Varovanje informacij

Skupina HSE dem
dravske elektrarne maribor

PRAZNA STRAN


!
Varovanje informacij
Navodila o varovanju podatkov in informacij
Priročnik za zaposlene in poslovne partnerje družbe Dravske elektrarne Maribor

Vsebina

Varovanje informacij
avtorja Samo Fekonja, Nina Jeznik
izdajatelj: Dravske elektrarne Maribor
zanj: mag. Viljem Pozeb, direktor
avgust 2011

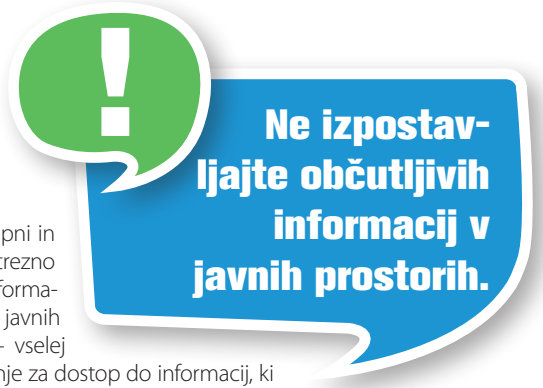
Idejna zasnova, oblikovanje
in ilustracije: Studio 8
tisk: Tiskarna Petrič
naklada: 1000 izvodov

Dravske elektrarne Maribor, d. o. o.
Obrežna ulica 170
2000 Maribor, Slovenija
www.dem.si


V VARNOSTNIH NAVODILIH JASNO PIŠE, NAJ PREPREČIMO, DA BI NAM NEPOOBLAŠČENE OSEBE SKOZI OKNO VIDELE NA ZASLON!
?

01. KAKO KLASIFICIRAMO INFORMACIJE IN KAKO UPRAVLJAMO Z ZAUPNIMI DOKUMENTI?

POGLAVJE KLASIFICIRANJE INFORMACIJ IN UPRAVLJANJE Z ZAUPNIMI DOKUMENTI OPISUJE, KAKO RAVNATI Z DOKUMENTI, KI VSEBUJEJO POSLOVNO OBČUTLJIVE INFORMACIJE.



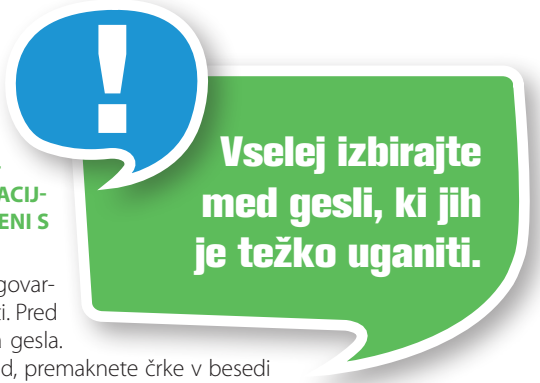
Dokumenti se označujejo kot tajni, zaupni, interno zaupni in javni. Dokumenti morajo imeti občutljive informacije ustrezno označene. Ne izpostavljajte tajnih, zaupnih ali internih informacij na letalih, restavracijah, dvigalih, čakalnicah in ostalih javnih prostorih. Bodite previdni pri telefonskih pogovorih – vselej vnaprej preverite, ali imajo vse vpletene osebe dovoljenje za dostop do informacij, ki jih boste omenjali. Pred izpolnjevanjem vprašalnikov in pred intervjuji pri lastniku informacij preverite, ali jih je dovoljeno razkriti. Računalnik vselej opremite z ohranjevalnikom zaslona, ki je zaščiten z geslom. Ob daljših prekinitvah dela z računalnikom se iz sistema odjavite. Računalniški zaslon obrnite tako, da nepooblaščene osebe ne vidijo na ekran skozi okno.

