



INFORMACIJSKA VARNOST

Verzija 2019

	VARNOSTNA POLITIKA	
	FORUM VAROVANJA INFORMACIJ	
	Oznaka: VP Forum	Datum izdaje: 02.12.2019
	Verzija: 1	Stran: 1/2

Klasifikacija: **INTERNO**

V skladu s 9. členom statuta o ustanovitvi družbe Mariborski vodovod d.d. z dne 29.6.2010, izdajam naslednjo

ODLOČBO
o imenovanju članov
v FORUM VAROVANJA INFORMACIJ

1) Za izvedbo Forum-a varovanja informacij se imenuje naslednje člane z vlogo oz. zadolžitvami:

➤ **Danilo Burnač – direktor, stalni član**

Svojo zavezanost vzpostavitvi, vpeljevanju, delovanju, spremljanju, pregledovanju, vzdrževanju in izboljševanju SUVI dokazuje tako, da:

- oblikuje SUVI,
- zagotovi, da so cilji in načrti za varovanje informacij določeni,
- določi vloge in odgovornosti pri varovanju informacij,
- obvešča organizacijo o pomenu SUVI,
- zagotavlja ustrezna sredstva za delovanje SUVI,
- skrbi za nadzor skozi notranje presoje in vodstvene preglede.

➤ **Vodje sektorjev – stalni člani:**

- Bojan Erker, vodja sektorja informatike
- Maja Lukič, vodja pravno kadrovskega sektorja
- Sergej Danč, vodja gospodarsko računovodskega sektorja
- Milka Pungartnik, vodja sektorja nabave
- Peter Levstek, vodja tehnično razvojno operativnega sektorja
- Boštjan Erjavec, vodja sektorja črpanja

Naloge foruma varovanja informacij so naslednje:

- skrb za organizacijo, uvajanje in izvajanje sistema upravljanja varovanja informacij
- organiziranje programa varnostnega osveščanja za vse zaposlene v podjetju
- vzpostavljanje procesa integracije informacijske varnosti
- vzpostavitev sistemskih navodil in postopkov,
- nadzor in pregled sistema upravljanja varovanja informacij,
- izvedba kontrol,
- vzdrževanje in izboljševanje sistema upravljanja varovanja informacij,
- upravljanje sistema upravljanja informacijskih tveganj.
- organizacija in oblikovanje poslovnika informacijske varnosti in varnostnih politik
- vzpostavitev dokumentacije SUVI,
- skrb za ažurnost in objavo dokumentacije
- odgovornost za sklic rednih srečanj foruma,
- sklic izrednih srečanj foruma na predlog posameznih članov ali direktorja družbe
- zastopanje poslovnih interesov podjetja pri vzpostavi varnostnih politik, standardov in postopkov
- skrb za skladnost z zakonodajo in ostalimi internimi pravilniki
- skrbi za sledljivost srečanj foruma- zapisniki



	VARNOSTNA POLITIKA	
	FORUM VAROVANJA INFORMACIJ	
	Oznaka: VP Forum	Datum izdaje: 01.06.2014
	Verzija: 1	Stran: 2/2

Klasifikacija: **ZAUPNO**

➤ **Nestalni člani – forum po potrebi dopolnjujejo nestalni člani za posamezna področja**

- svetovanje pri dopolnitvah sistema SUVI s specifičnimi področji (npr. SCADA, GIS, e-hramba, mobilne storitve,...), z uvajanjem sprememb v okolju, novimi tehnologijami in vsemi povezanimi tveganji
 - svetovanje, izobraževanje in preverjanje zaposlenim pri upravljanju sistema SUVI,
 - pomoč pri vzpostavitvi, upravljanju in organizaciji sistema SUVI,
 - pomoč pri uvajanju dobrih praks pri upravljanju sistema SUVI,
 - ostalo
- 2) Organiziranost informacijske varnosti in pripadajoče zadolžitve opredeljuje poslovnik informacijske varnosti v točki 6. Vloge in odgovornosti te odločbe so skladne z 6. točko poslovnika informacijske varnosti.
- 3) Odločba velja z dnem izdaje.

Pripravil: Bojan Erker

Vodja sektorja informatike



Odobril: Danilo Burnač, mag.ekon. in posl.ved

direktor



	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 1/13
	Datum zadnje revizije: 02.12.2019	

Klasifikacija: INTERNO

POSLOVNIK INFORMACIJSKE VARNOSTI MARIBORSKI VODOVOD D.D.

(KROVNI DOKUMENT INFORMACIJSKE VARNOSTI, VP-01-01)

Vizija, poslanstvo, vrednote, strategija

Vizija

Zagotavljati najkvalitetnejšo pitno vodo v Sloveniji

Poslanstvo

Varna oskrba s pitno vodo vseh uporabnikov

Vrednote

Poštenost, družbena in okoljska odgovornost, skladnost in neoporečnost, strokovnost in etične kvalitete

Strategija

Varna vodooskrba, trajnostni razvoj, ekonomska učinkovitost, zadovoljstvo uporabnikov

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 2/13
	Datum zadnje revizije: 02.12.2019	

Spremna beseda direktorja

V Mariborskem vodovodu se zavedamo, da so informacije in informacijsko tehnološki (IT) sistemi pomembna podpora poslovanju podjetja in glede na naravo našega dela tudi pomembna podpora poslovnih procesov naših poslovnih partnerjev. Podatke in informacije smatramo kot najpomembnejšo poslovno dobrino, ki ima neposreden vpliv na poslovni uspeh podjetja, na njegovo vrednost in njegovo podobo v javnosti.

Zavedamo se, da so informacije, programska in strojna oprema ter IT sistemi predmet potencialnih in realnih groženj, kriminala, sabotaž ter drugih odpovedi in nesreč. Prav tako vemo, da so varnostni ukrepi učinkovitejši in cenejši, če so vgrajeni neposredno v sisteme in IT storitve in če so osnovne varnostne zahteve sestavni deli naših projektov. Posebno pozornost posvečamo varovanju osebnih podatkov in konceptu vgrajene zasebnosti.

V ta namen smo pripravili ta Poslovnik informacijske varnosti, ter upošteva potrebe našega podjetja po varovanju informacij, vzpostavili sistem vodenja varovanja informacij, ki je v pogledu praktične implementacije ukrepov usklajen z zahtevami referenčnega standarda in dobre prakse - ISO/IEC 27001:2005.

Poslovnik informacijske varnosti, kot osnovni dokument vzpostavljenega sistema vodenja varovanja informacij, se skupaj s pripadajočimi referenčnimi dokumenti ustrezno vključuje v celotno piramido dokumentov sistema informacijske varnosti podjetja. Poslovnik opisuje podrobnosti vzpostavljenega sistema vodenja varovanja informacij v našem podjetju, vključno z navedbo Politike varovanja informacij, ciljev varovanja in izbranih kontrol ter opisom implementiranih ukrepov varovanja.

Vsi delavci Mariborskega vodovoda smo odgovorni za varovanje informacij, dolžni smo spoštovati določila Poslovnika informacijske varnosti ter odgovorni za izvajanje ukrepov v sistemu vodenja varovanja informacij.

Vodstvo podjetja bo s pregledovanjem sistema vodenja varovanja informacij, z izvajanjem rednih notranjih pregledov in zunanjih presoj zagotavljalo njegovo učinkovito izvajanje.

Danilo Burnač, mag. ekon. in posl. ved

direktor

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 3/13
	Datum zadnje revizije: 02.12.2019	

VSEBINA:

1. NAMEN	4
2. CILJI	4
3. PODROČJE IN VELJAVA.....	4
4. OBSEG	5
5. IZJAVA O VAROVANJU IN ZAŠČITI INFORMACIJ	6
6. ORGANIZIRANOST INFORMACIJSKE VARNOSTI IN PRIPADAJOČE ZADOLŽITVE .	7
7. STRUKTURA IN ORGANIZIRANOST DOKUMENTOV VARNOSTNE POLITIKE	10
8. PODROČJA INFORMACIJSKE VARNOSTNE POLITIKE	11
9. KRŠITVE	13
10. SEZNANJANJE UPORABNIKOV.....	13
11. UPRAVLJANJE S SPREMEMBAMI V DOKUMENTACIJI	13

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 4/13
	Datum zadnje revizije: 02.12.2019	

1. NAMEN

Namen poslovnika informacijske varnosti je zagotavljanje nemotenega poslovanja in omejitve poslovne škode na najmanjšo možno mero s preprečevanjem in zmanjševanjem učinkov varnostnih incidentov. Informacijski sistem Mariborskega vodovoda je neprecenljive vrednosti za podjetje, za njegovo poslovanje pa so zaupnost, neoporečnost in razpoložljivost informacij kritične pri doseganju konkurenčne prednosti, uspešnosti in ugleda podjetja v javnosti.

2. CILJI

Cilj varovanja informacij je omogočiti izpolnitev našega poslanstva in doseganje zastavljenih ciljev z vzpostavitvijo sistema za upravljanje informacijske varnosti v Mariborskem vodovodu, z namenom zagotoviti:

- **razpoložljivost:** informacija ali storitev je na voljo vedno, kadar je potrebna,
- **celovitost:** informacija je istovetna izvorni obliki in v procesu obdelave, prenosa ali hranjenja ni bila spremenjena,
- **zaupnost:** dostop do informacij imajo samo tisti, katerim je namenjena.

Ustvarjen mora biti ustrezen nivo varnostne zavesti in kulture varovanja informacij vseh zaposlenih. Vsi zaposleni se morajo zavedati in ravnati v skladu z ustrežno zakonodajo, standardi, politikami in notranjimi pravili s področja varovanja informacij.

3. PODROČJE IN VELJAVA

Poslovník informacijske varnosti velja na celotnem področju informacijske varnosti v podjetju. Nanaša na vse informacijske dobrine, ki so v trajni ali začasni lasti in pod upravljanjem Mariborskega vodovoda d.d., ne glede na to ali se nahajajo v prostorih podjetja ali pa izven njih.

Dokument je namenjen in velja za vse zaposlene ne glede na obliko zaposlitve (začasni, študenti, pogodbeniki,...), dobavitelje (zunanji sodelavci, dobavitelji storitev, serviserji,...), ki se pri svojem delu srečujejo s informacijskimi dobrinami Mariborskega vodovoda, ne glede na kateri lokaciji delo opravljajo.

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 5/13
	Datum zadnje revizije: 02.12.2019	

4. OBSEG

- **Informacijske dobrine** predstavljajo:
 - informacijska sredstva: baze podatkov in datoteke, dokumentacija sistema, uporabniški priročniki, gradivo za usposabljanje, načrti za neprekinjeno delovanje in drugo,
 - sredstva programske opreme: uporabniške rešitve, temeljna programska oprema, razvojna orodja in podporni programi,
 - fizična sredstva: računalniška in komunikacijska oprema, magnetni nosilci podatkov, listine ter druga tehnična oprema (ključi, štipaljke, ...),
 - ostala nematerialna sredstva: gesla, osebne podatke, zaupne informacije, do katerih imamo dostop med nam zaupanim opravljanjem poslovnih procesov in podobno,
 - storitve: storitve računalniškega obdelovanja, tehnične in komunikacijske storitve.
- **Uporabniki** informacijskih dobrin:
 - zaposleni v podjetju ne glede na obliko zaposlitve (redno, začasno, pogodbeno, študentje in dijaki),
 - predstavniki drugih poslovnih subjektov - dobavitelji (podizvajalci, pogodbeni izvajalci, svetovalci),
 - predstavniki nadzornih institucij (revizorji, nadzorni organi, inšpektorji..).
- **Lastnik**: posameznik ali organizacijska enota (OE), ki nosi odgovornost za določen informacijsko dobrino in vzdrževanje varnostnih ukrepov v zvezi z njim.
- **Varnostna arhitektura**:
 - varnostni incident: vsak dogodek, ki ima, ali bi lahko imel za posledico zlorabo informacijske dobrine, ali dejanje, ki krši varnostne postopke v podjetju,
 - varnostne kontrole: politike, standardi, ukrepi, mere, predpisi, postopki, programska ali strojna oprema, ki zmanjšuje ali odpravlja posledice na informacijski dobrini, če se grožnja uresniči,
 - varnostna infrastruktura in organizacija z določitvijo vlog in odgovornosti osebja,
 - identifikacija in upravljanje tveganj,
 - varnostno osveščanje in usposabljanje,
 - skladnost, ki vključuje nadzor, revizijske preglede, raziskave.

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 6/13
	Datum zadnje revizije: 02.12.2019	

5. ZAVEZANOST K VAROVANJU IN ZAŠČITI INFORMACIJ

Informacijsko varnostna politika izhaja:

1. iz potreb podjetja Mariborski vodovod d.d.,
2. iz zakonodaje, ki velja v Republiki Sloveniji za podjetja: Zakon o varstvu osebnih podatkov (ZVOP), Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP: dokazna vrednost elektronske oblike), Zakon o varstvu dokumentarnega gradiva ter arhivih (ZVDAGA: notranja pravila) Zakon o tajnih podatkih (ZTP: klasifikacija tajnih podatkov), Kazenski zakonik (KZ-1: Napad na informacijski sistem), Zakon o kazenskem postopku (ZKPJ: komunikacijska zasebnost), in ostala.
3. mednarodnega standarda ISO/IEC 27001:2005, ISO/IEC27002)

in deluje v skladu z vso veljavno zakonodajo Republike Slovenije, s statutom ter sklepi podjetja.

Mariborski vodovod bo uporabil ustrezne ukrepe, da zagotovi razpoložljivost in neoporečnost podatkov in informacij, ki so vitalne za poslovanje podjetja.

Mariborski vodovod bo zagotavljal zaupnost podatkov in informacij, njihovo zaščito pred nepooblaščenim razkritjem, namerno ali slučajno spremembo ali uničenjem.

Mariborski vodovod bo omejil dostop do informacij na način, da bo omogočen dostop do informacij le tistemu osebju, za katere to narekuje poslovna potreba ali narava dela, skladno s pooblastili in odgovornostjo.

Mariborski vodovod bo vpeljal organizacijske in tehnične ukrepe za zagotavljanje varovanja osebnih podatkov.

Informacijski sistemi in komunikacijsko omrežje podjetja morajo biti načrtovani, grajeni in vzdrževani, da zagotovijo delovanje na ustreznem nivoju zaupnosti, neoporečnosti in razpoložljivosti, glede na kritičnost, tveganje in poslovno odvisnost podjetja od teh sistemov.

Mariborski vodovod bo zagotovil z ustreznimi ukrepi varno okolje za ustvarjanje, uporabo in vzdrževanje podatkov in informacij znotraj podjetja, pri prenosu podatkov in informacij med poslovnimi enotami podjetja ter zunanjimi strankami. Prav tako bo zagotovil ustrezno pripravo podatkov in informacij za zakonito rabo izven podjetja.

Mariborski vodovod izvaja ustrezne procese in obrambne mehanizme za identifikacijo, preprečitev in okrevanje ob nastanku neljubih dogodkov, z ali brez zaznave škode, ki so lahko povzročeni namerno ali nenamerno, vključno z okvarami, nedelovanjem, krajo, poškodbami, izgubo informacij, zlorabo pooblastil, vedenje izven dobre prakse in etičnih načel ter izgubo podporne infrastrukture.

Vse organizacijske enote v Mariborskem vodovodu (sektorji, službe, PE, oddelki) so dolžne imeti in vzdrževati načrte neprekinjenega poslovanja, ki tudi opredeljujejo zahteve po razpoložljivosti informacijskih dobrin.

Sistem za upravljanje informacijske varnosti vsebuje tudi sistem (opredeljuje politika) upravljanja informacijskih tveganj, kot osnovnega orodja informacijske varnosti v podjetju. Področje upravljanja z informacijskimi tveganji določajo procesi s katerimi nadzorujemo tveganja: analiza, identifikacija, ocenjevanje, obravnava tveganj, vpeljevanje nadzoritev. Sistem za upravljanje temelji na takem pristopu do poslovnih tveganj, da zagotovi

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 7/13
	Datum zadnje revizije: 02.12.2019	

vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje sistema varovanja informacij.

6. ORGANIZIRANOST INFORMACIJSKE VARNOSTI IN PRIPADAJOČE ZADOLŽITVE

V tej točki so definirane posamezne odgovornosti vseh zaposlenih Mariborskega vodovoda z vidika informacijske varnosti.

Vodstvo podjetja

Zagotavlja potrebna sredstva in vire za uspešno izvajanje ter nadzora sistema za upravljanje informacijske varnosti, skladno z zahtevami zakonodaje, standardov, regulativ, poslovnih zahtev, varnosti ter dobro prakso. Je odgovorno za odobritev dobrin (tehničnih, kadrovskih, finančnih...) za postavitev in izvedbo programa politike varovanja informacij in upravljanja informacijskih tveganj, sodeluje pri sprejemu varnostnih kontrol, ter sprejema vse posledice, ki lahko nastanejo ob uresničitvi tveganj. Vodstvo je seznanjeno in prevzema tveganja, ki se nanašajo na uporabo informacijske tehnologije pri poslovanju. Vodstvo določa poslovne lastnike informacijskih dobrin.

Vodja sektorja informatike

Nosi polno odgovornost za varnost, neprekinjeno poslovanje, upravljanje z informacijskimi dobrinami in zagotavljanje varnih in kakovostnih informacijskih storitev.

Skrbnik dokumentacije informacijske varnosti

Je zadolžen za organizacijo in oblikovanje poslovnika informacijske varnosti in varnostnih politik. Njegove odgovornosti in naloge so:

- vzpostavitev dokumentacije SUVI,
- skrbi za ažurnost dokumentacije (posodobitve, verzioniranje, dopolnitev sprememb, veljavnost),
- objava dokumentacije v skladu z obsegom,
- odgovoren za sklic rednih srečanj foruma,
- sklicuje izredna srečanja foruma na predlog posameznih članov ali direktorja družbe
- zastopa poslovne interese podjetja pri vzpostavi varnostnih politik, standardov in postopkov.

Forum varovanja informacij

Je interdisciplinarni organ, ki ga skladno s statutom podjetja imenuje uprava Mariborskega vodovoda. Sestaja vsaj enkrat na leto ali pogosteje po potrebi. Forum varovanja informacij pomaga pri določitvi potrebnega nivoja varovanja informacijskih dobrin, glede na poslovne, zakonske in organizacijske zahteve ter predlaga kontrole, ki na najučinkovitejši način zagotavljajo potrebno stopnjo varovanja informacijskih dobrin.

Namen foruma je:

- deliti in izmenjevati izkušnje, informacije in vire med OE podjetja z vidika informacijske varnosti in implementacije,
- pomoč pri razvoju in vzdrževanju politik, standardov, postopkov, navodil, priročnikov, ki so implementirani v podjetju,
- podpora razvoju, uvajanju in vzdrževanju visokega nivoja zavesti informacijske varnosti v podjetju,
- potrditev in sprejem varnostnih politik,

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 8/13
	Datum zadnje revizije: 02.12.2019	

- ugotavlja in ocenjuje kršitve določil informacijskih varnostnih politik,
- v primeru ugotovitve kršitev določil informacijskih varnostnih politik opozori upravo podjetja in direktorja službe za splošnopravne in kadrovske zadeve,
- naloga foruma je sodelovanje pri analizi tveganj in pri ustrezni izbiri varnostnih kontrol,
- spremlja upravljanje sistema informacijskih tveganj.

Zaposleni in drugo osebje

Vsi uporabniki podatkov, informacij in informacijskih dobrin (računalniških in komunikacijskih sistemov) Mariborskega vodovoda:

- morajo biti seznanjeni z informacijsko varnostno politiko in drugimi varnostnimi standardi, postopki in priporočili,
- so odgovorni, da se poslovanje podjetja izvaja v skladu s tem poslovnikom,
- so odgovorni za prispevek k izboljšanju varnostnega stanja in odpravljanju vseh vrst tveganj,
- smejo dostopati le do tistih podatkov, informacij in sistemov za katere so pooblaščen, i,
- morajo uporabljati sisteme, podatke in informacije samo za namene odobrene s strani pooblaščenih oseb,
- ne smejo razkriti zaupnih informacij nepooblaščenim osebam,
- morajo delovati skladno z vso veljavno zakonodajo Republike Slovenije,
- so dolžni poročati svojim vodjem o vsakem varnostnem incidentu oz. neljubemu dogodku, zaznavi pomanjkljivosti in kršitvi informacijske varnosti politike.

Vodje sektorjev in vodje oddelkov

Poleg odgovornosti, ki jih imajo kot uporabniki podatkov in informacij, so vodje sektorjev in vodje oddelkov še dodatno odgovorni, da:

- seznanijo podrejene delavce z vsebino informacijsko varnostnih politik, varnostnih standardov, postopkov in drugih pravilnikov podjetja in da jih seznanijo o nevarnostih, tveganjih in obrambnih mehanizmi,
- seznanijo podrejene delavce s posledicami kršitve informacijsko varnostnih politik, merodajne zakonodaje, varnostnih standardov, postopkov in drugih pravilnikov podjetja,
- potrjujejo in preverjajo, v rednih časovnih intervalih, pravice dostopa do podatkov in informacij pri svojih podrejenih delavcih,
- podpirajo in razvijajo dobro prakso informacijske varnosti na poslovnih področjih za katere so odgovorni,
- sproti in nemudoma poročajo o varnostnih incidentih nadrejenim vodjem – direktorjem in obvestijo podporo uporabnikom (IT podpora).
- zagotovijo, da so njihovi načrti neprekinjenega poslovanja ažurni.

