni sistemi v varovanih območjih…).

Zagotoviti moramo ustrezno redundanco podpornih zmogljivosti povsod, kjer so kritični sistemi odvisni od delovanja podpornih zmogljivosti.

2.12. VARNOST OŽIČENJA

Napajalni kabli in podatkovni kabli morajo biti ustrezno ločeni (odmaknjeni, da ne prihaja do motenj. Vse trase, kjer se vodijo informacijski kabli, morajo biti zaščiteni pred poškodbami, prestrezanjem ali nedovoljenimi priklopi.
Napajalni vodi morajo biti zaščiteni pred poškodovanjem. Vsi vodi, ki vodijo v varovana območja in vodijo izven le-teh, se morajo zaščititi na način, ki onemogoča dostop (zaščita v kanalih, vodi na višini…)
Vse podatkovne vtičnice, ki niso v uporabi, morajo biti fizično ali logično odklopljene od omrežja.
Vsi podatkovni vodi morajo biti ustrezno označeni in redno preverjani, da ne pride do nepooblaščenih sprememb ožičenja.

2.13. VZDRŽEVANJE OPREME

Za vso opremo je potrebno zagotoviti vzdrževanje v skladu s priporočili proizvajalca, tako glede pogostosti kakor tudi načina vzdrževanja. Če vzdrževanja ne moremo izvesti sami, je za vzdrževanje opreme pooblaščen izključno dobavitelj opreme.
Vsa vzdrževalna dela se morajo opravljati znotraj TBP. Če to ni mogoče, se mora nosilce podatkov iz opreme odstraniti in jih varno shraniti. Če podatkov ni mogoče odstraniti ali kako drugače zaščititi, mora biti postopek vzdrževanja nadzorovan. Po vzdrževalnih delih mora biti oprema, preden se jo vključi v obratovanje, varnostno pregledana.

2.14. VARNO UNIČENJE ALI PONOVNA UPORABA OPREME

Opremo, predvideno za uničenje ali za ponovno uporabo je potrebno preveriti, ali vsebuje občutljive informacije in licenčno programsko opremo. V tem primeru izvedemo postopke za varno fizično uničenje ali pa z uporabo tehnik, ki preprečujejo obnovitev izvirnih informacij, uničimo informacije, ki jih ta oprema vsebuje.

Vedno uporabljamo nove nosilce podatkov; ponovna uporaba starih nosilcev podatkov je prepovedana, razen po predhodnem strokovnem uničenju podatkov z ničelnim prepisom in formatiranjem.

Poškodovane nosilce podatkov, ki vsebujejo občutljive podatke, vedno fizično uničimo, prepovedano jih je pošiljati v popravilo ali zavreči. Izjema je, če nosilec vsebuje pomembne informacije, katerih kopije ne obstajajo, in je obnovitev v korist TBP. V takem primeru se nosilec podatkov pošlje v za to pooblaščen laboratorij za obnovo podatkov, kjer le-te varno obnovijo in pošljejo nazaj v TBP.

Lenart, 13.12.2023

Uprava TBP d.d.
Direktor družbe

Danilo ROJKO