Več informacij:
ODOS, modul Sistem vodenja – SN 35-01


ODKAR SEM SI V SKLADU Z VARNOSTNIMI NAVODILI IZBRAL GESLO, KI GA JE TEŽKO UGANITI, PRIHAJAM V SLUŽBO DVE URI PREJ. TOLIKO ČASA NAMREČ POTREBUJEM, DA GA VTIPKAM V RAČUNALNIK...
Vpišite geslo
****
****
****
****
****
******

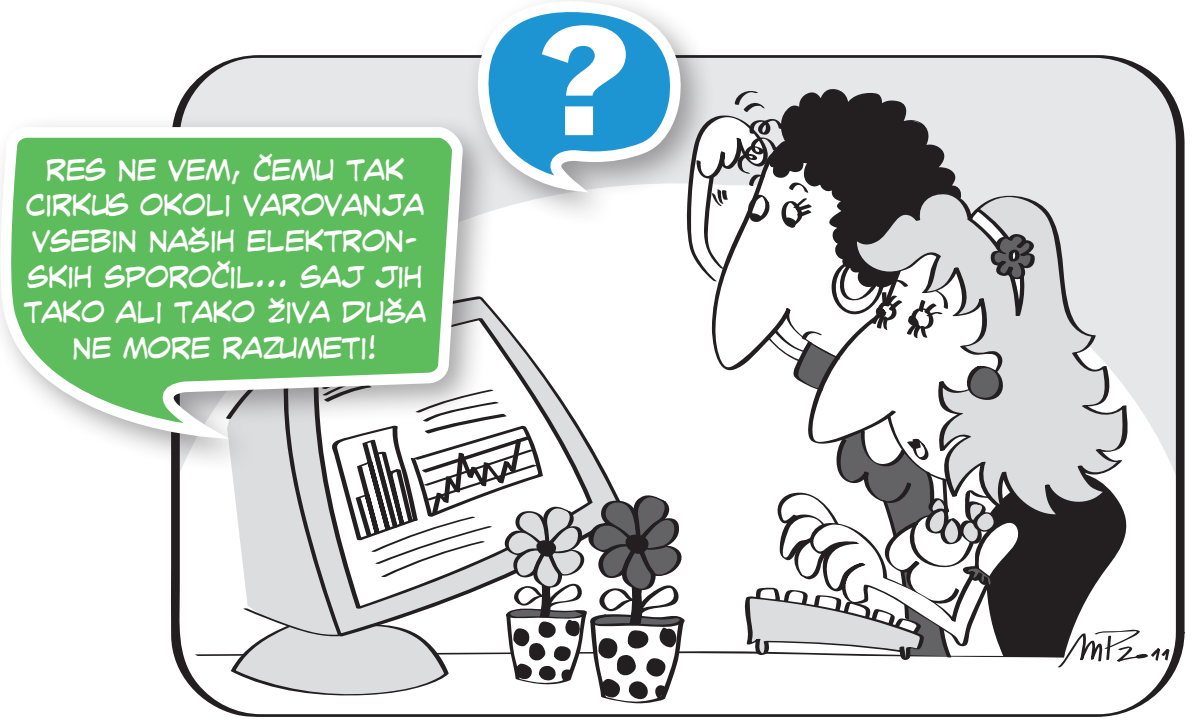
02. KAKO UPRAVLJAMO Z UPORABNIŠKIMI IMENI IN GESLI?

Z UPRAVLJANJEM UPORABNIŠKIH RAČUNOV TER DODELJEVANJEM IN NADZOROM DOSTOPOV DO INFORMACIJSKIH SISTEMOV ZAGOTAVLJAMO NADZOROVAN DOSTOP DO INFORMACIJSKIH VIROV. TAKO SKRBIMO, DA SO VSI UPORABNIKI SEZNANJENI S PRAVILNIMI IN VARNIMI NAČINI DOSTOPANJA DO SISTEMOV.



Za uporabo svojega uporabniškega imena in gesla odgovarjate sami. Vselej izbirajte med gesli, ki jih je težko uganiti. Pred izbiro gesla se seznanite s postopki za izbiro dobrega gesla. Dobro geslo lahko ustvarite tako, da združite več besed, premaknete črke v besedi za določeno število znakov navzgor ali navzdol po abecedi, premaknete besedo navzgor, navzdol, levo ali desno po tipkovnici, transformirate navadno besedo z določeno metodo (primer: vsako drugo črko v besedi zamenjate z zaporedno številko črke v abecedi), izdelate akronime iz besedil pesmi, popevk ali drugih znanih besedil, namenoma napačno zapišete besedo, kombinirate različne pojme (primer: vaša najljubša barva in številka) ali izpeljete kombinacije zgoraj naštetih postopkov. Najbolje je, da si geslo zapomnite. Če posumite, da je bilo vaše geslo razrkito, ga morate spremeniti.