Poslovni lastniki informacijskih dobrin

Podatki in informacije obravnavani v ročnih ali elektronskih sistemih, morajo imeti definiranega lastnika in dodelitev lastništva mora biti dokumentirana. Poslovni lastniki informacijskih dobrin imajo pravico odločanja in odgovornost glede uporabe in zaščite podatkov, informacij in informacijskih dobrin, ki so v njihovem lastništvu. Poslovni lastniki informacijskih dobrin lahko delegirajo odgovornost na drugo osebo.

Poslovni lastnik informacijskih dobrin ima pravico in dolžnost da:

- oceni vrednost podatkov in informacij in jih klasificira,
- specifikira in uskladi kontrole in varnostne zahteve uporabnikov z vidika razpoložljivosti, zaupnosti in neoporečnosti za svoje podatke in sisteme, s sektorjem za informatiko,

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 9/13
	Datum zadnje revizije: 02.12.2019	

- redno preverja veljavnost in pravilno delovanje varnostnih ukrepov in uporabnikom dodeljena pooblastila in ob pomoči sektorja za informatiko in organizacijo nadzoruje dostop do podatkov, informacij in informacijskih dobrin, ki so v njihovi lasti,
- razpoznavajo tveganja, ki izhajajo iz nepooblaščenega dostopa do informacij in sistemov v njegovi lasti,
- zagotavljajo primeren načrt neprekinjenega poslovanja in njegovo redno testiranje.

Za izvajanje informacijsko varnostne politike na informacijskih dobrinah so odgovorni poslovni lastniki informacijskih dobrin, ki so zadolženi, da se informacijske dobrine varujejo v skladu z informacijsko varnostno politiko.

Skrbniki informacijskih dobrin

V sektorju informatike, zagotavljajo storitev informacijskega obdelovanja za podporo poslovnih operacij, ki se izvajajo v podjetju. Odgovorni so za:

- da imajo podatki, informacije in informacijske dobrine, ki so pod njihovim nadzorom, določenega lastnika,
- uvajajo in vzdržujejo nadzor, kot jih je specificiral lastnik podatkov, informacij in informacijskih dobrin, da zagotavljajo njihovo razpoložljivost, zaupnost in neoporečnost,
- nadzorujejo dostop do podatkov, informacij in informacijskih dobrin,
- pripravljajo in testirajo podrobnejše načrte neprekinjenega poslovanja, da lahko zagotovijo nemoteno informacijsko obdelovanje.

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 10/13
	Datum zadnje revizije: 02.12.2019	

7. STRUKTURA IN ORGANIZIRANOST DOKUMENTOV VARNOSTNE POLITIKE

Struktura dokumentacije upravljanja informacijske varnosti je tri nivojska (3) glede na raven odobranja.

Poslovnik informacijske varnosti je krovni dokument informacijske varnostne politike. Podaja zavezanost vodstva k varovanju informacij. Določa namen, cilje, obseg, organiziranost in strukturo varovanja informacij ter opredeljuje seznanjanje uporabnikov in jih opozarja na kršitve. *Je najvišji nivo upravljanja, dokument odobri uprava Mariborskega vodovoda.*

Politike vsebujejo pravila, ki se nanašajo na rokovanje, uporabo in upravljanje z informacijskimi dobrinami. Politike so neodvisne od tehnologije in opredeljujejo način, kako doseči ustrezen nivo varovanja in zaščite informacijskih dobrin, z opredelitvijo in predpisano uporabo varnostnih mehanizmov. Opredeljuje pravilno uporabo informacijskih dobrin, ter odgovornosti zaposlenih. *Politike so dokumenti na drugem nivoju, odobrava jih Forum varovanja informacij.*

Sistemske postopke opisujejo obvladovanje ključnih procesov.

So pravila o ravnanju z informacijskimi dobrinami in vsebujejo natančna navodila za uporabo in upravljanje pomembnejših informacijskih dobrin.

Sistemska navodila

vsebujejo začasne ukrepe in navodila o ravnanju in se uporabljajo takrat, kadar postopki in standardi še niso v celoti razviti, vendar je potrebno hitro reagirati na določene spremembe. Npr. pojavi se nova grožnja v internetu, nova tehnologija, ne ve se še natančno kakšen je njen vpliv, niti kako se zavarovati. Znano pa je, da obstaja možnost, da z določeno akcijo zmanjšamo tveganje. Ta akcija bo podana v obliki navodil, ki pa lahko ocenijo, prevedejo v politiko, standard ali postopek. Navodilo je neke vrste "standard na čakanju" in ima začasen status ter velja tako dolgo, dokler se ne izoblikujejo ustrezni interni standardi in postopki.

Sistemske postopke in navodila so dokumenti na tretjem nivoju, skladni z višjimi nivoji in jih predpisujejo vodje organizacijskih enot. Tretji nivo dokumentov lahko dopolnjuje tudi zunanja dokumentacija, ko so priročniki, standardi, dobre prakse...

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 11/13
	Datum zadnje revizije: 02.12.2019	

Struktura posamezne politike

- 1. Oznaka in ime politike**
Politike imajo oznako "VP XX-YY Ime politike", pri čemer XX označuje področje politike, YY pa njeno zaporedno številko znotraj področja
- 2. Namen**
Opis osnovnega namena in ciljev, ki jih želimo doseči.
- 3. Področje uporabe**
Komu je namenjena in/ali nad katerimi dobrinami se izvaja.
- 4. Opredelitev pojmov, okrajšav**
Opredeljen je pomen pojmov, ki se v dokumentu uporabljajo.
- 5. Politika**
Zapis o ravnanju z informacijskimi dobrinami.
- 6. Uveljavljanje politike**
Identifikacija, nespoštovanje, pravni pouk.
- 7. Reference**
Povezava z ostalimi politikami, standardi, pravilniki, navodili...povezanimi z to politiko.
- 8. Metapodatki dokumenta**
Osebe, ki so pripravile, pregledale in sprejele politiko. Datum izdaje, zadnje revizije, naslednje revizije ter verzija dokumenta. Klasifikacija in zgodovina dokumenta.

8. PODROČJA INFORMACIJSKE VARNOSTNE POLITIKE

Področja politik so v celoti povzeta po standardu ISO/IEC 27001:2013, *Priloga A - Normativa*.

Mariborski vodovod bo vzpostavila zgolj tiste (ne vse) varnostne politike, katerih področja ali njihov del, smatra za tvegana in katerih vzpostavitev prinaša neposredno korist za informacijsko varnost podjetja.

VP 01 Informacijske varnostne politike

Vzpostavitev sistema za učinkovito in uspešno varovanje informacij.

VP 02 Organiziranje informacijskih varnosti

(Notranja organizacija, Mobilne naprave in delo na daljavo)

VP 03 Varnost človeških virov

(Pred zaposlitvijo, Med zaposlitvijo, Prekinitev ali sprememba delovnega razmerja)

VP 04 Upravljanje dobrin

(Odgovornost za dobrine, Razvrstitev informacij)

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 12/13
	Datum zadnje revizije: 02.12.2019	

VP 05 Nadzor dostopa

(Poslovne zahteve pri nadzoru dostopa, Upravljanje dostopa uporabnikov, Odgovornosti uporabnikov, Nadzor dostopa do omrežja, Nadzor dostopa do operacijskega sistema, Nadzor dostopa do aplikacij)

VP 06 Kriptografija

(Zagotavljanje ustrezne uporabe kriptografije za zaščito zaupnosti, neoporečnosti in celovitosti informacij)

VP 07 Fizična in okoljska varnost

(Varovana območja, Varovanje opreme)

VP 08 Varnost operacij

(Operativni postopki, zaščita pred zlonamerno kodo, varnostno kopiranje, beleženje in spremljanje, nadzor, upravljanje tehničnih ranljivosti)

VP 09 Varnost komunikacij

(Zagotoviti zaščito informacij v omrežjih)

VP 10 Pridobivanje, razvoj in vzdrževanje sistemov

(Zagotoviti, da je informacijska varnost sestavni del informacijskih sistemov v celotnem življenjskem ciklu)

VP 11 Odnosi z dobavitelji

(Zagotoviti zaščito dobrin organizacije, ki so dostopne dobaviteljem in vzdrževati dogovorjeno raven informacijske varnosti v izvajanju storitev v skladu z dobaviteljem)

VP 12 Upravljanje informacijskih varnostnih incidentov

(Zagotoviti uporabo doslednega in uspešnega dostopa k upravljanju informacijske varnosti s sporočanjem o varnostnih dogodkih in slabostih)

VP 13 Vidik informacijske varnosti pri upravljanju neprekinjenega poslovanja

(neprekinjena informacijska varnost mora biti vključena v sisteme upravljanja neprekinjenega poslovanja)

VP 14 Skladnost

(Preprečiti kršitve pravnih obveznosti, predpisov, zakonskih ali pogodbenih obveznosti v zvezi z informacijsko varnostjo)

	POSLOVNIK INFORMACIJSKE VARNOSTI	
	Oznaka: VP 01-01	Datum izdaje: 16.4.2018
	Verzija: 2	Stran: 13/13
	Datum zadnje revizije: 02.12.2019	

9. KRŠITVE

Vsak zaposlen Mariborskega vodovoda, ki je identificiran in je ugotovljeno, da je prekršil to politiko, je glede na obseg in vsebino kršitve, lahko podvržen sankcioniranju in ustreznim disciplinskim ukrepom znotraj podjetja skladno z disciplinskim pravilnikom (»Pravilnik o odgovornosti za kršitve pogodbenih in drugih obveznosti iz delovnega razmerja«).

10. SEZNANJANJE UPORABNIKOV

Vsi uporabniki se morajo seznaniti z informacijsko varnostno politiko po načelu potrebnega vedenja. To pomeni, da se jih seznani s tistimi deli dokumenta informacijske varnostne politike, ki se tičejo njihovega dela, oziroma delovnih nalog, ki jih opravljajo.

S seznanjanjem uporabnikov zagotovimo, da se uporabniki zavedajo ogrožanja varnosti informacij, tveganja katerim so informacije, ki so povezane z njihovim delom izpostavljene in da so seznanjeni s politiko varovanja informacij in njihovimi obveznostmi.

11. UPRAVLJANJE S SPREMEBAMI V DOKUMENTACIJI

Dokumentacijo poslovnika informacijske varnostni, je potrebno pregledati vsaj enkrat na leto in preveriti ali še odraža dejansko stanje v zvezi z varovanjem informacij. Prav tako je potrebno ob implementaciji pomembnejših novih rešitev, v okviru podjetja, preveriti ali se implementacija novih rešitev odvija skladno s politiko varovanja informacij in če takšna implementacija ne zahteva tudi spremembe v programu varovanja informacij kot v samem dokumentu informacijska varnostna politika.

Spremembe tega krovnega dokumenta predlagajo člani Foruma varovanja informacij, strokovnjaki in odgovorni za varovanje podatkov. Sprejme ga direktor Mariborskega vodovoda na podlagi predloga Foruma varovanja informacij.

Obstoj tega dokumenta se posreduje z uporabo sistema obveščanja po elektronski pošti, dokument pa je dostopen na intranetu Mariborskega vodovoda. Politike bodo zaposlenim posredovane po navodilih, ki jih določi forum varovanja informacij.

Za upravljanje s spremembami je zadolžen *vodja Foruma varovanja informacij*.

Dokument se obnavlja enkrat letno (na 12 mesecev) ali po potrebi.

Izvor dokumenta: Usklajen na Forumu varovanja informacij, sprejet z odobritvijo direktorja podjetja.

	<i>Ime</i>	<i>Podpis</i>
<i>Direktor:</i>	Danilo Burnač	
<i>Sprejet na Forumu varovanja informacij, dne:</i>	3. 12. 2019	

	VARNOSTNA POLITIKA	
	SPISEK VARNOSTNIH POLITIK	
	Oznaka: VP 01-02	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 1/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKE	2
5. UVELJAVLJANJE POLITIKE	4
6. REFERENCE	4
7. PRILOGA: Zgodovina dokumenta.....	5

	VARNOSTNA POLITIKA	
	SPISEK VARNOSTNIH POLITIK	
	Oznaka: VP 01-02	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 2/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Dokument sistematično dopolnjuje »Poslovnik informacijske varnosti«. Vsebuje spisek vseh aktualnih, sprejetih varnostnih politik.

2. OBSEG

Skrbnik dokumenta je administrator informacijske varnosti. Namenjen je Forumu varovanja informacij.

3. POJMI

- **Poslovnik** informacijske varnosti je krovni dokument informacijske varnostne politike.
- **Politike** vsebujejo pravila, ki se nanašajo na rokovanje, uporabo in upravljanje z informacijskimi dobrinami.
- **Sistemske postopki** opisujejo obvladovanje ključnih procesov.
- **Sistemska navodila** vsebujejo začasne ukrepe in navodila o ravnanju in se uporabljajo takrat, kadar postopki in standardi še niso v celoti razviti, vendar je potrebno hitro reagirati na določene spremembe.

4. POLITIKE

Arhitektura dokumentov je tro (3) nivojska:

1. Poslovnik informacijske varnost, Spisek politik
2. Politike po področjih
3. Postopki, navodila, priročniki,...

Sprejeta politika je označena z:

- imenom,
- verzijo in
- datumom,

sprejema s strani Forumu.

V dokumentu je mogoče označevati tudi druge statuse politik:

- v pripravi,
- v pregledovanju (dokument je pripravljen vendar še ni pregledan),
- v sprejemanju (dokument pregledan in čaka na potrditev Forumu),
- ...

	VARNOSTNA POLITIKA	
	SPISEK VARNOSTNIH POLITIK	
	Oznaka: VP 01-02	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 3/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Spisek zadnjih verzij politik informacijske varnosti:

Področje	Ime	verzija	status	datum
1. NIVO				
VP 01 Informacijske varnostne politike (Dodatek A- A.5)				
1	VP 01-01 Poslovnik Informacijske Varnosti	2	sprejeto	2018
2	VP 01-02 Spisek varnostnih politik	2	sprejeto	2018
3	VP 01-03 Politika upravljanje tveganj	2	sprejeto	2018
2. NIVO				
VP 02 Organiziranje informacijske varnosti (dodatek A- A.6)				
4	VP 02-01 Politika mobilnih naprav	2	sprejeto	2018
5	VP 02-02 Politika dela na daljavo	2	sprejeto	2018
VP 03 Varovanje človeških virov (Dodatek A- A.7)				
6	VP 03-01 Politika varovanja človeških virov	2	sprejeto	2018
7	VP 03-02 Politika primerne rabe informacijske tehnologije	2	sprejeto	2018
VP 04 Upravljanje dobrin (Dodatek A- A.8)				
8	VP 04-01 Politika upravljanja dobrin	1	Nova - sprejeto	2018
VP 05 Nadzor dostopa (Dodatek A- A.9)				
9	VP 05-01 Politika nadzora dostopa	2	sprejeto	2018
10	VP 05-02 Politika uporabe gesel	2	sprejeto	2018
VP 06 Kriptografija (Dodatek A- A.10)				
11	VP 06-01 Politika kriptografije	1	Nova - sprejeto	2018
VP 07 Fizična in okoljska varnost (Dodatek A- A.11)				
12	VP 07-01 Politika fizičnega varovanja	2	sprejeto	2018
13	VP 07-02 Politika čiste mize in zaslona	1	Nova - sprejeto	2018
VP 08 Varnost operacij (Dodatek A- A.12)				
14	VP 08-01 Politika varnosti operacij	2	sprejeto	2018
15	VP 08-02 Politika varnostnega kopiranja	2	sprejeto	2018
16	VP 08-03 Politika zaščite pred zlonamerno programsko opremo	2	sprejeto	2018
VP 09 Varnost komunikacij (Dodatek A - A.13)				

	VARNOSTNA POLITIKA	
	SPISEK VARNOSTNIH POLITIK	
	Oznaka: VP 01-02	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 4/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

17	VP 09-01 Politika varnosti komunikacij	1	sprejeto	2018
18	VP 09-02 Politika uporabe elektronske pošte	2	sprejeto	2018
19	VP 09-03 Politika uporabe interneta	2	sprejeto	2018
20	VP 09-04 Politika varnega e-poslovanja	1	sprejeto	2018
VP 10 Pridobivanje, razvoj in vzdrževanje sistemov (Dodatek A- A.14)				
21	VP 10-01 Politika razvoja in vzdrževanja sistemov	1	Nova - sprejeto	2018
VP 11 Odnosi z dobavitelji (Dodatek A- A.15)				
22	VP 11-01 Politika odnosov do dobaviteljev	2	sprejeto	2018
VP 12 Upravljanje informacijskih varnostnih incidentov (Dodatek A- A.16)				
23	VP 12-01 Politika upravljanja incidentov	2	sprejeto	2018
VP 13 Vidiki informacijske varnosti pri upravljanju neprekinjenega poslovanja (Dodatek A- A.17)				
24	VP 13-01 Politika upravljanja neprekinjenega poslovanja IT (poslovna skrivnost)	osnutek	V pripravi	
VP 14 Skladnost (Dodatek A- A.18)				
3. NIVO				
Postopki, Navodila				

5. UVELJAVLJANJE POLITIKE

Vsebina dokumenta nima vpliva na sprejete varnostne politike.

6. REFERENCE

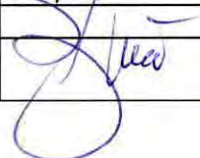
- Poslovník informacijske varnosti
- ISO/IEC 27001 - 2013, 27002

	VARNOSTNA POLITIKA	
	SPISEK VARNOSTNIH POLITIK	
	Oznaka: VP 01-02	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 5/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

7. PRILOGA: Zgodovina dokumenta

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	Apr.2018	Dodane spr.	VP_01_02_SpisekVP	Posodobitev vseh politik
2	2019-12	Dodane spr.		Dodal:
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 1/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA.....	3
4.1 Pristop	3
4.2 Identifikacija procesov	4
4.3 Identifikacija informacijskih dobrin.....	5
4.3 Vrednotenje informacijskih dobrin	5
4.4 Ocena ogroženosti	6
4.5 Ocena tveganj	8
4.6 Obravnavanje tveganj	8
4.7 Podrobno ocenjevanje (izjemoma).....	8
4.8 Uvajanje nadzorstev	9
4.9 Ostanek tveganja	9
4.10 Vzdrževanje sistema upravljanja tveganj	9
5. UVELJAVLJANJE POLITIKE	9
6. REFERENCE.....	10
7. ZGODOVINA	10

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 2/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**

1. NAMEN

Mariborski vodovod d.d. skladno z sistemom upravljanja varovanja informacij (SUVI) po smernicah ISO/IEC 27001 vpeljuje sistem obravnave informacijskih tveganj, kot glavnega orodja informacijske varnosti (*Poslovnik informacijske varnosti, poglavje 5*).

Ta politika opredeljuje metodologijo iskanja in ovrednotenja informacijskih tveganj, ki jim je podjetje izpostavljena pri svojem poslovanju. Mariborski vodovod si postavlja kriterij za sprejemanje tveganj in v skladu s tem kriterijem določena izmed ugotovljenih tveganj sprejme. Za nesprejemljiva tveganja podjetje opredeli, načrtuje in izvede primerne načine za njihovo znižanje na sprejemljiv nivo. Mariborski vodovod redno spremlja izvajanje opredeljenih načinov zniževanja tveganj in ugotavlja, ali dejansko učinkujejo v skladu z zastavljenimi nameni.

2. OBSEG

Mariborski vodovod bo obravnaval informacijska tveganja za temeljne (ključne) poslovne procese sektorjev.

Upravljanje tveganj je namenjeno in dostopno vodstvu sektorja informatike, lastnikom procesov (vodjem sektorjev in oddelkov) in vodstvu podjetja ter ga obravnava forum varovanja informacij.

3. POJMI

- **Podjetje:** pomeni Mariborski vodovod d.d.
- **SUVI:** sistem upravljanja varovanja informacij
- **Z/N/R:** okrajšava za Zaupnost/Neoporečnost/Razpoložljivost
- **Informacijska dobrina:** ali skrajšano dobrina je opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema,...). Sem lahko štejemo tudi potrebne podatke, ljudi... potrebne za delovanje storitve
- **Sestavljena dobrina:** združena dobrina iz več posameznih dobrin

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 3/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**

4. POLITIKA

4.1 Pristop

Kvalitativna metoda

Mariborski vodovod ocenjevanje tveganj izvede po kvalitativni metodi, kar pomeni, da ocene temeljijo na mnenju osebja, ki daje ocene, pri čemer se ocene razvrstijo v nekaj naprej pripravljenih razredov. Temelji na scenarijih in vprašalnikih in je v osnovi subjektivna.