Več informacij:
ODOS, modul Sistem vodenja – SP 26


RES NE VEM, ČEMU TAK CIRKUS OKOLI VAROVANJA VSEBIN NAŠIH ELEKTRONSKIH SPOROČIL... SAJ JIH TAKO ALI TAKO ŽIVA DUŠA NE MORE RAZUMETI!
?

03. KAKO VARNO UPORABLJAMO ELEKTRONSKO POŠTO?

VARNA UPORABA ELEKTRONSKE POŠTE UPORABNIKA ŠČITI PRED VIRUSI TER GA OPOZARJA NA ŠTEVILNE GROŽNJE, KI SO PRISOTNE PRI NJENI UPORABI. UPORABNIK MORA BITI POUČEN, KAKO IN KDAJ UPORABLJATI ELEKTONSKO POŠTO TER KAKO PRAVILNO POŠILJATI PRIPONKE.

Sistemi za pošiljanje elektronske pošte ne veljajo za varne za komuniciranje z občutljivimi in zaupnimi informacijami. Vaše elektronsko sporočilo je lahko med pošiljanjem prestreženo, dostavljeno napačnemu prejemniku, dostavljeno z zamudo ali celo sploh ne. Vsebina sporočila naj bo primerna in zapisana v skladu s pravili dobrega poslovnega komuniciranja. Ne uporabljajte neprimernih ali žaljivih besed, ne uporabljajte žargona, izogibajte se besednih zvez, ki namigujejo na raso, religijo, nacionalnost, državljanstvo, spol, sposobnosti, spolno usmerjenost ... Sporočila, ki jih prejmete nepričakovano in od nepoznanih pošiljateljev, smatrajte kot sumljiva in jih ne odpirajte. Pri shranjevanju elektronskih sporočil upoštevajte načelo racionalnosti. Izogibajte se shranjevanju dokumentov, ki zavzamejo veliko prostora (filmi, slike, glasba). Pri pošiljanju ali sprejemanju elektronske pošte je velikost sporočila skupaj s priponko omejena. Dostop do elektronske pošte izven delovnega časa: http://owa.dem.si.

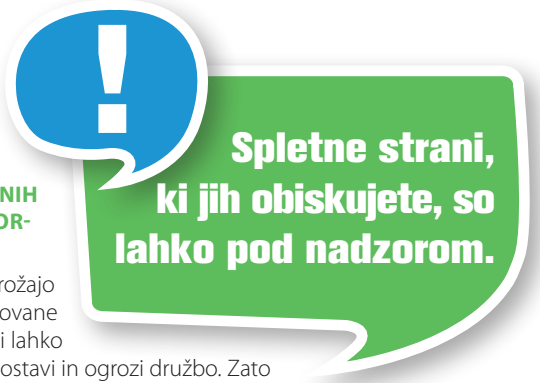
Ne odpirajte sporočil, ki jih prejmete nepričakovano in od nepoznanih pošiljateljev.

Več informacij:
ODOS, modul Sistem vodenja – SP 26


NE VEM ZAKAJ, A VČASIH IMAM ČUDEN OBČUTEK, DA ME NEKDO OPAZUJE ...
?
WWW

04. KAKO VARNO UPORABLJATI INTERNET?

VAROVANJE DRUŽBE IN UPORABNIKOV PRED GROŽNJAMI Z INTERNETA ZAJEMA KONTROLE ZA VARNO PREGLEDOVANJE DOVOLJENIH SPLETNIH STRANI, NADZOR OBISKA SPLETNIH STRANI TER OSVEŠČANJE UPORABNIKOV O VAROVANJU INFORMACIJ.