Kombiniran pristop

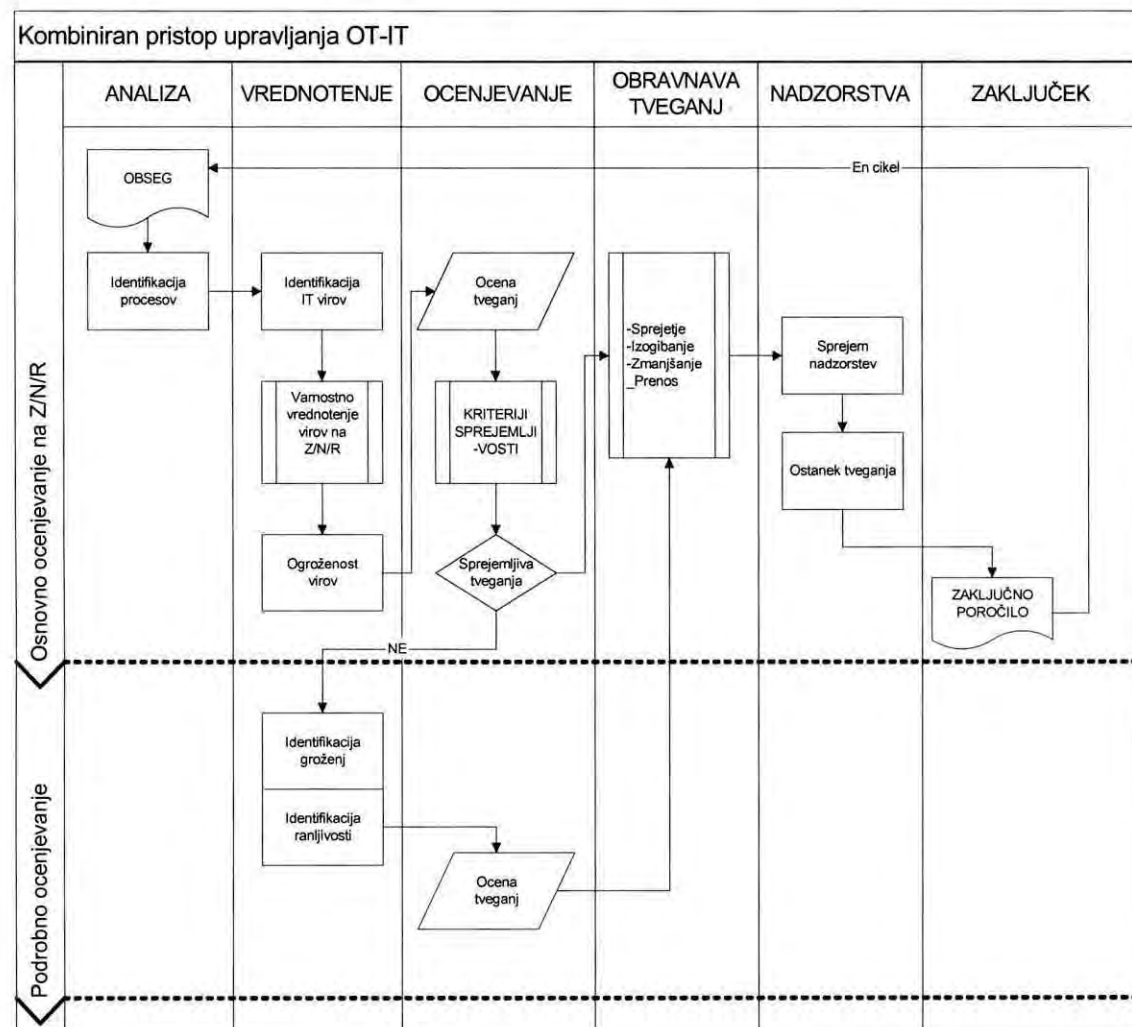
Skladno z poslovnimi potrebami se med osnovnim in podrobnim ocenjevanjem uporabi kombiniran pristop, ki je kombinacija osnovnega in po potrebi podrobnega ocenjevanja tveganj. Smiselnost sočasne uporabe zmanjša nepotrebno kompleksnost ter poveča učinkovitost.

- **Osnovno ocenjevanje** tveganj se izvede glede na Z/N/R. Tveganja tako predstavlja dve dimenziji (dvojček) sestavljen iz varnostne ocene dobrine in varnostnih vidikov, povezanih z njim.
- **Podrobno ocenjevanje** tveganj, kjer se vsaki dobrini ob vrednosti, določajo ranljivosti in grožnje, ki mu grozijo (3 dimenzija) je smiselno v nekaterih primerih, kadar rezultat osnovnega ocenjevanja kaže na nesprejemljiva tveganja. Takšno ocenjevanje se lahko izvede tudi za posamezne poslovne procese kadar to prinaša dodatno korist.

Optimizacija ocenjevanja s kombiniranim pristopom podjetju skrajša trajanje in zmanjša količino potrebnih sredstev, ter se podrobno posveti predvsem pomembnejšim večjim tveganjem, s čimer zagotavlja večjo učinkovitost izvajanja ocenjevanja

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 4/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**



Slika 1: proces upravljanja informacijskih tveganj

4.2 Identifikacija procesov

Sektor informatike ima vzpostavljen katalog informatiziranih procesov. Ta vsebuje poslovne procese po posameznih področjih (sektorjih), določa lastništvo procesov in informacijsko podporo procesom. Temeljni informatizirani procesi so identificirani z:

- Kataloga informatiziranih procesov
- Razgovora z lastnikom procesa – vodjem sektorja oz. službe
- Vodjem sektorja informatike

Za identificirane procese se izvede vprašalnik »Zahtevana zaščita podatkov« procesov v sektorju glede na kriterije Z/N/R.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 5/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**

Škodni kriteriji se opredelijo tako:

- 4 - Grožnja poslovnemu preživetju
- 3 – Resna škoda (do 50.000€)
- 2- Srednja škoda (do 5.000€)
- 1 - Manjša škoda (do 1.000€)
- 0 - Brez vpliva

4.3 Identifikacija informacijskih dobrin

V okviru ugotavljanja in ocenjevanja dobrin, Mariborski vodovod ugotovi tiste dobrine, ki predstavljajo vse, kar ima zanjo, za njeno poslovno delovanje ali neprekinjenost njenega poslovanja poslovno vrednost ali koristnost s stališča tajnosti, celovitosti, razpoložljivosti ali zakonskih in pogodbenih zahtev.

Vsaka identificirana dobrina znotraj seznama je okarakteriziran z :

- ID – uporabi se inventarna številka za opredmetene dobrine, ali zaporedna oznaka
- Naziv dobrine – kratek naziv
- Opis – razpoznaven opis dobrine
- Skrbnik – skrbnik iz IT
- Lokacija – naziv mikrolokacije

Zaradi lažje obravnave se dobrine združuje v skupine (sestavljene dobrine). Skupine se tvorijo glede na skupne varnostne značilnosti dobrin in pomembnosti za poslovanje. Skupine naj imajo znane posamične dele ali njihove lastnike. Vsaka skupina dobrin predstavlja nov sestavljen dobro, posameznih sestavnih delov pa ne vodi več kot samostojne dobrine. Sestavljenim dobrinam se določi enega glavnega lastnika.

Dobrine so razvrščeni v naslednje tipske razrede glede na njihovo vrsto :

- okolje in infrastruktura,
- strojna oprema,
- programska oprema,
- sistemska programska oprema,
- komunikacije,
- dokumenti in podatki ,
- splošni dobrine.

4.3 Vrednotenje informacijskih dobrin

Za potrebe osnovnega ocenjevanja tveganj se vzpostavi vrednostne razrede dobrin in določi jasne kriterije za razvrstitev vanje. Kriteriji lahko vključujejo več vidikov za ocenjevanje in naj med drugim zajemajo naslednje vidike:

- finančna vrednost dobrine,
- vpliv na denarni tok poslovanja,
- vpliv na zakonske in pogodbene obveznosti,
- vpliv na ugled.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 6/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**

Identificiranim IT dobrinam se dodeli varnostna ocena glede na Z/N/R in ostalo po sledeči varnostni klasifikaciji. Le ta upošteva njegove lastnosti in poslovno okolje, kjer se dobrina nahaja.

Zaupnost	0	ni vpliva
	1	razkriti nekritični podatki
	2	razkriti posamezni zaupni podatki
	3	razkriti kritični podatki
	4	ogrožen obstoj podjetja
Neoporečnost	0	ni vpliva
	1	takojšnje odkritje in samodejna povrnitev oz. zavrnitev
	2	delna motnja poslovanja za obnovo podatkov
	3	velika časovna zahtevnost obnovitve podatkov(delno ustavljeno poslovanje)
	4	podatki so uničeni ali neuporabni
Razpoložljivost	0	ni vpliva
	1	ni ogroženo osnovno poslovanje podjetja
	2	posamezni poslovni procesi podjetja so nefunkcionalni
	3	ustavljeno poslovanje za manj kot 2 dni
	4	ustavljeno poslovanje za več kot 2 dni
(Ostalo)	0	ni vpliva
	1	minimalen vpliv na ugled
	2	srednji vpliv na ugled
	3	bistven vpliv na ugled
	4	ustavitev poslovanja podjetja

Tabela 1: varnostno ocenjevanje IT dobrin

4.4 Ocena ogroženosti

Za zbiranje informacij o oceni ogroženosti dobrin, (ki je glede na osnovno ocenjevanje, skupna ocena, groženj in ranljivosti) se lahko analizira statistika prijave napak – incidentov in opravilo osebni intervjuji s skrbniškim osebjem. Kriteriji za oceno zaupnosti in neoporečnosti pa se dopolnijo z uvedenimi kontrolami na pomembnejših področjih- avtentifikacija, pooblastila za dostop, izmenjava podatkov, sledljivost.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 7/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**

RAZPOLOŽLJIVOST	
Kako pogosto je bil sistem v preteklosti nedosegljiv?	
Koliko časa je traja odprava napake?	
Kako pogosti so posegi z administratorskimi pooblastili?	
Kaj če teh posegov ne bi bilo?	
I-zelo nizka	1x na 2 let1, odprava napake 1 ura
II-nizka	Do 1x letno, odprava napake 2 uri
III-srednja	do 2x letno, odprava napake 4 ure
IV-visoka	več krat mesečno, poslovanje moteno 1 uro, odprava do 1 dan
V-zelo visoka	zelo visoka: tedensko, moteno 4ure, odprava napake v podatkih 1 dan
ZAUPNOST IN NEOPOREČNOST	
Avtentifikacija v sistem	
I-zelo nizka	Certifikat ali biometrija?
II-nizka	Obvezno geslo- vsiljena menjava?
III-srednja	obvezno geslo- redna menjava
IV-visoka	Stalno geslo-ne kriptiran prenos?
V-zelo visoka	Nikakršna kontrola identitete?
Pooblastila za dostop	
I-zelo nizka	pooblastila skladna z delovnim procesom, obstaja SuperUser (SU)
II-nizka	pooblastila skladna z delovnim procesom, ne obstaja SU
III-srednja	sistem pooblastil v app ni povsem skladen z delitvijo, SU ima nekaj ljudi
IV-visoka	precejšnja neskladnost med sistemom pooblastila in procesom, veliko SU
V-zelo visoka	vsem uporabnikom so dostopne vse funkcionalnosti in vsi podatki
Izmenjava podatkov	
I-zelo nizka	LAN in WAN šifrirana
II-nizka	LAN ni šifrirana, WAN šifrirana
III-srednja	WAN šifrirana
IV-visoka	WAN ni šifrirana
V-zelo visoka	WAN ni šifrirana
Sledljivost	
I-zelo nizka	Beleži se zgodovina vseh sprememb in vpogledov v podatke?
II-nizka	Beleži se zgodovina vseh sprememb in vpogledov v podatke?
III-srednja	Beleži se zgodovina sprememb, NE pa vpogledov?
IV-visoka	Beležijo se podatki o zadnji spremembi ne pa zgodovina?
V-zelo visoka	Ni nobene sledljivosti, kaj je kdo delal na sistemu?

Tabela 2: Kriterij za ocenjevanje ogroženosti glede Z/N/R.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 8/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**

4.5 Ocena tveganj

Glede na varnostno oceno in oceno ogroženosti se po matriki določi stopnja – ocena tveganja:

Ocena dobrine	Ogroženost na Z/N/R				
	I- Zelo nizka	II-Nizka	III-Srednja	IV-Visoka	V-zelo visoka
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Tabela 3: matrika za izračun ocene tveganja

Kriterij sprejemljivosti tveganja:

- tveganja ni: 0,
- sprejemljivo tveganje: 1-4,
- pogojno sprejemljivo tveganje: 5,
- nesprejemljivo tveganje: 6-8.

4.6 Obravnavanje tveganj

Obravnavanje tveganj je sistematična metodologija za zmanjšanje vpliva tveganj, ki jo uporablja Mariborski vodovod. Možni so različni načini obravnave tveganj:

- Izogibanje tveganj: izogibanje vključno z vzroki in posledicami nastanka tveganj.
- Sprejetje tveganj: zavestno sprejetje z vsemi posledicami zaradi njihove nepomembnosti ali drugih poslovnih vzrokov.
- Prenos tveganj: tveganje se prenese na drugo osebo, zavarovalnico, dobavitelja, vzdrževalca...
- Zmanjšanje tveganj: z izvajanjem ukrepov, ki ublažijo nezaželene posledice ogroženosti (groženj in ranljivosti).

4.7 Podrobno ocenjevanje (izjemoma)

Mariborski vodovod lahko razširi osnovni način ocenjevanja tveganj z podrobnim ocenjevanjem. Tak način je zaradi kompleksnosti primeren le v kolikor prinaša dodatne koristi za podjetje, glede na vložen trud. Takšno ocenjevanje se lahko koristi recimo v naslednjih primerih:

- Ocena tveganja v osnovnem načinu kaže na nesprejemljiva tveganja (Točka 4.6 - področje 7-9).
- Vrednotenje informacijske dobrine (točka 4.4) ali ocena ogroženosti (4.5) ni primerna (ne zajema primernih lastnosti) za označevanje posamezne dobrine.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 9/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**

- Z obravnavo tveganj (točka 4.7) ni možno vplivati na zmanjšanje tveganj, za to je potrebna podrobna analiza.
- Kadar obstaja zahteva, da se informacijska tveganja dopolnijo z ostalimi oblikami tveganj (ljudi, procesov,...)
- Ostali razlogi, regulative, ETZ...

V podrobnem ocenjevanju se za posamezna ali sestavljena dobrina pripravita tabela ranljivosti in tabela groženj.

4.8 Uvajanje nadzorstev

Mariborski v okviru zmanjševanja tveganja po potrebi vpeljuje kombinacijo **tehničnih in ne tehničnih nadzorstev**. Le ta se delijo po načinu delovanja oziroma zmanjševanja tveganj na:

- preventivna (varnostna politika),
- svarilna - nas opozarja, da ne pride do napak,
- Detektorska - obvestila o poskusih zlorabe in poskusih zlorabe varnostnih sistemov,
- Okrevalna - pomoč pri okrevanju in doseganje neprekinjenosti poslovanja,
- Popravljalna - izboljševanje varnostnih mehanizmov, ko se je tveganje že uresničilo,
- Spremljevalna - omogočajo boljši nadzor nad dogajanjem,
- Ozaveščevalna - seznanjanje osebja z varnostno problematiko.

4.9 Ostanek tveganja

Vsa tveganja, ki jih z uvedbo naprednih nadzorstev ni mogoče izničiti se imenujejo **ostanek tveganja**. Ostanek tveganj odobri vodstvo Mariborskega vodovoda, s čemer potrjuje, da se tveganja zaveda in, da ga zavestno sprejema zaradi poslovnih razlogov.

4.10 Vzdrževanje sistema upravljanja tveganj

Upravljanje tveganj v Mariborskem vodovodu je vgrajeno v upravljanje sistema varovanja informacij (SUVI), kot del dobre prakse in ker podpira poslovne cilje podjetja.

Mariborski vodovod bo redno vzdrževal ta sistem upravljanja tveganj. Pogostost rednega pregledovanja te politike in priprava poročila bo najmanj enkrat letno, po večjih incidentih ali spremembi informacijskih rešitev pa lahko sledi tudi izredni pregled.

Mariborski vodovod bo pri ponovnih izvedbah ocenjevanja in obravnave tveganj opravil le tiste korake te metodologije, ki jih je treba izvesti zaradi sprememb v okolju ali poslovanju.

Mariborski vodovod se lahko pri ponovni izvedbi ocenjevanja in obravnave tveganj, pri posameznem koraku omeji na ožji obseg, če je to utemeljeno.

5. UVELJAVLJANJE POLITIKE

Odgovornost za sistem upravljanja informacijskih tveganj nosi forum varovanja informacij.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INFORMACIJSKIH TVEGANJ	
	Oznaka: VP 01-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 10/10
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **POSLOVNA SKRIVNOST**

6. REFERENCE

Metodologijo podpirajo mednarodni standardi:

- ISO/IEC 27001:2005 - Information Security
- ISO/IEC 31000:2011 – Risk Management
- dobra praksa v slovenskih finančnih institucijah (Metodologija ZBS - Metodologija ocenjevanja in obravnave informacijskih tveganj v bankah)

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	dec. 2014	Osnutek	VP_01_03_Upravljanje tveganj	Pripravi: Bojan Erker
2	Apr. 2018	Dodane spr.	VP_01_03_Upravljanje tveganj	Spremembe: terminologija, popravki
3	Dec 2019	Dodane spr.		Revizija
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA MOBILNIH NAPRAV	
	Oznaka: VP 02-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 1/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	3
4.1. Evidenca in nadzor mobilnih in pomnilniških naprav	3
4.2. Overitev uporabe mobilnih naprav in varnostne zahteve	3
4.3. Varovanje informacij na mobilnih napravah	3
4.4. Aplikacije na mobilnih napravah (App Store, Google- trgovina Play)	4
5. UVELJAVLJANJE POLITIKE	5
6. REFERENCE	5
7. ZGODOVINA	5

	VARNOSTNA POLITIKA	
	POLITIKA MOBILNIH NAPRAV	
	Oznaka: VP 02-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 2/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Mobilne računalniške naprave, ki se preko WiFi, Ethernet ali USB vmesnikov priključujejo v informacijski sistem Mariborskega vodovoda odpirajo širok spekter tveganj in pomenijo veliko grožnjo občutljivim informacijam. Mobilne naprave so orodje in hkrati priročen pripomoček tako za odnašanje podatkov iz podjetja, kot za vnos škodljive programske opreme. Mariborski vodovod je na ta način izpostavljen tveganjem izgube ali zlorabe osebnih podatkov in drugih zaupnih podatkov. Zaradi vseh omenjenih groženj in tveganj moramo zagotavljati ustrezne postopke in uporabo ustreznih tehnoloških rešitev za varno rabo teh naprav. Z upoštevanjem postopkov in z uporabo priporočenih tehnoloških rešitev bomo omejili škodo zaradi škodljive programske opreme, izgube pomembnih podatkov in se v največji možni meri izognili ranljivosti podjetja, možnim tožbam ali izgubi ugleda.

Namen politike uporabe mobilnih računalniških naprav je vzpostaviti varnostne mehanizme za uporabo prenosnih pomnilniških in računalniških naprav in neposredno in posredno priključevanje teh naprav v informacijski sistem Mariborskega vodovoda.

2. OBSEG

Ta politika se nanaša na vse uporabnike, posebno pa na vse tiste, ki imajo svoje mobilne računalniške naprave, ali jim je bila dana v uporabo mobilna naprava, ki je last Mariborskega vodovoda. Politika se nanaša tudi na tretje stranke, ki prinašajo mobilne naprave v informacijsko okolje podjetja.

Politika se ne nanaša na mobilne računalniške naprave, ki se ne priključujejo v omrežje, ki jih upravlja Mariborski vodovod in se uporabljajo za dostop do javno dostopnih vsebin.

S to politiko so seznanjeni in so jo dolžni spoštovati vsi zaposleni Mariborskega vodovoda in ostali uporabniki.

3. POJMI

Uporabniki: so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, tretje osebe in ostali delavci

Mobilne (računalniške) naprave: prenosni računalniki ter pametni telefoni in tablice, ki koristijo operacijski sistem IOS, Android, Windows, Symbian, BlackBerry in ostale.

Pomnilniška naprava: naprava namenjena shranjevanju informacij, brez možnosti procesiranja, največkrat prenosni disk ali ključ z USB vmesnikom.

Oddaljen dostop: dostop preko interneta za delo na daljavo ali mobilno delo

Delo na daljavo: delo na opremi in napravah, ki niso v lasti podjetja t.i. »delo od doma« ali delo tretjih oseb, dobaviteljev.

Mobilno delo: delo na opremi in napravah, ki so v lasti in upravljanju Mariborskega vodovoda (izposojena oprema)

Informacijska dobrina: opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema,...)

VPN: (ang. *Virtual Private Network*) navidezno zasebno omrežje

	VARNOSTNA POLITIKA	
	POLITIKA MOBILNIH NAPRAV	
	Oznaka: VP 02-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 3/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4. POLITIKA

4.1. Evidenca in nadzor mobilnih in pomnilniških naprav

Mariborski vodovod ima pripravljen seznam in vzdržuje evidenco vseh mobilnih naprav, ki se neposredno ali posredno priključujejo v informacijski sistem podjetja. Evidenca naprav vsebuje podatke o vrsti, proizvajalcu, tipu, serijski številki, uporabniku in datumu začetka uporabe naprave. Spisek se nahaja v datoteki **seznam_mobilnih_naprav.xls**

Nadzor evidence in uporabe naprav prenosnih računalnikov in dlančnikov izvaja redno sektor za informatiko. Evidenco mobilnih (pametnih) telefonov vzdržuje Sektor črpanja, povezovanje teh naprav v omrežje mariborskega vodovoda pa sektor informatike.

4.2. Overitev uporabe mobilnih naprav in varnostne zahteve

V informacijski sistem podjetja se lahko priključujejo (preko WiFi, Ethernet, USB, Bluetooth) le naprave, ki so v lasti Mariborskega vodovoda d.d..