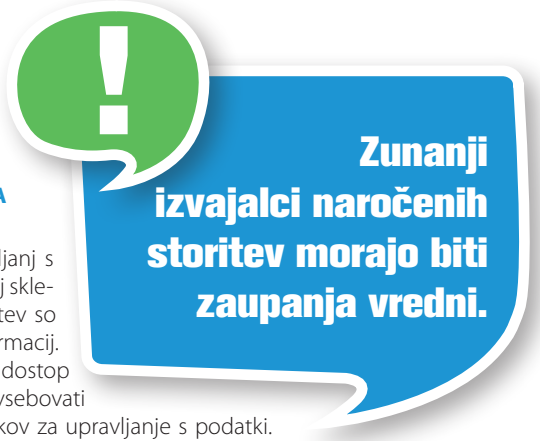
Zavedajte se, da prinaša internet veliko pasti, ki ogrožajo varovanje informacij. Vedeti morate, da so lahko obiskovane spletne strani pod nadzorom. Lastniki spletnih strani si lahko zabeležijo, od kod dostopate, kar posledično lahko izpostavi in ogrozi družbo. Zato ne brskajte po piratskih, hekerskih, seksualno in rasistično obarvanih straneh. Ne pridobivajte, hranite ali širite podatkov, ki lahko negativno vplivajo na ugled družbe. Ne podajajte svojih mnenj v imenu družbe in ne objavljajte ali izdajajte gradiv, ki so v lasti družbe. Uporaba interneta v privatne namene je dovoljena, a le v primeru, ko s tem ne motite poslovnih procesov in sodelavcev.

Več informacij:
ODOS, modul Sistem vodenja – SP 26


... DAVČNA ŠTEVILKA, MATIČNA ŠTEVILKA, SLUŽBENI NASLOV, DOMAČI NASLOV, PRETEKLI IN SEDANJI POSLOVNI PARTNERJI, ŽENINO IME, MATERINO IME, BABIČINO IME, PAPAGAJEVO IME, ŠTEVILKA NOGE - ODKLJUKANO! MISLIM, DA MI MANJKA SAMO ŠE VAŠ RENTGENSKI POSNETEK, PA SVA KONČALA S PREVERJANJEM!
?
POTENCIALNI POSLOVNI PARTNER: PODATKI, KI JIH JE POTREBNO PREVERITI
MPZ-11

05. KAKO VARNO NAROČITI STORITEV PRI ZUNANJIH IZVAJALCIH?

NAVODILA O VAROVANJU INFORMACIJ PREDSTAVLJAJO OKVIR ZA UREJANJE NAROČANJA STORITEV PRI ZUNANJIH IZVAJALCIH IN NUDIJO PODPORO PROCESOM DODELJEVANJA STORITEV V IZVAJANJE ZUNANJIM IZVAJALCEM.



Vsak zunanji izvajalec mora upoštevati pravila upravljanj s podatki podjetja. Družba z zunanjim izvajalcem najprej sklene pogodbo. V pogodbo o zunanjem izvajanju storitev so vključene določbe, ki se nanašajo na varovanje informacij. Ko je pogodba sklenjena, se izvajalcu dodeli varen dostop do virov. Vsaka pogodba z zunanjim izvajalcem mora vsebovati dogovor glede tveganj, varnostnih zahtev in postopkov za upravljanje s podatki. Dostop do informacijskega sistema s strani zunanjih izvajalcev mora biti nadzorovan. Posrednik pri pošiljanju programske opreme mora biti zaupanja vreden. Pošiljke morajo biti dostavljene s priporočeno pošto ali s kurirsko službo.

Več informacij:
ODOS, modul Sistem vodenja – SP 22


NE, NI ZLONAMERNA OPREMA. SAMO JEZEN JE, KER MU ZARADI VARČEVANJA NISMO DOKUPILI SPOMINA ...
?
TEHNIČNA PODPORA DEM
ANTI VIRUS ŠČITNIK

06. KAKO SE ZAŠČITITI PRED ZLONAMERNO PROGRAMSKO OPREMO?

VARNO IN USPEŠNO POSLOVANJE JE KLJUČNEGA POMENA ZA DRUŽBO. ZAŠČITA PRED ZLONAMERNO PROGRAMSKO OPREMO PREPREČUJE NENAČRTOVANE PREKINITVE PROCESOV, RAZKRITJA INFORMACIJ, NEPOOBLAŠČENA DOSTOPANJA DO PODATKOV TER ODPRAVLJA NEVŠEČNOSTI, KI JIH LAHKO POVZROČI ZLONAMERNA PROGRAMSKA OPREMA.

Ne zaganjajte programov in datotek, za katere niste prepričani, čemu služijo. Prenosne nosilce podatkov pred vsako uporabo preverite s protivirusnim programom. Če sumite ali ugotovite, da sistem za protivirusno zaščito ne deluje ali ni ustrezno posodobljen, takoj obvestite skrbnika. Zabeležite si simptome in sporočila, ki se pojavijo na zaslonu. Ne poskušajte sami in brez dovoljenja skrbnika odpraviti napak na programski opremi. Osebje, ki je zadolženo za odkrivanje in odstranjevanje zlonamerne programske opreme, se redno usposablja, zato odpravljanje napak prepustite njim.

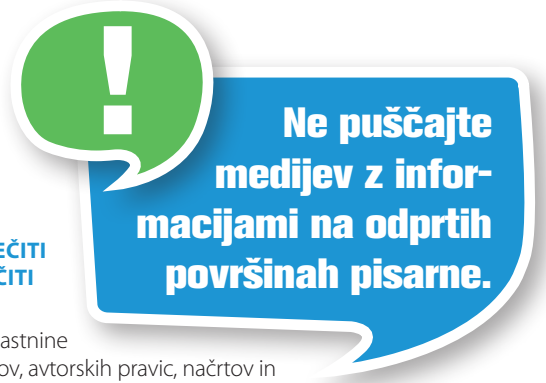
Ne poskušajte sami odpraviti napak na programski opremi.

Več informacij:
ODOS, modul Sistem vodenja – SP 26


NE, NE, TO NI NERED, TO JE VARNOSTNI UKREP! TAKO LAHKO VSELEJ BREZ SKRBI ZAPUSTIM SVOJE DELOVNO MESTO, SAJ ZALUPNIH PODATKOV TAKO ALI TAKO NIHČE NE BO MOGEL NAJTI!

07. VAROVANJE V ZVEZI Z OSEBJEM

CILJI VAROVANJA V ZVEZI Z OSEBJEM SO ZMANJŠATI TVEGANJA, KI NASTAJAJO ZARADI ČLOVEŠKIH NAPAK, KRAJE, PONEVERBE ALI ZLORABE SREDSTEV, PREPREČITI NEPOOBLAŠČENE FIZIČNE DOSTOPE, POŠKODOVANJA INFORMACIJ IN MOTENJE V POSLOVNIH PROSTORIH, PREPREČITI IZGUBE, POŠKODOVANJA IN ZLORABE OPREME TER PREPREČITI PREKINITVE POSLOVNIH DEJAVNOSTI.



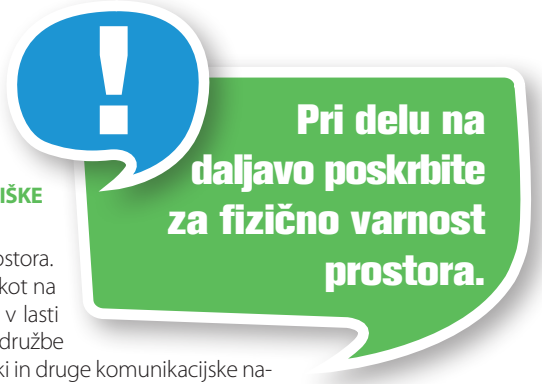
Seznanite se z veljavnimi predpisi glede intelektualne lastnine družbe in podpišite izjavo o varovanju osebnih podatkov, avtorskih pravic, načrtov in patentov. Redno usposabljanje na področju varovanja informacij zmanjšuje možnost človeške napake. Obnašajte se odgovorno in vselej poskrbite, da medijev z zaupnimi podatki (papirnati, elektronski mediji) ne puščate na odprtih površinah pisarne. V primeru oddaljitve od računalnika vselej aktivirajte ohranjevalnik zaslona, ki ste ga zaščitili z geslom. Zaposlenim v družbi vstop na območje družbe omogoča prepustnica. Izgubo ali krajo prepustnice takoj prijavite. Obiskovalci in druge osebe morajo biti znotraj družbe vselej v spremstvu oziroma pod nadzorom.