Priključevanje osebnih mobilnih naprav je strogo prepovedano! Izjema je priključitev do odprtega WiFi omrežja znotraj podjetja (odprta dostopna točka MV), kjer je ta na voljo. Dovoljenje za vključitev osebne mobilne naprave (ki ni v lasti podjetja) v omrežje Mariborskega vodovoda izda Sektor za informatiko na podlagi predhodne preveritve naprave.

Za priključitev in delo na daljavo velja politika *VP-07-04 Politika oddaljenega dostopa*.

Za pripravo oz. za overitev naprav za uporabo v okviru informacijskega sistema podjetja poskrbi Sektor za informatiko. Osnovni vodili za pripravo oz. overitev naprave sta:

- Vsaka naprava za katero obstaja programska oprema za zaščito pred zlonamerno programsko opremo mora to programsko opremo imeti nameščeno in pravilno vzdrževano (požarna pregrada, antivirus...).
- Obvezne sistemske nastavitve naprav se ne smejo spreminjati brez predhodnega soglasja Sektorja informatike. Skrbnik prenosnih računalniških in pomnilniških naprav morajo poskrbeti za pravočasno nameščanje vseh varnostnih popravkov sistemske in druge programske opreme naprav.

4.3. Varovanje informacij na mobilnih napravah

Zaradi svoje majhnosti in priročnosti so mobilne naprave bolj izpostavljene odtujitvi, kot namizni osebni računalniki. Ob odtujitvi mobilne naprave se pojavi tudi tveganje, da občutljivi podatki in informacije zaidejo v nepravne roke.

Izguba ali odtujitev mobilne naprave predstavlja varnostni incident, ki ga je potrebno nemudoma prijaviti na enotno vstopno točko za podporo uporabnikom »pomoč uporabnikom« int. tel. 261 ali na elektronski naslov it.podpora@mb-vodovod.si. (VP 09-01 Politika upravljanja incidentov)

	VARNOSTNA POLITIKA	
	POLITIKA MOBILNIH NAPRAV	
	Oznaka: VP 02-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 4/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

V primeru uporabe mobilne naprave je uporabnik dolžan spoštovati vse politike informacijske varnosti, ki veljajo za delo znotraj Mariborskega vodovoda. (Enako kot točka 4.2. *Varovanje informacij Politika oddaljenega dostopa*)

Kadar uporabnik dostopa z mobilno napravo do informacijskega sistema Mariborskega vodovoda, mu je (lahko) na voljo identično okolje, kakor znotraj podjetja. Mobilna naprava s katero dostopa v omrežje podjetja je glede na zunanje okolje izpostavljena različnim tveganjem. Za to je uporabnik dolžan sprejeti dodatne ukrepe, da zagotovi enako raven varovanja, kot je znotraj podjetja.

Glavna tveganja, ki jim je izpostavljen uporabnik mobilne naprave in posledično podjetje:

- V kolikor uporablja **osebne podatke**, katere upravljaavec je Mariborski vodovod je odgovoren za zagotavljanje skladnosti z Zakonom o varstvo osebnih podatkov (ZVOP).
- Uporabnik prevzema odgovornost za shranjevanje podatkov na mobilni napravi.
- Mobilne naprave, na katerih hranimo občutljive podatke, morajo biti pod stalnim nadzorom.
- Poskrbeti je dolžan za iztiskane občutljive podatke in njihovo varnostno uničenje.
- Za mobilno napravo velja pravilo »čistega zaslona«. Uporabnik poskrbi za zaklepanje zaslona z geslom.
- Mobilne naprave morajo biti zaščitene pred krajo.
- Uporabnik naj poskrbi za varnostne kopije pomembnih lokalnih podatkov, ter jih mora ustrezno zaščititi za primer odtujitve ali okvare oddaljene naprave(npr. na strežnik podjetja).

Ukrepi za varovanje informacij:

Poslovna skrivnost	Interno	Za javnost
Tudi za Osebne podatke • Zaklepanje naprave (pin, geslo) je obvezno! • Informacije morajo biti kriptirane! • Varnostne kopije takšnih podatkov so lahko le na strežnikih podjetja ali lokalno zaklenjene.	• Zaklepanje naprave (pin, geslo) je obvezno! • Kriptiranje informacij je priporočljivo!	• Zaklepanje naprave (pin, geslo) je obvezno!

4.4. Aplikacije na mobilnih napravah (App Store, Google- trgovina Play)

Aplikacije so posebna dodana vrednost mobilnih naprav, vendar je problematična njihova zasebnost!

Veliko aplikacij na trgu zahteva od vas preveč dovoljenj, lahko bi dejali, da imajo »prevelike apetite«, dostopajo lahko do vseh podatkov na vaši napravi ali celo prevzamejo nadzor nad funkcijami naprave.

	VARNOSTNA POLITIKA	
	POLITIKA MOBILNIH NAPRAV	
	Oznaka: VP 02-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 5/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- Na prenosnih računalnikih je dovoljena uporaba zgolj licenčne programske opreme za katero poskrbi sektor za informatiko.
- Na dlančnike, ki so namenjeni uporabi službenih aplikacij je prepovedano kakršnokoli nameščanje mobilnih aplikacij brez dovoljenja sektorja za informatiko.
- Na dlančnike in pametne mobilne telefone, ki ne koristijo službenim aplikacijam ali povezovanju, razen elektronske pošte je dovoljena instalacija programske opreme samo z uradnih trgovin (Google trgovina, App Store, Amazon) skladno z licenčni pogoji.

Prepovedano je t.i. »lomljenje« naprave z namenom pridobitve popolnega nadzora ang. »jailbreak« ali »rooting« naprav.

5. UVELJAVLJANJE POLITIKE

Vsak zaposleni, na katerega se nanaša ta politika, ki je identificiran in je ugotovljeno, da je prekršil to politiko, je glede na obseg in vsebino kršitve lahko podvržen sankcioniranju in ustreznim disciplinskim ukrepom podjetja.

Tretje osebe, ki kršijo to politiko so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

- Uporabljena nadzorstva ISO/IEC 27001-2013:
A.6.2.1 Politika na področju mobilnih naprav
A.6.2.2 Delo na daljavo
- Politika je v soodvisnosti z politikami: VP 02-02 Politika oddaljenega dostopa
VP 12-01 Politika upravljanja incidentov

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VP_07_03_P olitikaMobilnih Naprav	VP_02_01_PolitikaMobilnihNaprav.docx	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Revizija
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3. 12. 2019	

	VARNOSTNA POLITIKA	
	POLITIKA DELA NA DALJAVO	
	Oznaka: VP 02-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 1/5
	Datum zadnje revizije: 01.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1. Avtorizacija za oddaljen dostop	2
4.2. Varovanje informacij.....	3
4.3. Uporabniška oprema za delo na daljavo.....	4
4.4. Nadzor oddaljenega dostopa do omrežja (VPN)	4
5. UVELJAVLJANJE POLITIKE	4
6. REFERENCE	5
7. ZGODOVINA.....	5

	VARNOSTNA POLITIKA	
	POLITIKA DELA NA DALJAVO	
	Oznaka: VP 02-02	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 2/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Politika oddaljenega dostopa uveljavlja pravila dela na daljavo in mobilnega dela. Delo na daljavo za razliko od mobilnega dela pomeni najpogostejše »delo od doma« ali »dostop tretjih oseb«, na domači opremi ali opremi (prenosna ali fiksna oprema), ki ni v lasti in upravljanju Mariborskega vodovoda. Mobilno delo poteka na službeni opremi (prenosna ali fiksna oprema), ki je v lasti ali upravljanju podjetja, ki pa se po načinu povezovanja, povezuje v omrežje podjetja preko interneta.

Oddaljen dostop postavlja dodatna varnostna vprašanja, saj se uporabniki povezujejo v omrežje podjetja preko javno dostopnega omrežja – interneta, ob zahtevi, da bodo imeli na voljo iste storitve in podatke, kakor v pisarni.

Ker imajo oddaljeni uporabniki enak dostop, kot uporabniki znotraj podjetja, vnašajo v informacijski sistem dodatna varnostna tveganja. Posebno tveganje vnaša domača oprema in oprema tretjih strank.

2. OBSEG

Politika opredeljuje način povezovanja z informacijskim sistemom Mariborskega vodovoda in zahteve opreme, z njo pa morajo biti seznanjeni vsi tisti uporabniki (zaposleni ali tretje osebe), ki so za takšen način oddaljenega dostopa pooblašeni.

3. POJMI

Uporabniki: so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, tretje osebe in ostali delavci.

Oddaljen dostop: dostop preko interneta za delo na daljavo ali mobilno delo

Delo na daljavo: delo na opremi in napravah, ki niso v lasti podjetja t.i. »delo od doma« ali delo tretjih oseb, pogodbenikov.

Mobilno delo: delo na opremi in napravah, ki so v lasti in upravljanju podjetja (izposojena oprema)

Oprema in naprave: vse vrste opreme, ki omogočajo daljinski dostop - računalniki, prenosnik, dlančniki, pametni telefoni...

Informacijski vir: opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema,...)

VPN: (ang. *Virtual Private Network*) navidezno zasebno omrežje

4. POLITIKA

4.1. Avtorizacija za oddaljen dostop

Vsi uporabniki, katerih narava dela to zahteva imajo možnost za oddaljen dostop. Mariborski vodovod nima formaliziranega postopka, dostop se dodeli glede na zahtevo vodje

	VARNOSTNA POLITIKA	
	POLITIKA DELA NA DALJAVO	
	Oznaka: VP 02-02	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 3/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

organizacijske enote. Poslovni partnerji, ki so dobavitelji programske opreme lahko imajo za vzdrževanje njihove programske opreme omogočen oddaljen dostop, ki ga odobri in je pod nadzorom sektorja informatike. Podrobnosti dostopa so opredeljene v pogodbi o vzdrževanju programske opreme ali drugem dokumentu.

Podrobnosti v *VP 05-01 Politika nadzora dostopa*.

4.2. Varovanje informacij

V primeru oddaljenega dostopa je uporabnik dolžan spoštovati vse politike informacijske varnosti, ki veljajo za delo znotraj Mariborskega vodovoda.

Kadar uporabnik oddaljeno dostopa do informacijskega sistema podjetja, mu je na voljo enako okolje, kakor znotraj podjetja. Informacijska naprava s katero dostopa v omrežje je glede na zunanje okolje izpostavljena različnim tveganjem. Za to je uporabnik dolžan sprejeti dodatne ukrepe, da zagotovi enako raven varovanja, kot je znotraj Mariborskega vodovoda.

Glavna tveganja, ki jim je uporabnik (posledično podjetje) pri oddaljenem dostopu izpostavljen:

- V kolikor uporablja **osebne podatke**, katere upravljaavec je podjetje je odgovoren za zagotavljanje skladnosti z Zakonom o varstvo osebnih podatkov (ZVOP).
- Uporabnik prevzema odgovornost za shranjevanje podatkov na oddaljeni lokaciji.
- Elektronske naprave, na katerih hranimo občutljive podatke (računalnik, USB ključ, zunanji disk,...) . morajo biti pod stalnim nadzorom.
- Poskrbeti je dolžan za iztiskane občutljive podatke in njihovo varnostno uničenje.
- Za oddaljeno napravo velja pravilo »čistega zaslona«. Uporabnik poskrbi za zaklepanje zaslona z geslom.
- Naprave za daljinski dostop morajo biti zaščitene pred krajo.
- Uporabnik mora poskrbeti za varnostne kopije pomembnih lokalnih podatkov, ter jih mora ustrezno zaščititi za primer odtujitve ali okvare oddaljene naprave skupni imenik strežnika podjetja.

Ukrepi za varovanje informacij:

Zaupne informacije (Osebni podatki, visoka stopnja tajnosti)	Srednje zaupne informacije (klasifikacija: interno gradivo)	Nizko zaupne informacije (brez klasifikacije zaupnosti)
• So lahko le v elektronski obliki in jih je prepovedano tiskati. • Datoteke na disku morajo biti kriptirane. • Varnostne kopije takšnih podatkov so lahko le na strežnikih podjetja ali lokalno zaklenjene.	• Se lahko nahajajo v elektronski ali tiskani obliki. • Iztiskane ali lokalne varnostne kopije morajo biti pod nadzorom, zaklenjene. • Papirno gradivo je potrebno vrniti podjetju ali uničiti (rezalnik).	• Se lahko nahaja v elektronski ali papirni obliki.

Uporabnik ob odobritvi oddaljenega dostopa pisno potrjuje seznanitev s to politiko.

	VARNOSTNA POLITIKA	
	POLITIKA DELA NA DALJAVO	
	Oznaka: VP 02-02	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 4/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.3. Uporabniška oprema za delo na daljavo

Za delo na daljavo koristijo uporabniki lastne naprave in opremo (primer: domač računalnik, internet preko operaterja), ali naprave, ki so v lasti druge družbe (tretje osebe) in niso v upravljanju ali pod nadzorom Mariborskega vodovoda.

V kolikor uporabnik deli svoj delovni prostor in napravo z drugimi udeleženci (družninski člani, sodelavci tretjih oseb...) mora na napravi imeti lasten profil, ki onemogoča dostop drugih oseb do priviligiranih storitev in podatkov uporabnika in podjetja.

Osebna oprema (ali oprema tretjih oseb), ki se uporablja za povezavo z omrežjem Mariborskega vodovoda mora izpolnjevati zahteve, ki veljajo za opremo v lasti podjetja. Varnost oddaljene naprave je lahko ogrožena z nalaganjem neavtorizirane programske opreme ali dostopom do spletnih strani, ki vsebujejo vohunsko ali drugo zlonamerno kodo, kar predstavlja kršitev varnostne politike in verjetnost širitve znotraj omrežja podjetja.

Organizacije in posamezniki, ki želijo vzpostaviti povezavo za oddaljen dostop do notranjega omrežja Mariborskega vodovoda s pomočjo nestandardne opreme, morajo pred vzpostavitvijo povezave pridobiti posebno soglasje sektorja informatike.

Za mobilno delo koristijo uporabniki namensko opremo podjetja. Uporabnik je dolžan vrniti opremo, ki mu je bila zaupana (reverz) v dogovorjenem času. Uporabnik ravna z najeto opremo v skladu varnostnimi politikami podjetja, ki opredeljujejo tudi omejeno zasebno rabo.

Izbira brezžične dostopne točke WI-FI: Uporabnikom se odsvetuje uporaba brezžičnih dostopnih točk neznanega ponudnika. Uporabnik naj izbira med preverjenimi ponudniki (telekomunikacijski operater, občinski ponudnik, znano podjetje...).

4.4. Nadzor oddaljenega dostopa do omrežja (VPN)

Napravam, ki niso v popolnem nadzoru Mariborskega vodovoda je onemogočen nepooblaščen dostop do omrežnih storitev in aplikacij.

Pooblaščen oddaljeni uporabniki, lahko komunicirajo neposredno z informacijskim sistemom podjetja za sprejem / pošiljanje podatkov in posodobitve. V kolikor obstaja poslovna potreba po takšnem povezovanju je le to možno, zgolj ob preverjanju pristnosti naprave in uporabo ustreznega avtentifikacijskega in avtorizacijskega mehanizma.

Oddaljena povezava z omrežjem podjetja, je dovoljena le, kadar je pooblaščen uporabnik potrjen, podatki pri prenosu so šifrirani.

V praksi se ti uporabniki na daljavo (od doma, na službeni poti...) povezujejo na informacijski sistem Mariborskega vodovoda preko navideznega privatnega omrežja (VPN).

5. UVELJAVLJANJE POLITIKE

Vsak zaposleni, na katerega se nanaša ta politika, ki je identificiran in je ugotovljeno, da je prekršil to politiko, je glede na obseg in vsebino kršitve lahko podvržen sankcioniranju in ustreznim disciplinskim ukrepom podjetja.

	VARNOSTNA POLITIKA	
	POLITIKA DELA NA DALJAVO	
	Oznaka: VP 02-02	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 5/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

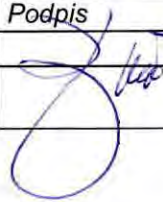
Tretje osebe, ki kršijo to politiko so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

- Uporabljeni nadzorstva ISO/IEC 27001-2013:
A.6.2.1 Politika na področju mobilnih naprav
A.6.2.2 Delo na daljavo
- Politika je v soodvisnosti z politikami: VP 05-01 Nadzor dostopa
VP 02-01 Politika mobilnih naprav

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VP_07_04_P olitikaOddalje negaDostopa	VP_02_02_PolitikaDelaNaDaljavo.docx	Pripravil: Bojan Erker
2	2019	Dodane spr.		Uredil : Bojan Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3. 12. 2019	

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA ČLOVEŠKIH VIROV	
	Oznaka: VP 03-01	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 1/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	3
4.1. Pred zaposlitvijo	3
4.2. Med zaposlitvijo	3
4.3. Prekinitev ali sprememba zaposlitve	3
5. UVELJAVLJANJE POLITIKE	4
6. REFERENCE	4
7. ZGODOVINA	4

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA ČLOVEŠKIH VIROV	
	Oznaka: VP 03-01	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 2/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Ena temeljnih obvez Mariborskega vodovoda je varovati zaposlene in podjetje pred nezakonitimi ali škodljivimi namernimi ali nenamernimi aktivnostmi s strani posameznikov.

Namen te politike je:

- Zagotoviti, da vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, tretje osebe in ostali delavci (uporabniki) razumejo njihove odgovornosti in so primerni za vloge, ki so jim namenjene, ter za zmanjšanje tveganja kraje, prevare ali zlorabe zmogljivosti.
- Zagotoviti, da se uporabniki zavedajo groženj in skrbi, ki ogrožajo varnost informacij, njihovih odgovornosti in obveznosti in da so opremljeni za podporo politike varovanja informacij.
- Zagotoviti, da zaposleni, začasno zaposleni, pogodbeniki, tretje osebe in ostali delavci, zapustijo podjetje ali zamenjajo zaposlitev na urejen način.

2. OBSEG

Politika velja za vse uporabnike informacijskih dobrin Mariborskega vodovoda.

Politika se nanaša tudi na vso opremo, ki je v lasti oz. najemu s strani Mariborskega vodovoda.

3. POJMI

- **Informacijska dobrina:** opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema, poljuben nosilec informacij...)
- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, tretje osebe in ostali delavci.
- **Lastnik:** je posameznik (uporabnik), kateremu je vodstvo odobrilo odgovornost za uporabo, nadzorovanje, razvoj, vzdrževanje in varovanje informacijske dobrine. Izraz "lastnik" ne pomeni, da ima ta oseba dejanske lastniške pravice v zvezi z tem informacijskim virom.
- **Pooblaščen oseba:** strokovni sodelavec sektorja informatike, zunanji sodelavec,...

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA ČLOVEŠKIH VIROV	
	Oznaka: VP 03-01	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 3/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4. POLITIKA

4.1. Pred zaposlitvijo

Vsak uporabnik informacijske tehnologije v podjetju mora biti seznanjen z varnostnimi politikami informacijske varnosti glede na naravo dela, ob dodelitvi oz. prvi uporabi informacijskega vira (email, osebni računalnik, pametni telefon...)

- Vsak zaposleni podpiše izjavo o seznanjenosti kot jo opredeljuje Politika primerne rabe.
- Poslovni partnerji (dobavitelji) podpišejo pogodbeno zavezo kot jo opredeljuje Politika odnosa z dobavitelji (VP 11-01 Odnosi z dobavitelji)

4.2. Med zaposlitvijo

Vodstvo podjetja zahteva, da zaposleni uporabniki izvajajo varovanje v skladu z določenimi varnostnimi politikami in pravilniki podjetja.

Vsi uporabniki informacijske tehnologije, kjer je to primerno, se udeležijo ustreznega usposabljanja za seznanjanje in se redno obveščajo o posodobitvah v postopkih in politikah podjetja, ki zadevajo njihovo delovno mesto. Varnostne politike so vedno dosegljive na intranetu podjetja.

Uporabnikom je v skladu z ostalimi politikami omejeno omogočena zasebna raba informacijskih virov, kot so: omejena raba interneta, omejena raba elektronske pošte, omejen zasebni prostor na disku osebnega računalnika.

Mariborski vodovod ima uradni disciplinski postopek za zaposlene, ki kršijo politike varovanja informacij – »Pravilnik o odgovornostih zaposlenih za kršitve pogodbenih obveznosti iz delovnega razmerja«.

4.3. Prekinitev ali sprememba zaposlitve

Uporabniki po koncu zaposlitve, pogodbe ali sporazuma vrnejo vsa sredstva podjetja, ki so jih imeli v uporabi.

Odgovornost vsakega uporabnika ob prekinitvi je, da sam odstrani podatke iz zasebne rabe (mapa »ZASEBNO«). Podjetje ne odgovarja za razkritje neodstranjenih podatkov iz zasebne rabe.

Uporabnikom se ob prekinitvi zaposlitve, pogodbe ali sporazuma odvzamejo vse pravice do dostopa do informacijskih virov (dostop do informacij, zmogljivosti za obdelavo informacij,...)

V primeru spremembe zaposlitve, pogodbe ali sporazuma, se pravice do dostopa informacijskih virov ustrezno prilagodijo.