Več informacij:
ODOS, modul Sistem vodenja – SP 27


ODKAR SMO UVEDLI STROGO VAROVANJE INFORMACIJ TUDI PRI DELU NA DALJAVO, NA SLUŽBENIH POTOVANJIH NISEM NIKOLI OSAMLJENA!
?
RECEP
SECURI
SECURI

08. VARNOST PRENOSNE KOMUNIKACIJSKE IN RAČUNALNIŠKE OPREME IN DELA NA DALJAVO

VARNOSTNE ZAHTEVE GLEDE PRENOSNE KOMUNIKACIJSKE IN RAČUNALNIŠKE OPREME TER DELA NA DALJAVO DOLOČAJO POSTOPKE ZA IDENTIFIKACIJO, PREDAJO IN ODOBRITEV RAČUNALNIŠKE IN KOMUNIKACIJSKE OPREME ZA PODPORO DELA NA DALJAVO.



Pri delu na daljavo vselej zagotovite fizično varnost prostora. Ne glede na to kje se nahajate, informacije varujte tako kot na delovnem mestu. Ne posojajte nobenih sredstev, ki so v lasti družbe. Na službeni poti pazite, da zaupnih informacij družbe ne prenašate v tuje države. Prenosni računalniki, dlančniki in druge komunikacijske naprave, ki vsebujejo občutljive informacije družbe, se obravnavajo kot osebna prtljaga, zato jih imejte vselej pri sebi. Komunikacijskih naprav in občutljivih dokumentov ne puščajte v nenadzorovanem vozilu, hotelski sobi ali pisarni. Ne berite ali izpostavljajte občutljivih informacij na javnih mestih, kjer jih lahko prestrežejo nepooblaščene osebe. Dokumente ali komunikacijske naprave s tajnimi ali zaupnimi informacijami družbe vselej hranite v sefih ali težkih omarah s ključavnico. Komunikacijske naprave, ki omogočajo oddaljen dostop so VPN povezava in brezžična ali druga povezava. Ko zaključite z oddaljenim dostopom do računalnikov družbe, se odjavite in prekinite povezavo. Družba preko oddaljenega nadzora nadzira delovne postaje, prenosnike in mobilne telefone.

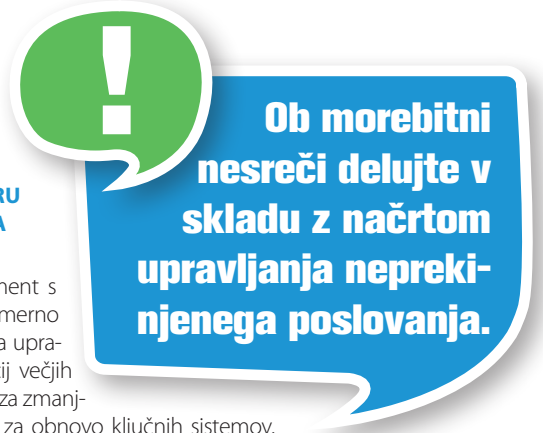
Več informacij:
ODOS, modul Sistem vodenja – SP 26


POKLICALI STE TIM ZA ZAGOTAVLJANJE NEPREKINJENEGA DELOVANJA. PROSIMO, POČAKAJTE TRENUTEK...
?
NAČRT UPRAVLJANJA NEPREKINJENEGA POSLOVANJA
1. V PRIMERU OGROŽENOSTI NEMUDOMA POKLIČITE NAŠ STROKOVNI TIM.
00:01
MPZ-11

09. UPRAVLJANJE NEPREKINJENEGA POSLOVANJA

NAČRT UPRAVLJANJA NEPREKINJENEGA POSLOVANJA PREDSTAVLJA AKTIVNOSTI ZA HITRO IN UČINKOVITO OKREVANJE KRITIČNIH POSLOVNIH FUNKCIJ IN OPERACIJ V PRIMERU INCIDENTA ALI FIZIČNE NESREČE, KI BI SE LAHKO ZGODILA NA KATEREM KOLI DELU POSLOVNEGA PROCESA.