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA ČLOVEŠKIH VIROV	
	Oznaka: VP 03-01	Datum izdaje: 15.6.2018
	Verzija: 2	Stran: 4/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

5. UVELJAVLJANJE POLITIKE

Vsi zaposleni in drugi uporabniki informacijske tehnologije Mariborskega vodovoda so odgovorni za izvajanje določil te politike. Vsak zaposleni, ki ugotovi kršitev te politike, je dolžan o tem obvestiti svojega nadrejenega ali vodstvo sektorja za informatiko oz. tehnično pomoč uporabnikom (Help desk), telefonska številka **int. 261** ali na elektronski naslov **it.podpora@mb-vodovod.si**.

Če zaposleni krši določila te politike ali nepravilno uporablja informacijsko tehnologijo, bo njegovo ravnanje podvrženo ukrepom, ki lahko vodijo tudi do prenehanja delovnega razmerja.

Tretje osebe, ki kršijo to politiko, so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

- Uporabljena nadzorstva ISO/IEC 27001-2013 poglavja:
 - A.7.1 Pred zaposlovanjem
 - A.7.2 Med zaposlovanjem
 - A.7.3 Prekinitev ali sprememba zaposlitve
 - A.9.2.6 Preklic ali prekinitev dostopa

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VP_04_03_Človeški Viri	VP_03_01_CloveskiViri.doc	Pripravil: Bojan Erker
2	2019-12	Dodane spr.		Uredil: Bojan Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA PRIMERNE RABE INFORMACIJSKE TEHNOLOGIJE	
	Oznaka: VP 03-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 1/9
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1 Splošna raba in lastništvo informacij	2
4.2 Varnost	3
4.3 Nesprejemljiva raba	3
4.4 Aktivnosti, ki so brez izjeme strogo prepovedane	3
4.5 Namestitvev in zaščita opreme	5
4.6 Oskrba z energijo	5
4.7 Varovanje kabelskih vodov	5
4.8 Vzdrževanje opreme	5
4.9 Varovanje opreme zunaj prostorov Mariborskega vodovoda	6
4.10 Varno uničenje ali ponovna uporaba opreme	6
4.11 Zasebna raba	6
4.12 Nadzor	7
5. UVELJAVLJANJE POLITIKE	7
6. REFERENCE	7
7. ZGODOVINA	8
8. PRILOGA	9

	VARNOSTNA POLITIKA	
	POLITIKA PRIMERNE RABE INFORMACIJSKE TEHNOLOGIJE	
	Oznaka: VP 03-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 2/9
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Ena temeljnih obvez Mariborskega vodovoda je varovati zaposlene in podjetje pred nezakonitimi ali škodljivimi namernimi ali nenamernimi aktivnostmi s strani posameznikov. Informacijska infrastruktura in vsi sistemi, povezani vanjo (zlasti računalniška strojna oprema, aplikativna in systemska programska oprema, komunikacijska oprema in podatkovne zbirke), so last Mariborskega vodovoda in omogočajo njegovo delovanje.

Za zagotavljanje učinkovitega varovanja informacij in podatkov, ki se nahajajo v omenjenih sistemih in v povezanih podatkovnih zbirkah, je pomembno sodelovanje in podpora vseh zaposlenih v podjetju, ter povezanih oseb, ki delajo s tovrstnimi informacijami in podatki oz. z informacijskimi sistemi. Odgovornost vsakega uporabnika je, da se seznani s smernicami, določenimi s to politiko in v skladu z njimi tudi ravna.

Namen te politike je opredelitev primerne rabe računalniške in druge informacijske tehnologije v Mariborskem vodovodu. Politika je oblikovana predvsem z namenom zaščite zaposlenih ter podjetja, v katerem delajo.

Neustrezna uporaba računalniške in druge informacijske tehnologije izpostavlja podjetje in njene zaposlene tveganjem, kot so okužbe informacijske tehnologije z zlonamerno kodo (npr. virusi), ki lahko ogrožajo delovanja sistemov in storitev, zlorabijo informacije in podatke shranjene v informacijskem sistemu.

2. OBSEG

Politika velja za vse uporabnike informacijskega sistema, ali njegovih delov Mariborskega vodovoda.

Politika se nanaša na vsa informacijska dobrine, ki je v lasti oz. najemu s strani Mariborskega vodovoda.

3. POJMI

- **Informacijska dobrina:** opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema,...)
- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, tretje osebe in ostali delavci.
- **Pooblaščen oseb:** strokovni sodelavec sektorja informatike, zunanji sodelavec,...

4. POLITIKA

4.1 Splošna raba in lastništvo informacij

Vsi podatki, ki se ustvarijo na informacijski opremi in sistemih podjetja, so v lasti Mariborskega vodovoda. Pooblaščen osebe podjetja lahko z namenom zagotavljanja varnosti in upravljanja omrežja, kadarkoli izvajajo nadzor nad opremo, sistemi in pretokom podatkov, z omejitvami, določenimi v tej politiki, ter v politiki uporabe interneta in elektronske

	VARNOSTNA POLITIKA	
	POLITIKA PRIMERNE RABE INFORMACIJSKE TEHNOLOGIJE	
	Oznaka: VP 03-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 3/9
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

pošte Mariborskega vodovoda, ki se nanašata na nadzor nad elektronsko pošto in nad uporabo interneta.

Zaposleni odgovarjajo za razumno in primerno rabo informacijskih sredstev za zasebne namene. Takšna uporaba informacijskih sredstev za zasebne namene se jim omeji v primerih, ko bi lahko bila zaradi tega ogrožena varnost informacijskega sistema, ali ko bi bile zaradi tega kakorkoli ogrožene pravice ostalih zaposlenih ali delovni proces.

4.2 Varnost

Zaposleni morajo izvajati vse potrebne ukrepe za preprečevanje nepooblaščenega dostopa do zaupnih informacij in osebnih podatkov.

Gesla morajo biti varovana pred nepooblaščenno uporabo, uporabniških računov za uporabo računalnikov oz. za dostop do informacijskih sistemov pa ni dovoljeno deliti z ostalimi zaposlenimi. Uporabniki so odgovorni za varovanje svojih gesel in uporabniških računov.

Režim uporabe sistemskih in uporabniških gesel z namenom preprečitve možnosti nepooblaščenega vstopa v sistem in zlorabe gesla, je določen v politiki uporabe gesel.

Osební, prenosni računalniki in delovne postaje so varovani z geslom na ravni operacijskega sistema in z geslom na ravni posamezne aplikacije.

Izmenljivi nosilci podatkov morajo biti ustrezno označeni in varovani glede na stopnjo zaupnosti shranjenih informacij oz. podatkov.

Vsa strojna in programska oprema, ki je v uporabi v podjetju, mora biti zaščitena s kvalitetno in redno vzdrževano zaščito pred zlonamerno kodo, za katero poskrbijo s sektorju za informatiko.

Ob izločitvi iz uporabe morajo biti vsi nosilci podatkov, vključno s papirno dokumentacijo, na ustrezen način uničeni, tako da so podatki nečitljivi (anonimizirani, blokirani ali izbrisani).

Zaposleni morajo s strojno, programsko, komunikacijsko in drugo povezano informacijsko opremo, ravnati pazljivo in jo, kolikor je v njihovi moči, tudi redno vzdrževati (npr. brisanje prahu, čiščenje zaslona, zaščita pred poškodbami, ipd.). Za vsa ostala zahtevnejša vzdrževalna dela je v podjetju zadolžena strokovna oseba iz Sektorja za informatiko. Tej so zaposleni dolžni sporočiti vsako poškodbo, napako ali drugo nepravilnost, ki so jo odkrili pri delovanju opreme.

4.3 Nesprejemljiva raba

Nesprejemljiva raba informacijske opreme v Mariborskem vodovodu pomeni vse aktivnosti, ki so navedene v nadaljevanju te politike in vse ostale, ki bi povzročale enake ali podobne učinke in s katerimi bi bila informacijski opremi, zaposlenim ali ustanovi povzročena kakršnakoli materialna ali nematerialna škoda ali bi bila zaradi njih kakorkoli ogrožena varnost zaposlenih.

V nobenem primeru zaposleni nimajo pooblastil za izvajanje nezakonitih dejanj, medtem ko uporabljajo informacijsko opremo podjetja.

4.4 Aktivnosti, ki so brez izjeme strogo prepovedane

- Priklučevanje v računalniško omrežje in/ ali spreminjanje konfiguracije računalniške opreme brez odobritve vodje sektorja za informatiko;

	VARNOSTNA POLITIKA	
	POLITIKA PRIMERNE RABE INFORMACIJSKE TEHNOLOGIJE	
	Oznaka: VP 03-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 4/9
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- Kopiranje, shranjevanje in odnašanje podatkov na kakršnemkoli nosilcu podatkov izven prostorov podjetja ali kopiranje na spletna mesta (oblaki: dropbox, google drive...), brez predhodnega dovoljenja neposredno nadrejenega ali odgovorne osebe v Sektorju za informatiko. Ta prepoved ne velja za kopiranje, shranjevanje in odnašanje podatkov v sklopu izvajanja delovnih nalog in dolžnosti zaposlenih;
- Kršitev pravic katerekoli osebe ali podjetja (avtorskih pravic, pravic industrijske lastnine, poslovne skrivnosti, ipd.) vključno in ne izključno z nameščanjem ali razpečevanjem nelegalnih kopij programske opreme;
- Nepooblaščen kopiranje in razpečevanje avtorskih del, vključujoč digitalizacijo fotografij iz revij, knjig in ostalih virov ter nameščanje katerekoli avtorsko zaščitene programske opreme, za katero Mariborski vodovod nima ustrezne licence;
- Izvoz programske opreme, tehničnih informacij, šifrirnih metod ali tehnologije v druge države v nasprotju z mednarodno ali nacionalno zakonodajo
- Nameščanje ali posredovanje škodljive programske opreme v omrežje, na računalnike ali strežnike (npr. virusov, trojanskih konjev, črvov, e-poštnih bomb, ipd.);
- Razkritje gesla uporabniškega računa ali omogočanje uporabe lastnega uporabniškega računa drugim osebam (vključno sodelavcem, družinskim članom in drugim osebam, ko se delo opravlja na domu);
- Uporaba informacijskih sredstev za aktivno udeležbo pri pridobivanju in razširjanju materiala, ki pomeni spolno nadlegovanje ali nadlegovanje na delovnem mestu, kot to določa nacionalna zakonodaja;
- Razširjanje goljufivih ponudb za blago in storitve prek informacijskega sistema podjetja;
- Izvajanje vdorov ali motenje omrežnih komunikacij;
- Skeniranje komunikacijskih vrat ali zaščit;
- Izvajanje kakršnegakoli nadzora, ki prestreza pakete podatkov, ki niso namenjeni uporabnikovi napravi. Pri tem je izzet nadzor po službeni dolžnosti;
- Izogibanje ugotavljanju istovetnosti (avtentifikaciji) ali drugim varnostnim mehanizmom na kateremkoli strežniku, omrežju ali uporabniškemu računu;
- Motenje ali onemogočanje storitev kateremukoli uporabniku (napad z onemogočanjem storitve);
- Uporaba službenih tiskalnikov za zasebne namene;
- Nepooblaščen uporaba licenčne programske opreme za zasebne namene (zaradi določil licenčne pogodbe);
- Uporaba katerihkoli programov, ukaznih datotek, ukazov ali pošiljanje sporočil kakršnekoli vrste z namenom motenja ali onemogočanja uporabniških sej na kakršenkoli način;
- Posredovanje osebnih podatkov ali drugih podatkov in informacij o zaposlenih, strankah tretjim osebam, ki niso uporabniki (pooblaščenici), skladno z ZVOP;
- Pošiljanje ali posredovanje neželene elektronske pošte ali reklamnega materiala, verižnih e-sporočil ali piramidnih oz. podobnih shem kakršnekoli vrste;
- Vse oblike nadlegovanja po elektronski pošti, telefonu ali osebnem klicu, bodisi z besedami, prepogostostjo ali velikostjo sporočil;
- Nepooblaščen uporaba ali ponarejanje glave elektronske pošte;
- Uporaba samodejnega posredovanja vse prejete elektronske pošte na drug elektronski naslov izven domene Mariborskega vodovoda.

Uporaba intraneta in map v skupni rabi

	VARNOSTNA POLITIKA	
	POLITIKA PRIMERNE RABE INFORMACIJSKE TEHNOLOGIJE	
	Oznaka: VP 03-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 5/9
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Intranetni portal je namenjen internemu dostopu do informacij in aplikacij v podjetju. Zaradi zasnove odjemalec - strežnik s centralno bazo podatkov omogoča centralizacijo poslovno potrebnih informacij v podjetju, olajša objavo le-teh ter skrajša čas iskanja in dostopa do podatkov.

Zaposleni in drugi, s strani Mariborskega vodovoda pooblaščen uporabniki, uporabljajo intranet in mape v skupni rabi zaradi učinkovitejšega opravljanja delovnih obveznosti in zaradi seznanjanja z novostmi in usmeritvami podjetja.

Vsak uporabnik, ki mu je omogočen dostop do intraneta in skupnih map informacijskega sistema podjetja je dolžan sistem uporabljati skladno s pravili te politike in tako, da s svojo uporabo ne posega v pravice drugih uporabnikov ali ne ogroža varnosti informacijskega sistema podjetja.

Uporabniške pravice za dostop do intraneta in skupnih map informacijskega sistema dodelijo pooblaščen osebe v sektorju informatike.

4.5 Namestitev in zaščita opreme

Opremo je potrebno zaščititi in namestiti tako, da je zmanjšano tveganje pred naravnimi in drugimi nesrečami ter da so zmanjšane možnosti nepooblaščenega dostopa. Pri tem je potrebno upoštevati naslednje postopke in kontrole:

- oprema naj bo glede na potrebno stopnjo varovanja nameščena v ustrezna varovana območja;
- oprema z informacijami, ki so klasificirane s stopnjo zaupnosti »zaupno« ali višje, naj bo nameščena tako, da se prepreči nepooblaščen vpogled;
- oprema, ki zahteva posebno varovanje, naj bo ločena od preostale, da tako optimiziramo skupno raven zahtevane zaščite;
- namestiti je potrebno kontrole, za zmanjšanje nevarnosti pred možnimi grožnjami (npr. kraja, ogenj, eksplozija, dim, voda...);

4.6 Oskrba z energijo

Občutljiva oprema je zaščitena pred prekinitvami električnega toka in pred drugimi motnjami v oskrbi z energijo. V kolikor so določene vtičnice varovane, se posebej označijo z drugo barvo. V te zaščitene vtičnice je strogo prepovedano priklapljati ostale ne-informacijske porabnike.

4.7 Varovanje kabelskih vodov

Električne in telekomunikacijske vode, ki prenašajo podatke ali podpirajo informacijske storitve, je potrebno zaščititi pred prestrezanjem ali poškodbami.

4.8 Vzdrževanje opreme

Opremo je potrebno pravilno vzdrževati za zagotavljanje njene stalne razpoložljivosti in celovitosti. Pri tem je potrebno upoštevati naslednje postopke in kontrole:

- popravila in vzdrževanje opreme izvajajo izključno za to pooblaščen vzdrževalci;

	VARNOSTNA POLITIKA	
	POLITIKA PRIMERNE RABE INFORMACIJSKE TEHNOLOGIJE	
	Oznaka: VP 03-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 6/9
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- b) vzdrževanje opreme se vselej izvaja v skladu s priporočili proizvajalca (pogostost in način vzdrževanja);
- c) po vnaprej predpisanem in jasno določenem postopku je potrebno zabeležiti vsako opažanje, sum ali dejansko okvaro opreme ter vsa popravila ali preventivna vzdrževalna dela;
- d) če se vzdrževalna dela na opremi izvajajo zunaj organizacije, je potrebno poskrbeti za ustrezne kontrole;
- e) izpolnjene morajo biti vse zahteve, ki jih določajo zavarovalne police.

Za vzdrževanje opreme se obrnite na podporo uporabnikom »IT podpora« interni tel. 261 ali na elektronski naslov it.podpora@mb-vodovod.si !

4.9 Varovanje opreme zunaj prostorov Mariborskega vodovoda

Ne glede na lastništvo mora vodstvo sektorja za informatiko dati dovoljenje za uporabo opreme zunaj prostorov podjetja. S to opremo morajo uporabniki ravnati v skladu s pravili, določenimi v tej in ostalih politikah. Pri varovanju opreme zunaj prostorov podjetja je potrebno upoštevati naslednja priporočila:

- a) oprema ne sme biti nenadzorovana v javnih prostorih;
- b) potrebno je upoštevati proizvajalčeva navodila;
- c) potrebno je upoštevati navodila sektorja za informatiko;
- d) tudi za delo na domu je potrebno za opremo uvesti ustrezno varovanje;

Pri določanju najprimernejših kontrol je potrebno upoštevati, da se lahko ogroženost (npr. poškodbe, kraja, prisluškovanje, ipd.) precej razlikuje od kraja do kraja.

4.10 Varno uničenje ali ponovna uporaba opreme

Informacije lahko ogrozi tudi namerno uničenje ali ponovna uporaba opreme. Namesto običajnega izbrisa podatkov je treba nosilce podatkov, ki vsebujejo občutljive informacije fizično uničiti ali varnostno prepisati. Trde diske, je potrebno pred odstranitvijo pregledati, da so bili vsi občutljivi podatki in licenčna programska oprema odstranjeni ali prepisani, za kar poskrbi sektor za informatiko. Za poškodovane nosilce podatkov, ki vsebujejo občutljive podatke, sektor za informatiko in organizacijo oceni, ali naj bodo uničeni ali popravljeni. Za uničevanje papirne dokumentacije z občutljivimi podatki so na voljo rezalniki.

4.11 Zasebna raba

Uporabniki lahko informacijsko tehnologijo ob pogojih, ki jih določa ta in z njo povezane politike ter drugi interni predpisi Mariborskega vodovoda, v omejenem obsegu uporabljajo tudi v zasebne namene (brskanje po spletnih straneh, prejemanje in pošiljanje zasebnih elektronskih sporočil), vendar le v kolikor to ne ogroža delovnega procesa ali informacijske infrastrukture, ter v kolikor ne posega v pravice ostalih uporabnikov oz. zaposlenih. Za shranjevanje zasebnih podatkov si uporabnik uredi mapo "ZASEBNO". Količina vsebine imenika ne sme presegati 4GB podatkov. Uporabnik je dolžan zasebne datoteke (elektronska

	VARNOSTNA POLITIKA	
	POLITIKA PRIMERNE RABE INFORMACIJSKE TEHNOLOGIJE	
	Oznaka: VP 03-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 7/9
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

sporočila, dokumenti, slike,...) hraniti izključno znotraj te mape. Podjetje se zavezuje, da bo spoštovalo zasebnost uporabnika izključno znotraj te mape.

4.12 Nadzor

Mariborski vodovod nadzoruje izvajanje te politike, pri čemer je nadzor namenjen predvsem ugotavljanju varnostnih lukenj in pomanjkljivosti informacijskega in povezanih sistemov. Nadzor nad delom z informacijsko tehnologijo v podjetju je omejen na nadzor uporabe ter delovanja računalnikov in druge informacijske opreme (npr. pravilno rokovanje z opremo, vzdrževanje, ipd.).

V izjemnih primerih, skladno z določili te politike in politik o uporabi interneta in elektronske pošte se v Mariborskem vodovodu po predhodnem pisnem obvestilu zaposlenih, lahko nadzira elektronsko pošto in uporabo interneta zaposlenih, ki ju ti uporabljajo za izpolnjevanje delovnih nalog (oz. v druge službene namene) ter pregleduje vsebino datotek v datotečnih sistemih lokalnih računalnikov in strežnikov s katerimi delajo zaposleni.

Mariborski vodovod ima pravico pregledovati vsebino računalnikov in druge strojne opreme uporabnikov, ki je del informacijskega sistema podjetja, vendar le v kolikor s tem ščiti svoje imetje, poslovne interese, rezultate poslovanja, načrte ter vse podatke, ki iz navedenega izvirajo. Pred tem je podjetje dolžno zagotoviti vse potrebne ukrepe, ki v skladu z načelom sorazmernosti v najmanjši možni meri posegajo v zasebnost uporabnikov informacijskega sistema podjetja.

Mariborski vodovod se zavezuje, da bo pri nadzoru nad uporabo sredstev informacijske tehnologije upoštevala načela sorazmernosti, zakonitosti in ustavne dopustnosti.

Če posamezni uporabnik, ne upošteva priporočil zasebne rabe in svoje zasebne datoteke hrani v informacijskem sistemu podjetja, bodo le- te obravnavane kot službene in bodo lahko podvržene pregledu s strani podjetja v primerih in pod pogoji, določenimi v tem poglavju

5. UVELJAVLJANJE POLITIKE

Vsi zaposleni in drugi uporabniki informacijske tehnologije Mariborskega vodovoda so odgovorni za izvajanje določil te politike. Vsak zaposleni, ki ugotovi kršitev te politike, je dolžan o tem obvestiti svojega nadrejenega ali vodstvo sektorja za informatiko oz. pomoč uporabnikom, telefonska številka **int. 261** ali na elektronski naslov **it.podpora@mb-vodovod.si**.

Če zaposleni krši določila te politike ali nepravilno uporablja informacijsko tehnologijo, bo njegovo ravnanje podvrženo ukrepom, ki lahko vodijo tudi do prenehanja delovnega razmerja.

Tretje osebe, ki kršijo to politiko, so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

- Uporabljena nadzorstva ISO/IEC 27001 poglavja: A.7.1.2, A.7.2.2, A.8.1.2, A.8.1.3, A.8.2.3, A.8.3, A.11.2

	VARNOSTNA POLITIKA	
	POLITIKA PRIMERNE RABE INFORMACIJSKE TEHNOLOGIJE	
	Oznaka: VP 03-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 8/9
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- Nadzor in zasebnost v informacijski družni, Matej Kovačič, FDV 2006, poglavje: Zasebnost na delovnem mestu.
- Priloga 1- Izjava delavca o seznanjenosti s politikami informacijske varnosti

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1		Osnutek		Pripravi:
2	Apr.2018	Dodane spr.	Zamenja politiko VP_03-01_Primerna raba	Uredil: Bojan Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	VARNOSTNA POLITIKA	
	POLITIKA PRIMERNE RABE INFORMACIJSKE TEHNOLOGIJE	
	Oznaka: VP 03-02	Datum izdaje: 16.6.2018
	Verzija: 2	Stran: 9/9
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

8. PRILOGA

Izjava delavca o seznanjenosti s politikami informacijske varnosti

Če imate dodatna vprašanja v zvezi z Politiko varovanja človeških virov, Politiko primerne rabe informacijske tehnologije, Politiko uporabe elektronske pošte, Politiko uporabe interneta, Politiko uporabe gesel, jih naslovite na vodstvo sektorja za informatiko, preden podpišete naslednjo izjavo:

Spodaj podpisani izjavljam, da sem seznanjen z določili politik informacijske varnosti:

- Politika varovanja človeških virov,
- Politika primerne rabe informacijske tehnologije,
- Politika uporabe elektronske pošte,
- Politika uporabe interneta,
- Politika uporabe gesel.

in z njimi v celoti soglašam. Izjavljam, da razumem, da kršitev teh določil lahko vodi do disciplinskih postopkov ali do prenehanja delovnega razmerja.

ime uporabnika

podpis uporabnika

datum

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12. 2019	

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA DOBRIN	
	Oznaka: VP 04-01	Datum izdaje: 15.05.2018
	Verzija: 1	Stran: 1/8
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1 Seznami dobrin	2
4.2 Odgovornost za vzdrževanje seznamov	3
4.3 Redni pregledi seznamov	3
4.4 Lastništvo informacij	4
4.5 Lastništvo izpeljanih informacij	4
4.6 Odgovornosti, ki izhajajo iz lastništva informacij in dobrin	4
4.7 Sprejemljiva uporaba informacij in sredstev	5
4.8 Pravice uporabnikov	6
4.9 Razvrstitev informacij	6
5. UVELJAVLJANJE POLITIKE	6
6. REFERENCE	7
7. ZGODOVINA	7

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA DOBRIN	
	Oznaka: VP 04-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/8
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Namen politike je jasno prepoznati vse informacijske dobrine, ter sestaviti in vzdrževati sezname teh dobrin. Vsem informacijam in dobrinam (povezanim z zmogljivostmi za obdelavo informacij) je dodeljeno lastništvo določenega dela organizacije podjetja.

2. OBSEG

S to politiko so seznanjeni in so jo dolžni spoštovati vsi zaposleni podjetja Mariborski vodovod in ostali uporabniki dobrin. Odgovornosti posameznih uporabnikov so zapisane v posameznih poglavjih.

3. POJMI

- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, dobavitelji in ostali delavci.
- **Dobavitelji** – pravne in fizične osebe, ki sodelujejo z Mariborskim vodovodom in imajo dostop do IT dobrin
- **Poslovni lastnik:** je posameznik (uporabnik), ki mu je vodstvo odobrilo uporabo informacijske dobrine. Izraz ne pomeni, da ima ta oseba dejansko lastniško pravico nad tem sredstvom.
- **Informacijska dobrina:** opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, komunikacijska oprema, programska oprema, podatkovna baza, podatki, evidence, registri, listine,...)

4. POLITIKA

4.1 Seznami dobrin

Seznam dobrin in lastništvo dobrin je izrednega pomena pri zagotavljanju učinkovite varnosti in s tem povezane odgovornosti, ki mora biti za vsako dobrino jasno določena.

Mariborski vodovod ima vzpostavljen sistem fizičnih osnovnih sredstev. Vzpostavil bo tudi evidence podatkovnih dobrin, ki so povezani s procesiranjem informacij in jih opredeljeni s dokumentov v prilogi (predvsem poslovno lastništvo podatkov- primarni viri). Posebej označi podatke, ki imajo lastnosti osebnih podatkov.

V primeru, ko seznam dobrin vsebuje več tipov dobrin, mora vsaka dobrina v evidenci nositi oznako tipa dobrine vsebinsko in smiselno skladno z osnovno delitvijo dobrin. Po potrebi se posamezen tip dobrine razdeli še na podtipе dobrin.

Vsaka dobrina v posameznem seznamu dobrin mora biti opredeljena s trajno enoličnim identifikatorjem, ki ne sme opredeliti nobenega druge dobrine, tudi po prenehanju uporabe prve dobrine.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA DOBRIN	
	Oznaka: VP 04-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/8
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Pri opredeljevanju relacije dobrine do druge dobrin, različne po tipu, ki se nahaja v drugem seznamu dobrin, mora za ključ biti uporabljen trajno enolični identifikator druge dobrine.

Informacije o obstoju in naravi pomembnih dobrin podjetja morajo biti dostopne po načelu najmanjših pravic.

4.2 Odgovornost za vzdrževanje seznamov

Odgovornost za vzdrževanje posameznega seznama dobrin ali njegovega dela je razvidna iz dokumenta: »Seznam dobrin IT«.

Odgovorne osebe za vzdrževanje seznamov, izhajajoč iz zapisanih odgovornosti iz dokumenta: »Seznam dobrin IT«, so odgovorne, da vsi sezname dobrin **zavedeni** odražajo dejansko stanje in da so usklajeni z obstoječimi evidencami.

V primeru, da evidenca dobrin z isto vsebino ali delom vsebine zaradi različnih potreb obstaja v več seznamih, je odgovorna oseba dolžna poskrbeti za usklajenost teh seznamov.

V primeru, ko za seznam ni mogoče določiti enega nosilca odgovornosti, je za seznam odgovornih več oseb **ali organizacijskih enot**, vsaka za tisti del seznama, ki se nanaša na njen delokrog – **poslovni proces**.

4.3 Redni pregledi seznamov

Odgovorne osebe za vzdrževanje seznamov dobrin so dolžne redno, najmanj enkrat letno izvesti pregled seznama in uskladiti odstopanja v seznamu.

Lastnik informacije je odgovoren za redno pregledovanje in vzdrževanje razvrstitve informacij. Najmanj enkrat letno je potrebno pregledati razvrstitev informacij, da bi ugotovili, ali je potrebno spremeniti razvrstitev informacije ali jo izločiti iz razvrstitve.

Pregled lastnika informacij obsega:

- skladnost seznama dobrin s stanjem dobrin,
- ustreznost razvrstitve dobrin,
- ustreznost ravni dostopa.

V primeru ugotovljenih razlik med seznamom in dejanskim stanjem mora lastnik informacije potrditi novo stanje seznama dobrin, ter drugih virov informacij.

V primeru potrebne spremembe razvrstitve informacije, mora lastnik informacije spremembo razvrstitve potrditi.

V povezavi s tem mora lastnik informacije v nadaljevanju tudi pregledati dodeljene dostope do informacijskih dobrin, ter drugih virov informacij.

Odgovorne osebe za vzdrževanje seznamov dobrin morajo skrbeti za ažurnost seznamov.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA DOBRIN	
	Oznaka: VP 04-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/8
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.4 Lastništvo informacij

Lastnik dobrine je zaposleni, ki mu je dodeljena vloga lastništva nad dobrino in je razviden iz seznamov dobrin, praviloma je to oseba iz kroga lastnikov informacij, ki so povezani s temi dobrinami.

Lastnik informacije nosi odgovornost za informacije, uporabo z informacijami povezanih dobrin, izvajanje poslovnih procesov ter podaja zahteve za varovanje informacij.

Lastnik informacij in dobrin se praviloma določi na vlogo, ki jo opravlja v delovnem procesu in se poimensko zapiše.

V primeru, da je lastnikov neke dobrine več, lastništvo prevzame prvi skupni nadrejeni – vodja službe, oddelka v organizacijski strukturi.

Lastnik informacije je dolžan pisno sporočiti odgovorni osebi za vzdrževanje seznama dobrin – informatiku: nastanek, spremembo ali ukinitve vira.

4.5 Lastništvo izpeljanih informacij

Odgovorna oseba B, ki je odgovorna, da ustvari novo informacijo iz izvornih informacij, ki so v lastništvu odgovorne osebe A, je hkrati odgovorna za vse, kar je s to novo informacijo povezano:

- informacija bo imela pojavno obliko informacijske dobrine (ID) in odgovorna oseba B bo kot taka lastnik ID,
- ker je oseba B odgovorna, da ustvari informacijo v obliki ID, je kot lastnik odgovorna za vse dobrine, s katerimi jo ustvari, torej je odgovorna, da definira modul/aplikacijo, in je lastnik te aplikacije oz modula.

Pogoj, da to lahko naredi, je dostop do izvornih informacij. Če te niso v njegovem lastništvu, mora zato pridobiti pooblaščen dostop, ki ga odobri oseba A - lastnik izvornih informacij. Torej za informacije, ki so rezultat procesiranja (vmesnikov, poročil, poizvedb, izpisov in obdelav) velja:

- lastnik A izvornih informacij, ki so potrebne za procesiranje, je odgovoren za odobritev dostopa (tj. uporabe) do potrebnih podatkov (ki so pojavna oblika informacij),
- lastnik B pa je odgovoren za definicijo dobrin procesiranja (vmesnikov, poročil, poizvedb, izpisov in obdelav), in je kot tak lastnik teh dobrin in informacij v pojavni obliki informacijskih dobrin, ki jih te dobrine ustvarijo.

4.6 Odgovornosti, ki izhajajo iz lastništva informacij in dobrin

Lastnik informacij je odgovoren:

- za razvrstitev informacij,
- za ustrezno razvrstitev informacij tako, da so vsi, ki jih potrebujejo iz naslova opravljanja poslovnih dolžnosti, z razvrstitvijo tudi seznanjeni,

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA DOBRIN	
	Oznaka: VP 04-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 5/8
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- za opredelitev ravni dostopa do informacij in posredovanja informacij na podlagi razvrstitve informacij,
- za redno pregledovanje in vzdrževanje razvrstitve informacij,
- da so vse informacije pravilno in jasno označene,
- za omejitev dostopa in posredovanja informacij, skladno s »Politiko obvladovanja dostopov do sistemov« in podrejenimi pravilniki in navodili,
- za opredelitev varnostnih zahtev, s katerimi so zagotovljene zaupnost, razpoložljivost in celovitost informacije,
- za odobritev postopka za ravnanje z razvrščenimi informacijami.

Lastnik dobrin je odgovoren:

- da so dobrine, ki so povezane s procesiranjem informacij, razvrščene,
- da definira varnostne zahteve, ki izhajajo iz razvrstitve informacij in se nanašajo na uporabo dobrin, povezanih s procesiranjem informacij,
- za uveljavitev sprejemljive uporabe dobrin, ki so povezane s procesiranjem informacij, in da opredeli zahteve za vpeljavo sprejemljive rabe in varovanje informacije skrbniku,
- za preverjanje sprejemljive uporabe dobrin uporabnikov,
- za periodični pregled vsebinske ustreznosti, ažurnosti dobrine v skladu s področnimi pravilniki in drugimi dokumenti.

Skrbnik informacij in dobrin je odgovoren:

- za izvedbo označitve informacij,
- za opredelitev in dokumentiranje postopkov za ravnanje z razvrščenimi informacijami,
- za izvajanje varnostnih kontrol skladno z varnostnimi zahtevami lastnika informacije,
- za vpeljavo v skladu s področnimi pravilniki upravljanja sprememb in dokumentiranje sprejemljive uporabe dobrin v skladu z zahtevami lastnika informacije.

Uporabnik je odgovoren:

- za ravnanje z informacijami in dobrinami v skladu z opredelitvijo sprejemljive rabe dobrin,
- za pregledovanje, popravljanje in spreminjanje vsebine informacijske dobrin skladno z dodeljenimi pooblastili.

Vsi uporabniki so odgovorni za ravnanje z informacijami v skladu s predpisanimi postopki za ravnanje z razvrščenimi informacijami, ki so opredeljena v »Pravilniku o varovanju poslovne skrivnosti«.

V kolikor se podatki in informacije nanašajo na t.i. Osebnne podatke so vsi od lastnika, skrbnika do uporabni dolžni upoštevati navodila skladno s pravilnikom »**Pravilnik o varovanju osebnih podatkov**«.

4.7 Sprejemljiva uporaba informacij in sredstev

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA DOBRIN	
	Oznaka: VP 04-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 6/8
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Z informacijami in sredstvi je potrebno ravnati skladno z navodili proizvajalca ali dobavitelja oziroma internimi dokumenti podjetja. Posebne poslovne zahteve za posamezno rabo sredstev, morajo biti opredeljene v zahtevah lastnika in dokumentirane v navodilih za sprejemljivo rabo sredstev za potrebe podjetja.

Opreduje: *VP 03-02 Politika primerne rabe informacijske tehnologije*

Vsi, ki pri svojem delu prihajajo v stik s osebnimi podatki morajo biti pisno seznanjeni s vlogo in odgovornostjo skladno s s pravilnikom »**Pravilnik o varovanju osebnih podatkov**«.

4.8 Pravice uporabnikov

Uporabniki imajo pravico vedeti naravo vseh nevarnosti, s katerimi se lahko soočijo na delovnem mestu. Posebej so seznanjeni s tveganji pri delu s **osebnimi podatki**!

Vodstvo mora informirati uporabnike o obstoju nevarnosti, zagotoviti zaščite za zmanjšanje tveganj in za pravilno uporabo varnostnih mehanizmov.

Nekateri ukrepi za zmanjševanje tveganj so opisani v ostalih politikah:

- *Politika čiste mize in čistega zaslona*
- *Politika oddaljenega dostopa*
- *Politika mobilnih naprav*

4.9 Razvrstitev informacij

Lastnik informacije mora razvrstiti informacijo glede na njeno vrednost, zakonske zahteve, občutljivost in pomembnost za podjetje, ter s tem določiti njeno zaupnost.

Podjetje opredeljuje zaupnost informacij z vidika poslovne skrivnosti (klasifikacija), ki je opredeljena v »Pravilniku o varovanju poslovne skrivnosti«.

Za informacije, ki so zaupne in strogo zaupne narave, je potrebno opredeliti obdobje hranjenja ne glede na pojavno obliko, v kateri obstajajo. Informacije po pretečenem roku hranjenja je potrebno izločiti iz uporabe. V kolikor gre za informacijo v dokumentarnem gradivu, je potrebno upoštevati »Pravilnik o arhiviranju«.

5. UVELJAVLJANJE POLITIKE

Vsak uporabnik, ki ugotovi kršitev te politike, je dolžan o tem obvestiti vodstvo Sektorja informacijske tehnologije oz. tehnično pomoč uporabnikom int.tel.št. 261 ali na elektronski naslov it.podpora@mb-vodovod.si.

Ravnanje ob sumu razkritja informacij so opredeljena v Pravilniku o varovanju poslovne skrivnosti.

Če uporabnik krši določila te politike, bo njegovo ravnanje podvrženo ukrepom po Zakonu o delovnih razmerjih, ki lahko vodijo tudi do prenehanja delovnega razmerja.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA DOBRIN	
	Oznaka: VP 04-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 7/8
Datum zadnje revizije: 02.12.2019		Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

6. REFERENCE

- Uporabljeni nadzorstva ISO/IEC 27001-2013:
 - A.7.1.1 Popis sredstev
 - A.7.1.2 Lastništvo sredstev
 - A.7.1.3 Sprejemljiva uporaba sredstev
 - A.7.2.2 Ozaveščenost...
 - A.8.1 Odgovornost za dobrine (vse točke)
 - A.8.2 Razvrstitev informacij
- Politika je v soodvisnosti z politikami:
 - VP 03-01 Primerna raba informacijske tehnologije
 - VP 07-02 Politika čiste mize in čistega zaslona
 - VP 02-01 Politika mobilnih naprav
 - VP 02-02 Politika dela na daljavo naprav
 -
- Politika se navezuje na pravilnike:
 - Pravilnik o varovanju poslovne skrivnosti (klasifikacija informacij)
 - Pravilnik o arhiviranju

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	apr.2018	Sprejeto	VP_04_01_Upravljanje dobrin	Nova: vpeljuje lastništvo, odgovornost do osebnih podatkov
2	12-2019	Dodane spr.		Uredil: Bojan Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA DOBRIN	
	Oznaka: VP 04-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 8/8
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

	<i>Ime</i>	<i>Podpis</i>
<i>Direktor:</i>	Danilo Burnač	
<i>Sprejet na Forumu varovanja informacij, dne:</i>	3.12.2015	

	VARNOSTNA POLITIKA	
	POLITIKA NADZORA DOSTOPA	
	Oznaka: VP 05-01	Datum izdaje: 16.06.2018
	Verzija: 2	Stran: 1/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	3
4.1. Poslovne zahteve za dostop do informacijskih dobrin	3
4.2. Upravljanje uporabniških dostopov	3
4.3. Odgovornost uporabnikov	4
4.4. Nadzor dostopa do omrežja	4
4.5. Nadzor dostopa do operacijskega sistema	4
4.6. Nadzor dostopa do uporabniških aplikacij in informacij	5
4.7. Spremljanje uporabe in dostopa do sistema	5
5. UVELJAVLJANJE POLITIKE	6
6. REFERENCE	7
7. ZGODOVINA	7

	VARNOSTNA POLITIKA	
	POLITIKA NADZORA DOSTOPA	
	Oznaka: VP 05-01	Datum izdaje: 16.06.2018
	Verzija: 2	Stran: 2/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Namen vsebine politike obvladovanja dostopa do sistemov je zagotavljanje pravil za dodeljevanje in nadzor nad pravicami za dostop do vseh vrst informacijskih virov, ne glede na lokacijo, bodisi v Mariborskem vodovodu ali pri delu na daljavo, nadzor nad izvajanjem pravil, zaznavanje in beleženje varnostnih dogodkov ter odgovornosti vseh uporabnikov (tako zunanjih kot notranjih), katerim se podeljuje nadzorovan dostop do informacijskega sistema. Nadzor nad dostopom predstavlja nadzorstva, tako organizacijske postopke, kot uporabo primerne strojne in programske opreme, ki z ustrezno uvedbo in uporabo zmanjšujejo tveganja povezana z nepooblaščenim in nezakonitim dostopom do informacijskih virov in neposredno iz tega izhajajočih tveganj možnega ogrožanja razpoložljivosti (nepooblaščen zaustavitev sistema), celovitosti (nepooblaščen transakcija) in zaupnosti informacij (nepooblaščen dostop in kraja informacij).

Podjetje uporablja vsa razpoložljiva sredstva, da zagotavlja primerne postopke in infrastrukturo za nemoteno in varno poslovanje.

Vsi uporabniki informacijskega sistema morajo upoštevati in izvajati politiko obvladovanja dostopa. Do informacijskega sistema Mariborskega vodovoda imajo dostop samo pooblaščen uporabniki, obenem pa se zagotavljajo vsa potrebna nadzorstva.

2. OBSEG

Politika obsega vse informacijske vire na nivoju omrežja, operacijskih sistemov, podatkov v podatkovnih bazah in vse raznovrstne poslovne aplikativne rešitve ter druge medije in nosilce informacij. Obsega vse uporabnike, ki so v stiku z navedenimi sredstvi ter vse pogodbene delavce in izvajalce storitev za potrebe Mariborskega vodovoda, ki imajo pooblaščen dostop. Velja za zaposlene, ki so zadolženi za vzpostavitev in vzdrževanje informacijske varnosti, na nivoju vodstva, uporabnikov in ponudnikov storitve – skrbnikov sistemov.

Politika zajema obvladovanje novih nevarnosti, možnosti obrambe, poslovnih zahtev in izkušenj iz neljubih dogodkov (incidentov).

3. POJMI

- **Informacijski vir:** opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema,...)
- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, tretje osebe in ostali delavci.
- **Pooblaščen oseba:** strokovni sodelavec sektorja informatike, zunanji sodelavec, dobavitelj

	VARNOSTNA POLITIKA	
	POLITIKA NADZORA DOSTOPA	
	Oznaka: VP 05-01	Datum izdaje: 16.06.2018
	Verzija: 2	Stran: 3/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4. POLITIKA

4.1. Poslovne zahteve za dostop do informacijskih dobrin

Mariborski vodovod ima dokumentirana pravila za dodeljevanje dostopa:

Vse uporabniške poslovne aplikacije in ostali viri namenjeni uporabnikom morajo imeti izdelana in dokumentirana pravila za upravljanje dostopa. Pripravlja jih sektor za informatiko. Pravila morajo opredeljevati:

- kriterije za nivo pravic dostopa na podlagi poslovnih zahtev, za posameznega uporabnika ali skupino uporabnikov. Uporabniku se določi nivo pravic le do tistih informacij in informacijskih virov, ki jih potrebuje pri svojem delu v podjetju, po načelu najmanj dovoljenega («Need to know»).
- definirajo se varnostne zahteve pri uporabi posamezne poslovne aplikacije, kdo mora biti seznanjen z navedenimi postopki in pravili,
- odgovornost za odobritev dostopa in dodeljevanje pravic, ter odgovornost za administracijo in izvajanje dostopov,
- definirajo se skupine v katere se združuje uporabnike, ki opravljajo istovrstno delo. Če aplikacija neposredno ne omogoča kreiranja skupin v samem sistemu, je potrebno definirati v dokumentu pravila za dodeljevanje dostopa, tipe uporabnikov in njim ustrezne nastavitve v sistemu.