Načrt upravljanja neprekinjenega poslovanja je dokument s seznamom vseh storitev in postopkov, ki morajo biti primerno obravnavani in izvedeni ob morebitni nesreči. Cilj načrta upravljanja neprekinjenega poslovanja je določitev področij večjih tveganj in izpostavljenosti nesrečam, določitev ukrepov za zmanjšanje teh tveganj ter omogočanje izvedbe postopkov za obnovo ključnih sistemov. Načrt upravljanja neprekinjenega poslovanja ščiti vse pomembne in časovno kritične aktivnosti ter omogoča družbi, da v primeru nesreče v najkrajšem možnem času nadaljuje delo v skladu z vnaprej določenimi pogoji poslovanja. Z načrtom upravljanja neprekinjenega poslovanja morajo biti seznanjeni vsi lastniki procesov in ostali zaposleni. Upravljanje načrta neprekinjenega poslovanja in njegovih sprememb mora biti odgovorno in ažurno, saj le tako zagotovimo njegovo redno in ustrezno posodabljanje.

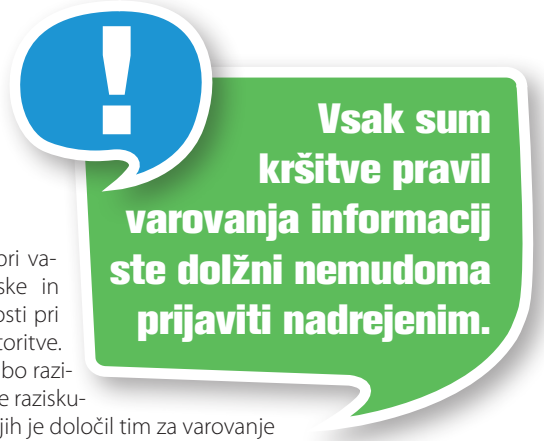


Več informacij:
ODOS, modul Sistem vodenja – SP 36


PREJELI SMO PRIJAVO SUMA KRŠITVE INFORMACIJSKE VARNOSTI. PREDAJAM VAS KOLEGU, KI BO RAZISKAL ZADEVO...
?

10. KRŠITVE VARNOSTNIH NAVODIL

ZAPOSLENI V DRUŽBI IN NJENI POSLOVNI PARTNERJI SO DOLŽNI PRIJAVITI VSAKRŠEN SUM KRŠITVE INFORMACIJSKE VARNOSTI SVOJIM NADREJENIM, TA PA NAPREJ SKRBNIKU INFORMACIJSKE STORITVE ALI VARNOSTNEMU INŽENIRJU.



Sumi kršitev ali kršitve so lahko: varnostni incidenti pri varovanju informacij, nepravilno delovanje programske in strojne opreme, pomanjkljivosti ali sumi pomanjkljivosti pri varovanju informacij ter vse, kar ogroža sisteme ali storitve. Vsako obvestilo o sumu kršitve informacijske varnosti bo raziskano in obravnavano posamično. Varnostne incidente raziskuje oseba ali skupina oseb, ki so zaposlene v družbi ter jih je določil tim za varovanje informacij. V času preiskave lahko pristojni preiskovalec uporabniku ali zunanjemu izvajalcu odvzame dodeljene pristopne pravice in pristojnosti oziroma pooblastila. Pogodbene stranke, ki ne sprejmejo pravil informacijske varnosti ali jih kršijo, izgubijo pravico sodelovanja z družbo.

Več informacij:
ODOS, modul Sistem vodenja – SP 36

11. POJMI

SUVI: sistem za upravljanje varovanja informacij (angl: ISMS – Information Security Management System)

Skrbnik storitve ali informacijskega sredstva: oseba, ki skrbi, da je sredstvo vzdrževano in deluje po vseh normativih.

Varnostni incident: dogodek, ki ogroža ali bi lahko ogrozil varnost podatkov v podjetju.

Informacijski sistem (IS): urejen in organiziran sistem, ki uporabnike oskrbuje z vsemi potrebnimi informacijami za odločanje.

Informacijsko sredstvo (INFS): vse, kar ima določeno vrednost za organizacijo.

Uporabnik storitve ali informacijskega sredstva: oseba, ki uporablja sredstvo in s svojim delom ne zmanjšuje njegove uporabne vrednosti.

Tim za varovanje informacij: ekipa strokovnjakov, ki skrbijo za koordinacijo varovanja informacij v podjetju.

Varnostni inženir: pooblaščenec tima za varovanje informacij.

Lastnik storitve ali informacijskega sredstva: oseba, ki ji je vodstvo dodelilo odgovornost za nadzorovanje proizvodnje, razvoja, vzdrževanja, uporabe in varovanja sredstev.

PRAZNA STRAN