4.2. Upravljanje uporabniških dostopov

Registracija uporabnika – Mariborski vodovod ima izdelan formalen postopek za registracijo uporabnika (obrazec), ki vsebuje vsaj naslednje:

- postopke za dodelitev, ukinitve in spremembo dostopa,
- preverjanje ali ima uporabnik odobritev od lastnika storitve,
- preverjanje ali je dodeljen nivo pravic primeren za poslovne potrebe in skladen z varnostno politiko,
- določajo okoliščine v katerih se lahko uporabniku odvzame pravica dostopa,
- določajo način vzdrževanja seznama uporabnikov,
- seznanijo uporabnika o dodeljenem dostopu, uporabniki pa morajo s podpisom potrditi odgovornosti in pogoje dostopa.

Vsi uporabniki morajo imeti v okviru enega sistema ali aplikacije unikatno uporabniško ime, iz katerega ga lahko povežemo z njegovimi dejanji ter zanje zahtevamo odgovornost. Upravljanje z navedenimi postopki mora v čim večji meri potekati centralizirano.

Neposredni vodja in kadrovska služba sta dolžna takoj ob vsakem prihodu, odhodu ali prerazporeditvi delavca, obvestiti sektor za informatiko, ki je zadolžen za administracijo uporabnikov. Neposredni vodja mora podati zahtevek za ažuriranje uporabnika. Pravice dostopa ažurirajo zadolženi administratorji izključno po prejemu (obrazca **registracija_novega_it_uporabnika.doc**) zahtevka s strani neposrednega vodje.

Mariborski vodovod zagotavlja trajno hranjenje podatkov povezanih z dodeljevanjem pravic posamezniku do informacijskih virov in informacij.

	VARNOSTNA POLITIKA	
	POLITIKA NADZORA DOSTOPA	
	Oznaka: VP 05-01	Datum izdaje: 16.06.2018
	Verzija: 2	Stran: 4/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Izvaja se redno preverjanje uporabniških imen, z namenom odkrivanja in odstranjevanja zastarelih ali odvečnih imen. Začasni računi morajo biti onemogočeni ali ukinjeni, če niso v uporabi.

Predhodno dodeljeno uporabniško ime ne sme biti ponovno dodeljena drugemu uporabniku.

Upravljanje uporabniških dostopov s posebno pravico. Poleg formalnih postopkov, ki veljajo za registracijo uporabnika, se upošteva še naslednje:

- opredeljena mora biti omejena uporaba dostopov s posebno pravico,
- uporabniki naj imajo za opravila, kjer so potrebne posebne pravice, ločene uporabniške račune, za običajno delo, pa naj uporabljajo običajne uporabniške račune,
- Iz uporabniškega imena ne sme biti razvidno, da gre za uporabnika s posebnimi pravicami,
- zagotovljena mora biti sledljivost uporabe posebnih pravic,
- Vzpostavljeni morajo biti postopki, za vzpostavitev dostopa s posebnimi pravicami v primeru nedosegljivosti uporabnika s posebnimi pravicami.

Predvideva se usposobljenost dodatnih delavcev in varno shranjevanje sistemskih gesel.

Pregled uporabniških pravic dostopa. Mariborski vodovod ima vpeljan postopek rednega pregledovanja uporabniških pravic dostopa do informacijskih virov. Pregledi se izvajajo redno na določen interval (letno) in neposredno ob spremembi pravic. Za uporabnike s posebnimi pravicami, se pregledi izvajajo pogosteje (polletno).

4.3. Odgovornost uporabnikov

Pri preprečevanju nepooblaščenega dostopa je ključnega pomena opredelitev odgovornosti in zavedanje uporabnikov informacijskih virov zlasti pri ustrezni uporabi gesel in varovanju uporabniške opreme. Sprejemamo dve osnovni nadzorstvi:

Uporaba gesel, ki je podrobneje opredeljena v *VP 05-02 Politiki uporabe gesel*. Varno uporabo opreme dodatno opisuje *VP 03-02 Politika primerne rabe informacijske tehnologije*.

4.4. Nadzor dostopa do omrežja

Opredeljuje in opisuje *VP 09-01 Politika varnosti komunikacij*.

4.5. Nadzor dostopa do operacijskega sistema

Je omejen le na pooblaščen uporabnike delovne postaje in druge strojne opreme in omogoča prepoznavanje (enoličen identifikator) in preverjanje identitete (sistem gesel), po potrebi tudi lokacije, vsakega pooblaščenega uporabnika.

	VARNOSTNA POLITIKA	
	POLITIKA NADZORA DOSTOPA	
	Oznaka: VP 05-01	Datum izdaje: 16.06.2018
	Verzija: 2	Stran: 5/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.6. Nadzor dostopa do uporabniških aplikacij in informacij

Cilj je preprečiti nepooblaščen dostop do podatkov, ki se nahajajo v aplikativnih sistemih. S tem namenom je zagotovljeno:

- Omejevanje dostopa do podatkov
 - Dostop do občutljivih podatkov je uporabnikom omejen po obsegu dostopa in pravici dostopa (npr. samo za branje ne pa tudi spreminjanje).
 - Vzpostavljen je postopek za obvladovanje dostopa do podatkovnih baz.
 - Omejen je dostop do podatkovnih baz, če jih uporabniki pri svojem delu ne potrebujejo.
 - Uporabniki imajo dostop le do omejenega dela podatkovne baze z omejenimi pravicami (npr. samo za branje)
 - Vpeljana je programska oprema, za nadzor in zaščito pred tiskanjem, kopiranjem in pošiljanjem različnih občutljivih dokumentov.
- Uporaba sistemskih podpornih programov
 - Dostop in uporaba sistemskih programov je omejena in varovana.
 - Ločeni so podporni programi od uporabniških in omejen je dostop in uporabo sistemskih programov na majhno število pooblaščenih uporabnikov.
 - Beležiti se uporaba sistemskih programov in kjer ni potrebna je odstranjena iz delovnih postaj.
- Dostop in osamitev občutljivih sistemov
 - Lastniki aplikacije ali podatkov določijo in dokumentirajo njeno občutljivost, kar nato zahteva posebno obravnavo.
 - Praviloma se za take sisteme zahteva posebno ločeno računalniško okolje, po potrebi tudi na ločenem omrežju, z omogočenim dostopom samo iz v sistemu definiranih delovnih postaj in z ustrezno varnim fizičnim dostopom.

4.7. Spremljanje uporabe in dostopa do sistema

Mariborski vodovod spremlja dostop do sistemov in njihovo uporabo z namenom zagotavljanja, da uporabniki izvajajo samo tiste dejavnosti, za katere imajo izrecno pooblastilo, da zagotovi skladno ravnanje s politiko dostopa, da z beleženjem varnostnih dogodkov zagotavlja dokazno gradivo v primeru varnostnega incidenta. Nivo beleženja varnostnih dogodkov je sorazmeren z občutljivostjo sistema in faktorji tveganja, kateri so: kritičnost aplikacije ali sistema, vrednost (aplikacije, podatkov, obsega posla,...), občutljivost, kritičnost vpletenih informacij, pretekle izkušnje z vdori in zlorabo sistema, razširjenost sistema.

Na informacijskih virih je implementirano beleženje varnostnih dogodkov – revizijskih sledi. Podatke o varnostnih dogodkih hrani na varnem mestu vsaj eno leto (druga lokacija, ognjevarne omare, ipd.)

Zabeležen dogodek vsebuje vsaj naslednje podatke:

- Uporabniško ime (User ID)
- Datum in čas dogodka

	VARNOSTNA POLITIKA	
	POLITIKA NADZORA DOSTOPA	
	Oznaka: VP 05-01	Datum izdaje: 16.06.2018
	Verzija: 2	Stran: 6/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- Lokacijo oziroma identifikacijo delovne postaje
- Vrsto uspešnega ali neuspešnega dogodka

Varnostni dogodki, ki jih beleži sistem so:

- Uspešna / neuspešna prijava v sistem
- Pooblaščen dostop do občutljivih datotek:
 - Beleži se vrsta dogodka.
 - Ime datoteke.
- Privilegirane operacije, kot so:
 - Uporaba računov s posebno pravico (administrator/operate)
 - Zagon in ustavitev sistema
 - Priklop/odklop vhodno izhodne naprave
- Poskusi nepooblaščenega dostopa, kot so:
 - Neuspešni poskusi
 - Kršitve politike dostopa in opozorilna sporočila mrežnih prehodov in požarne pregrade
 - Opozorila sistemov za zaznavanje vdorov
- Sistemska opozorila ali okvare, kot so:
 - Konzolna sporočila ali opozorila
 - Izjeme v dnevniku delovanja sistema
 - Alarmi pri upravljanju delovanja omrežja

Zabeležene varnostne dogodke se redno pregledujejo. Za pregledovanje dogodkov se uporablja namenska orodja in samodejne sisteme, ki pripomorejo k učinkovitemu prepoznavanju varnostno zanimivih dogodkov in možnostjo prepisovanja le teh v drugo bazo dogodkov.

Uvedena so nadzorstva, ki preprečujejo ali močno omejujejo možnost nepravilnega delovanja naprav in sistemov za beleženje varnostnih dogodkov. Mehanizmi ščitijo pred:

- izključitvijo naprave za beleženje,
- namerno spremembo vrste zabeleženega dogodka,
- spreminjanjem in brisanjem dnevniških datotek,
- prenapolnjenostjo nosilcev ali datotečnih sistemov z zapisi varnostnih dogodkov.

Za zagotovitev popolnosti in natančnosti dnevnikov za potrebe revizije in v primeru preiskav, je zagotovljeno pravilna sinhronizacija računalniških ur.

Pravila v tem poglavju, se smiselno uporabijo tudi pri dostopih do testnih, razvojnih in arhivskih informacijskih sistemov.

5. UVELJAVLJANJE POLITIKE

Direktor in vodje sektorjev morajo skrbeti, da delavci, ki so pod njihovim nadzorom, upoštevajo varnostne mehanizme navedene v tej politiki.

	VARNOSTNA POLITIKA	
	POLITIKA NADZORA DOSTOPA	
	Oznaka: VP 05-01	Datum izdaje: 16.06.2018
	Verzija: 2	Stran: 7/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Odgovornost vseh zaposlenih in drugih pooblaščenih izvajalcev je, da se ravna skladno s politikami opisanimi v 4. točki tega dokumenta. Pooblaščen uporabnik so dolžni o incidentih, sumu, da gre za nepooblaščen dostop do informacijskih virov in morebitnih zlorabah nemudoma poročati svojim vodjem, le ti pa sektorju za informatiko.

6. REFERENCE

- ISO/IEC 27001- 2013 poglavja:

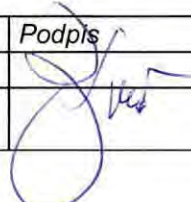
A.9.1.1 Politika nadzora dostopa
 A.9.1.2 Dostop do omrežij in omrežnih storitev
 A.9.2 Upravljanje uporabniškega dostopa
 A.9.3 Odgovornost uporabnikov
 A.9.4 Nadzor dostopa do aplikacij in informacij
 A.12.4.3 Beleženje aktivnosti administratorjev in operaterjev

- Politika se sklicuje tudi na:

VP_05_02 Politika uporabe gesel
 VP 03-02 Politika primerne rabe informacijske tehnologije.
 VP 09-01 Politika varnosti komunikacij

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VP_07_02_po litika obvladovanja DostopaDoSi stemov	VP_05_01_NadzorDostop a.docx	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Bojan Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE GESEL	
	Oznaka: VP 05-02	Datum izdaje: 15.05.2018
	Verzija: 2	Stran: 1/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1. Dodeljevanje uporabniških gesel	2
4.2. Uporaba gesla	3
4.3. Izbira uporabniških gesel	3
4.4. Skrbniška gesla	4
4.5. Postopek upravljanja z gesli	4
5. ODGOVORNOSTI	5
6. UVELJAVLJANJE POLITIKE	5
7. REFERENCE	6
8. ZGODOVINA	6

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE GESEL	
	Oznaka: VP 05-02	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 2/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Uporaba in ravnanje z gesli za dostop do informacijskega sistema je eden ključnih dejavnikov informacijske varnosti.

Namen te politike je določitev pravil za dodeljevanje in uporabo gesel za dostop do vseh vrst informacijskih dobrin, z namenom, da se prepreči možnost nepooblaščenega vstopa v sistem in zlorabe gesla.

Neustrezna sestava in uporaba gesla izpostavlja Mariborski vodovod in njegove zaposlene in druge uporabnike tveganjem, kot so nepooblaščen vdor in zloraba informacij in podatkov, shranjenih v informacijskem sistemu.

2. OBSEG

Politika obsega vse informacijske dobrine na nivoju omrežja, operacijskih sistemov, podatkov v podatkovnih bazah in vse raznovrstne poslovne aplikativne rešitve.

Obvezuje vse zaposlene, pogodbenike, svetovalce, začasno zaposlene in vse ostale delavce podjetja (v nadaljevanju: uporabniki).

3. POJMI

- **Informacijske dobrine:** opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema,...)
- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, tretje osebe in ostali delavci.

4. POLITIKA

Geslo je nabor znakov, ki ga mora poznati samo uporabnik in ne sme biti nikjer zapisano. Pomnjenje nabora znakov temelji na osnovi logičnega pomena gesla. Bolj je nabor znakov logičen, smiseln in povezan z nekim dejstvom, lažje si ga je zapomniti in s tem tudi lažje ugotoviti. Zato moramo poznati priporočila glede izbire gesla in jih upoštevati skupaj s podporo operacijskega sistema.

Najboljše geslo je nabor znakov, ki je vsem razen uporabniku nesmiseln in dovolj dolg zato, da je naključno ugotavljanje praktično nemogoče. Za uporabnika pa mora biti istočasno ta nabor znakov zelo smiseln in dovolj enostaven za pomnjenje. Takšnega idealnega gesla ni in zato nastanek gesla temelji na izvirnosti uporabnika in njemu lastnih asociacij.

4.1. Dodeljevanje uporabniških gesel

Uporabniška gesla so običajni in velikokrat edini način preverjanja identitete uporabnikov. Zaradi pomembnosti, dodeljevanje gesel opredeljuje formalni postopek:

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE GESEL	
	Oznaka: VP 05-02	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 3/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- Uporabniki gesel se s sprejemom gesla zavezujejo, da bodo osebna gesla obravnavali zaupno.
- Pooblaščen oseba, ki dodeljuje gesla, jih mora obravnavati zaupno in jih ne sme razkrivati nepooblaščenim osebam.
- Uporabniku začetna (inicialna) gesla izda skrbnik informacijskega sistema (domena). Začetna gesla morajo biti začasna in jih morajo uporabniki spremeniti takoj ob prvi prijavi.
- Uporabnikom, ki so pozabili svoje geslo, je mogoče izdati začetno geslo, potem ko se izvede pozitivna identifikacija uporabnika.
- Zahteva se varna izdaja začetnih gesel, potrebno se je izogibati vključevanju tretje stranke.
- Uporabnik ima možnost zavarovati geslo pred izgubo tako, da ga hrani v zaprti kuverti trezorja sektorja. To je priporočljivo za "ekskluzivna gesla", katerih ponovna izdaja ni enostavno mogoča.

4.2. Uporaba gesla

Zaposleni morajo izvajati vse potrebne ukrepe za preprečevanje nepooblaščenega dostopa do zaupnih informacij in osebnih podatkov. Za ravnanje z gesli veljajo sledeča pravila in odgovornosti:

- Uporabniki morajo skrbeti, da ostane njim dodeljeno geslo zaupno, svoje osebno geslo ne smejo zaupati nikomur, geslo pa se obravnava kot zaupna informacija.
- Ni dovoljeno razkrivanje gesel z namenom nadomeščanja odsotnih delavcev. Delavcu, ki nekoga nadomešča, mora njegov nadrejeni vodja zagotoviti dostop s potrebnimi pooblastili.
- Uporabniki naj upoštevajo pravila za ravnanje z gesli, ki jih predpisuje posamezna uporabniška aplikacija ali sistem.
- Če sistem sam ne omogoča samodejnega uveljavljanja pravil za ravnanje z gesli, morajo biti uporabniki še posebej pozorni in morajo upoštevati **pravila izbire uporabniških gesel**, glede gesla (menjava, dolžina, oblika,...).
- Uporabniki morajo redno menjavati gesla, pri tem se izogibajo ponovni uporabi ali kroženju starih gesel.
- Ob prvi prijavi obvezno zamenjajo začetno geslo, kjer je to mogoče.
- Uporabniki ne souporabljajo osebnih uporabniških gesel.
- Uporabniki ne zapisujejo gesel, posebej ne, na nevarovana mesta.
- Uporabniki ne omenjajo gesla v prisotnosti drugih oseb in ga ne prenašajo ga preko telefona;
- Uporabniki ne uporabljajo istega gesla za službene potrebe in za osebne račune, kot so osebni elektronski poštni predali na javnih ponudnikih Siol, Yahoo, Hotmail, drugi osebni računi v spletu, kot npr. eBay, Amazon.

V primeru razkritja ali suma razkritja gesla, mora uporabnik takoj spremeniti geslo. V primeru, da to ni možno, mora o tem obvestiti **IT podpora** uporabnikom na **int. tel. 261** ali elektronski naslov it.podpora@mb-vodovod.si.

4.3. Izbira uporabniških gesel

Pravila pri sestavi gesla:

- Geslo mora biti sestavljeno iz vsaj 8 znakov,
- Različno velike črke abecede,

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE GESEL	
	Oznaka: VP 05-02	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 4/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- Številke in ločila ter druge znake (0-9, !«#\$%&'()*=+/, ipd),
- Geslo, ki si ga boste zapomnili in ga ne bo potrebno zapisati
- Geslo, ki ga boste lahko hitro natipkali, kar bo otežilo prepoznavo gesla osebe, ki vas bo opazovala.

Priporočila, ki jih je potrebno upoštevati pri izbiri gesel:

- Pri sestavi gesla ne smemo uporabljati:
 - Izpeljank iz uporabniškega imena (npr. pisano od zadaj naprej, podvojeno, male in velike črke...).
 - Logičnih števil (telefonska številka, registrska tablica, rojstni datum...).
 - Nizi znakov, kot so: aaabbb, qwerty, zyxwvuts, 123321,...
 - Samostojnih besed (preproste besede, vulgarne besede, fraze, predmete iz vidnega polja ali pa besedne asociacije z uporabnikom).
 - Vaše ime ali priimek.
 - Imena članov družine.
 - Rojstnih datumov
 - Številke kreditnih kartic, modela in znamke vašega avtomobila, naslova bivališča in podobne osebne informacije, ki jih je mogoče izvedeti,
 - Vse enake številke ali črke,
 - Besede, ki se nahajajo v domačih ali tujih jezikovnih slovarjih.
- Zamisliti si je potrebno logično zaporedje, ki temelji na lastni izkušnji in samo nam nekaj pomeni,
- Uporabljati se sme združevanje besed, ki jih v normalnem pogovornem jeziku nikoli ne povežemo.

4.4. Skrbniška gesla

Skrbniška gesla (administratorji) zahtevajo strožjo obravnavo, kot je kompleksnejša sestava, pogostejša menjava in omejen dostop. To vključuje vsa skrbniška gesla na mrežnih napravah, usmerjevalnikih, stikalih, požarnih pregradah, strežnikih, operacijskih sistemih, podatkovnih bazah in drugih dobrinah, ki:

- morajo biti dolga vsaj 10 znakov,
- morajo vsebovati velike in male črke,
- morajo vsebovati posebne znake,
- morajo vsebovati vsaj 2 številke.

4.5. Postopek upravljanja z gesli

Zagotovljen mora biti postopek upravljanja z gesli. Prednost dajemo avtomatiziranim sistemom, ki samodejno uveljavljajo pravila za ravnanje z gesli. Kjer sistemi tega ne omogočajo samodejno, veljajo v čim večji meri enaka pravila, ki so dokumentirana in se izvajajo ročno s strani uporabnika.

Od sistema pričakujemo sledeče lastnosti:

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE GESEL	
	Oznaka: VP 05-02	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 5/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- Kjer je primerno, dopušča uporabnikom, da sami izbirajo in spreminjajo svoja gesla in vključuje postopek potrditve izbranega gesla, kar dovoljuje napake pri vnosu podatkov.
- Uveljavlja izbiro kakovostnih gesel, tako da sistem preverja, ali izbrano geslo ustreza izbranim varnostnim standardom opisanih v splošnih priporočilih. V primeru neustrezne izbire gesla, sistem opozori uporabnika in prepreči izbiro slabega gesla.
- Uveljavlja spreminjanje gesel, kjer uporabniki vzdržujejo lastna gesla, kot je opisano v splošnih pravilih.
- Kjer uporabniki sami izbirajo gesla, jih sistem prisili, da ob prvi prijavi zamenjajo začetno geslo.
- Začetno geslo ima omejen rok veljavnosti, če ni uporabljeno v določenem času, poteče in ne deluje.
- Vzdržuje zapise starih uporabniških gesel, npr. za 12 mesecev nazaj ali za določeno število gesel, da preprečuje ponovno uporabo starih gesel.
- Ob vpisu gesla ne izpiše gesla na zaslon.
- Shranjuje datoteko z gesli ločeno od podatkov v aplikacijskem sistemu.
- Shranjuje gesla v šifrirani obliki z uporabo enosmernega šifrirnega algoritma.
- Po namestitvi kupljene programske opreme, zahteva spremembo privzetih gesel prodajalca sistema.
- Vsa sistemska gesla produkcijskih sistemov morajo biti vpisana v centralni register sistemskih gesel, ki je deponiran v trezorju.

5. ODGOVORNOSTI

Direktor, vodje sektorjev in oddelkov morajo skrbeti, da delavci, ki so pod njihovim nadzorom, upoštevajo varnostne mehanizme navedene v tej politiki.

Sektor za informatiko skrbi za implementacijo in izvajanje politike gesel na informacijskih sistemih v njegovem skrbništvu, torej s tehničnimi sredstvi ter s sodelovanjem s končnimi uporabniki, (preko "IT podpore" in napotki za uporabo in ravnanje z gesli za posamezne sisteme).

Odgovornost vseh zaposlenih in drugih pooblaščenih izvajalcev je, da se ravna skladno s politikami opisanimi v 4. točki tega dokumenta. Pooblaščen uporabnik so dolžni o incidentih, sumu, da gre za nepooblaščen dostop do informacijskih dobrin in morebitnih zlorabah nemudoma poročati svojim vodjem in/ali sektorju za informatiko.

6. UVELJAVLJANJE POLITIKE

Vsi zaposleni in drugi uporabniki informacijske tehnologije Mariborskega vodovoda so odgovorni za izvajanje določil te politike.

Vsak zaposleni, ki ugotovi kršitev te politike, je dolžan o tem obvestiti sektor za informatiko Mariborskega vodovoda.

Če zaposleni krši določila te politike glede varovanja gesel, bo njegovo ravnanje predmet disciplinskih postopkov, ki lahko vodijo tudi do prenehanja delovnega razmerja.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE GESEL	
	Oznaka: VP 05-02	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 6/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

7. REFERENCE

Uporabljena nadzorstva ISO/IEC 27001-2013:

- A.9.2 Upravljanje uporabniških dostopov – vse kontrole
- A.9.3 Odgovornost uporabnikov
- A.9.4.2 Varni postopki prijave
- A.9.4.3 Sistem upravljanja gesel

Pravilniki, navodila povezana s politiko: VP_05_01_Politika nadzora dostopa

8. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	Apr.2008	Nadomešča VP_07_01_P olitikaUporab eGesel	VP_05_02_PolitikaUporab eGesel.docx	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Bojan Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA KRIPTOGRAFIJE	
	Oznaka: VP 06-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 1/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **INTERNO**

Vsebina:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1 Podpora uporabnikom, ki potrebujejo mobilnost	2
4.2 Daljinski dostop	3
4.3 Splet	3
4.4 Elektronska pošta	3
4.5 Spletne storitve za stranke	3
4.6 Varnostne in arhivske kopije	3
4.7 Komunikacije med fizično ločenimi organizacijskimi enotami	4
5. UVELJAVLJANJE POLITIKE	4
6. REFERENCE	4
7. ZGODOVINA	5

	VARNOSTNA POLITIKA	
	POLITIKA KRIPTOGRAFIJE	
	Oznaka: VP 06-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **INTERNO**

1. NAMEN

Politika kriptografije določa, kdaj in kako uporabiti šifriranje. Vključuje zaščito občutljivih informacij in komunikacij, upravljanje s ključi in postopke za obnovitev šifriranih informacij kadar je to potrebno.

Cilj politike je ustrezna in učinkovita kriptografija za zaščito zaupnosti, verodostojnosti in/ali celovitosti informacij.

2. OBSEG

Politika je v prvi vrsti namenjena zaposlenim v Službi informatike.

3. POJMI

- **Kriptiranje:** postopek skrivanja oz. šifriranja informacij
- **E- poslovanje:** izvajanje poslovnih procesov preko interneta in tudi preko telefona
- **Poslovno občutljive informacije (podatki):** so vse informacije, ki niso označene kot javne. Gre za interne in zaupne informacije družbe ter **osebne podatke**.

4. POLITIKA

Mariborski vodovod d.d. vpeljuje tehnike šifriranja poslovno občutljivih podatkov in prenosnih poti sorazmerno z identificiranimi tveganji. Pri tem se poslužuje preverjenih in po možnosti odprtokodnih rešitev.

Za nameščanje ustreznih kriptografskih mehanizmov je zadolžen Službi informatike.

4.1 Podpora uporabnikom, ki potrebujejo mobilnost

Poslovno občutljive informacije v elektronski obliki je dovoljeno fizično odnašati izven prostorov družbe le v kolikor so ustrezno šifrirane (prenosniki, mobilni diski, USB ključi,...) .

Uporabniki so seznanjeni z rokovanjem takšnih dobrin v politiki s *VP 02-01 Politika mobilnih naprav* in *VP 02-02 Politika dela na daljavo*.

Zaposleni v Službi informatike nudijo uporabnikom ustrezno podporo.

	VARNOSTNA POLITIKA	
	POLITIKA KRIPTOGRAFIJE	
	Oznaka: VP 06-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **INTERNO**

4.2 Daljinski dostop

Daljinski dostop do informacijskega sistema (VPN) družbe je dovoljen le za to pooblaščenim uporabnikom:

- Upravljanje VPN dostopov je centralno nadzorovano.
- Avtentifikacija je dvonivojska, povezava pa šifrirana:
 1. nivo predstavlja avtentifikacija s časovno omejenim enkratnim geslom,
 2. nivo je lokalna prijava.
- V primeru odpovedi avtentifikacije na prvem nivoju imajo določeni privilegirani uporabniki možnost daljinskega dostopa s pred naloženim digitalnim potrdilom, ta povezava je asimetrično šifrirana.

Glej tudi *VP 02-02 Politika dela na daljavo, odsek 4.4 Nadzor oddaljenega dostopa*.

4.3 Splet

Uporabniki, ki se povezujejo v splet (shttp, sftp) in delijo poslovno zaupne informacije o družbi ali **osebne podatke**, počno to le preko šifriranih povezav.

- Z varno uporabo so uporabniki seznanjeni s politiko *VP 06-02 Politika varnega e-poslovanja* in s *Spiskom varnih povezav*, ki so priloga politike. Služba informatike skrbi za redno dopolnjevanje in osveževanja liste varnih povezav.
- Dostop do državnih institucij, agencij,... je podprt z uporabo digitalnih certifikatov in asimetričnega šifriranja.
- Služba informatike skrbi za varnostne kopije digitalnih certifikatov s privatnimi ključi..
- Za prenos datotek se uporablja varovani SFTP.

Zaposleni v službi informatike nudijo uporabnikom ustrezno podporo.

4.4 Elektronska pošta

Uporabnikom, ki zaradi zagotavljanja ustreznega izvajanja poslovnih procesov koristijo elektronsko pošto za pošiljanje poslovno občutljivih informacij, nudijo zaposleni v Službi informatike ustrezno podporo. Vsi zaposleni se lahko obrnejo po pomoč na prijavo napak (HelpDesk), po telefonu int 261, ali po elektronski pošti it.podpora@mb-vodovod.si.

Glej tudi *VP 09-04 Politika varnega E-poslovanja*.

4.5 Spletne storitve za stranke

Spletne storitve Mariborskega vodovoda www.mb-vodovod.si so informativnega značaja za stranke.

Avtentifikacija do spletnih storitev preko portala "komunala.info" in "Moja voda na dlani" za stranke je mogoča ob registraciji s uporabniškim imenom in geslom.

- Komunikacija je varovana preko https povezave – asimetrično kriptiranje.
- Storitve "Komunala.info" in "Moja voda na dlani" ima nameščena strežniška digitalna potrdila zaupanja vredne certifikatske agencije.

4.6 Varnostne in arhivske kopije

Vse varnostne kopije se avtomatsko šifrirajo s centralizirano programsko opremo za izvajanje varnostnih in arhivskih kopij. Glej tudi *VP 08-02 Varnostno kopiranje*.

	VARNOSTNA POLITIKA	
	POLITIKA KRIPTOGRAFIJE	
	Oznaka: VP 06-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **INTERNO**

4.7 Komunikacije med fizično ločenimi organizacijskimi enotami

Opredeljeno v VP 09-01 Politika varnosti komunikacij.

Mariborski vodovod se zaveda, da so eden najpomembnejših dejavnikov varnosti oziroma učinkovite uporabe šifriranja uporabniki, za to se zavezuje k trajnostnemu izobraževanju uporabnikov in dvigu njihove informacijsko-varnostne zavesti.

5. UVELJAVLJANJE POLITIKE

Vsi zaposleni in drugi uporabniki informacijske tehnologije Mariborskega vodovoda so odgovorni za izvajanje določil te politike.

Vsak zaposleni, ki ugotovi kršitev te politike, je dolžan o tem obvestiti Služba za informatiko Mariborskega vodovoda.

Če zaposleni krši določila te politike glede varovanja gesel, bo njegovo ravnanje predmet disciplinskih postopkov, ki lahko vodijo tudi do prenehanja delovnega razmerja.

6. REFERENCE

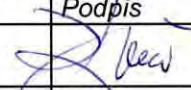
- ISO/IEC 27001 poglavja:
 - A.10 Kriptografske kontrole
 - A.10.1.1 Kriptografske kontrole
 - A.10.1.2 Upravljanje ključev
- Politika se sklicuje tudi na:
 - VP 06-02 Politika varnega E-poslovanja*
 - VP 02-02 Politika dela na daljavo*
 - VP 02-01 Politika mobilnih naprav*
 - VP 09-01 Politika varnosti komunikacij*
- Spisek varnih elektronskih povezav

	VARNOSTNA POLITIKA	
	POLITIKA KRIPTOGRAFIJE	
	Oznaka: VP 06-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 5/5
Datum zadnje revizije: 02.12.2019		Datum nove revizije: 2020

Klasifikacija: **INTERNO**

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	15.06.2018	Dodane spr.		Pripravil: Bojan Erker
2	12.2019	Dodane spr.		Uredil: Bojan Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2015	

	VARNOSTNA POLITIKA	
	POLITIKA FIZIČNEGA VAROVANJA	
	Oznaka: VP 07-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 1/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1. Varovana območja	2
4.2. Kontrole fizičnega dostopa	3
4.3. Varovanje opreme	4
5. UVELJAVLJANJE POLITIKE	6
6. REFERENCE	6
7. ZGODOVINA	6

	VARNOSTNA POLITIKA	
	POLITIKA FIZIČNEGA VAROVANJA	
	Oznaka: VP 07-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Sistemi za procesiranje in hranjenje kritičnih in občutljivih informacij se nahajajo v varnih okoljih, da se prepreči nepooblaščen fizični dostop, škoda ali motnja.

Namen vsebine politike fizične varnosti je zagotavljanje varnega okolja za podatke in informacijsko opremo, kar v grobem opredeljuje kontrolne mehanizme za vzpostavitev varnih območij, varovanja opreme in pravil za zaposlene.

2. OBSEG

Obsega vse prostore z "varnimi" območji, kjer se nahaja občutljiva oprema, dokumenti, podatki v elektronski, papirni ali kaki drugi obliki. Obsega vse uporabnike, ki so ali lahko pridejo v stik z navedenimi sredstvi.

3. POJMI

- **Informacijske dobrine:** opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema,...)
- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, tretje osebe in ostali delavci.
- **Podjetje:** Mariborski vodovod d.d.
- **Pooblaščen oseba:** strokovni sodelavec sektorja informatike, zunanji sodelavec,...

4. POLITIKA

4.1. Varovana območja

Varovano območje, je vsako območje, za katerega Mariborskega vodovoda glede na oceno tveganja meni, da potrebuje nadzor dostopa. Ta območja lahko vključujejo različna območja podjetja, obvezno pa vključujejo računalniški center. Sem sodijo tudi prostori, kjer se obravnavajo občutljivi podatki (ETZ) ali podatki o poslovanju s strankami in prostori v katerih se nahajajo nosilci podatkov in občutljiva strojna oprema. Vzpostavimo jih, da preprečimo nepooblaščen fizični dostop, škodo in motnje v poslovnih prostorih in podatkih. Prav tako varovana območja ščitijo občutljivo opremo in podatke pred nevarnostmi naravnih nesreč, požara, poplave, eksplozije in civilnih nemirov.

Zasnovi varovanih območij Mariborski vodovod posveča posebno pozornost in poleg vseh ostalih zahtev upošteva tudi:

- pogoje proizvajalca strojne opreme,
- lego sosednjih prostorov, zaradi možnih dodatnih prehodov v varovano območje,
- uporabo sosednjih prostorov zaradi možnih vplivov ali groženj, (plinske, vodne instalacije),
- oceno požarno varnostne ustreznosti na podlagi veljavnih predpisov in standardov,

	VARNOSTNA POLITIKA	
	POLITIKA FIZIČNEGA VAROVANJA	
	Oznaka: VP 07-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- ustreznost storitev elektroenergetike, vodovoda, telekomunikacij,
- skladnost z ostalimi zahtevami in veljavnimi standardi na področju varovanja.

Varovana območja lahko obsegajo celoto ali dele etaže, poslopja ali pisarniškega prostora. Varovana območja so določena v dokumentih: »**Navodila za izvajanje fizičnega varovanja premoženja družbe**» in »**Sklep o uvedbi videonadzora**«. Varovana območja, so ustrezno ograjena, za prehod se uporablja primerna zaščita pred nepooblaščenim dostopom. Varovana območja imajo ustrezno požarno zaščito.

Prostori v katerih poteka obdelava podatkov, so navzven nevtralni in ne nakazujejo svojega namena.

Nevarni in gorljivi materiali se ne hraniti neposredno v varovanih območjih, temveč na primerni oddaljenosti. Podporne funkcije in oprema, npr. kopirni stroji, telefaksi ter rezervna oprema in nosilci varnostnih kopij, praviloma niso nameščeni znotraj varovanega območja, s čemer smo se izognili zahtevam po dodatnih dostopih v varovano območje.

V varovana območja spadajo prostori za zajem, centralno procesiranje in hrambo informacij. To so:

- sistemski prostor - soba 109,
- sistemski prostor - replikacija,
- sprejemna pisarna,
- fizični arhiv v kleti.

4.2. Kontrole fizičnega dostopa

Dostop v varovano območje je opremljen z ustreznimi kontrolami dostopa - ključavnicami, ki varujejo pred nepooblaščenim vstopom ali vdorom. Ločimo naslednje skupine oseb, glede na potrebo po dostopu:

- Pooblaščen delavci, ki imajo reden dostop
- Vzdrževalci naprav, delavci podjetja in zunanji izvajalci, ki potrebujejo dostop občasno

Vzpostavljene kontrole:

- Upoštevajo se naslednje kontrole glede na stopnjo tveganja na varovanem območju skladno z »**Navodili za izvajanje fizičnega varovanja premoženja družbe**«.
- Za dostop se na vhodu varovanega območja uporabi ključavnica.
- Nameščeni so alarmni sistemi (senzor gibanja), video kamere in zagotovljena je prisotnost varnostne službe – samo zunaj.
- Vzpostavljen je pregleda nad pooblastili dostopa – sektor za informatiko.
- Urejen je postopek za vstop obiskovalcev: Ti morajo na vidnem mestu nositi priponko »obiskovalec« in v primeru dostopa v najstrožje varovana območja smejo vstopati le v spremstvu pooblaščenega delavca. Vsi obiskovalci morajo biti vpisani v dnevnik varnostne službe, s točno navedbo časa prihoda in odhoda.
- Zagotovljen je postopek za brezpogojni dostop v primeru izrednih razmer, npr. požar, izlitje vode.

	VARNOSTNA POLITIKA	
	POLITIKA FIZIČNEGA VAROVANJA	
	Oznaka: VP 07-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Z upoštevanjem navedenih kontrol so vzpostavljeni pogoji, ki ne omogočajo nenadzorovanega dela na varovanem območju.

4.3. Varovanje opreme

Splošno o opremi

Podatki in oprema na kateri se podatki nahajajo, so zaščiteni pred uničenjem zaradi izrednih dogodkov, kot so požar, poplava in drugo, oziroma so sprejeti ustrezni ukrepi (replikacija podatkov). Nivo zaščite je določen glede na vrednost podatkov in ocenjeno tveganje, da v izrednem dogodku lahko pride do izgube podatkov.

Medije z zaupnimi podatki, podatki in materiali zaupne ali velike vrednosti, hranimo v ustreznih ognjevarnih omarah. Dostop imata sodelavca sektorja za informatiko.

Za opremo je zagotovljeno varno okolje, pri tem se upošteva sledeče zahteve oziroma se glede na občutljivost opreme:

- Naprave, ki zahtevajo posebno zaščito, so ločene od drugih naprav, da so zmanjšani nepotrebni dostopi v ta delovna območja in da omejimo skupno varno območje.
- Vzpostavljeni so ukrepi, ki varujejo opremo pred vplivi iz okolja, kot so: ogenj, vdor vode in poplave, motnje v dobavi električne energije. Potrebno je upoštevati tudi možnost vpliva tovrstnih nesreč v sosednjih prostorih (npr. puščanje strehe), sosednji zgradbi ali na ulici (požar ali eksplozija).
- V neposredni bližini občutljivih naprav je prepovedano uživanje hrane in pijače ter kajenje.
- Požar: Pri načrtovanju prostorov, je bilo pri ustrezno usposobljenih institucijah naročena izdelavo požarne študije – Požarni načrt (Požarni red).
- Po potrebi je nameščen sistem javljanja požara. Za same prostore z občutljivo opremo služi dodatni sistem zgodnjega odkrivanja požara.
- Nameščeni pa so redno vzdrževani ročni gasilni aparati.
- Zaposleni so seznanjeni s postopki ravnanja v primeru požara.
- Klimatiziranje: V prostorih z občutljivo IT opremo, je zagotovljeno zadostno in redundantno klimatiziranje upoštevajoč zahteve proizvajalca IT opreme in dobavitelja klimatske naprave.
- Po potrebi so nameščeni javljalci izpusta vode.
- Podjetje ima vzpostavljene postopke za ukrepanje 24 ur dnevno ter zagotovljeno redno vzdrževanje.

Oskrba z energijo

Za občutljivo opremo, je zagotovljena ustrezna zaščita pred izpadom električnega napajanja in drugimi motnjami pri oskrbi z električno energijo, kot so različna nihanja, prenapetostne konice in atmosferski vplivi.

To zaščito zagotavljamo s sistemom brezprekinitvenega napajanja (UPS), ki se nahaja znotraj strežniških omar in posamične.

Sistemi, kjer je zahtevana možnost delovanja opreme tudi pri daljšem izpadu javnega omrežja, so po potrebi dodatno opremljeni z generatorje električne energije in z zadostno količino goriva.

Posebno pozornost posvečamo načrtovanju brezprekinitvenega napajanja, pri čemer se upoštevajo poslovne zahteve, predvidena poraba, neplanirana poraba in poraba ob predvideni širitvi sistema, da je zagotovljena ustrezna zmogljivost sistema.

	VARNOSTNA POLITIKA	
	POLITIKA FIZIČNEGA VAROVANJA	
	Oznaka: VP 07-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 5/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Pred vsako namestitvijo nove opreme, se preveri, da je zagotovljena ustrezna zmogljivost sistema brezprekinitvenega napajanja ter če je potrebno, zagotovijo potrebne zmogljivosti. Sistem brezprekinitvenega napajanja omogoča oddaljen nadzor in alarmiranje.

Odgovorni zaposleni so usposobljeni za ukrepanje ob izpadu, podjetje pa ima vzpostavljene postopke za ukrepanje 24 ur dnevno, z dežurstvi ali usposobljeno varnostno službo ter zagotovljeno redno vzdrževanje naprav, kar je opredeljeno v »Navodilih za izvajanje fizičnega varovanja premoženja družbe« in »Načrtom zaščite in reševanje oz. delovanja v primeru izrednih razmer in neskladnosti«.

Varovanje ožičenja

Za ožičenje, elektroenergetske in telekomunikacijske vode, ki prenašajo podatke ali zagotavljajo delovanje informacijskih storitev, je zagotovljena ustrezna zaščita pred mehanskimi poškodbami.

Ustrezno varnost ožičenja je potrebno načrtovana že ob vzpostavitvi računalniških prostorov, ob gradnji in prenovi objektov.

Izvedbo in načrtovanje ožičenja lahko izvaja ustrezno usposobljeno osebje, ob upoštevanju veljavnih standardov.

Omarice ali prostori, v katerih se zaključujejo priključki ožičenja, so varovani in ne omogočajo fizičnega dostopa nepooblaščenim osebam.

Vzdrževanje strojne opreme

Vsa računalniška oprema je redno vzdrževana, kar izvajajo pooblašteni strokovno usposobljeni zaposleni ali zunanji pooblašteni vzdrževalci. Zunanji izvajalci imajo sprejeti dogovor o varovanju zaupnosti, skladno s **politiko do dobaviteljev**.

Pri vzdrževanju opreme s strani zunanjih izvajalcev, se ustrezno varuje podatke. Vsa vzdrževalna dela se opravijo na mestu, kjer se nahaja oprema. Če to ni izvedljivo, se prepreči nepooblaščen dostop do podatkov. Kadar obstaja možnost odstranitve nosilcev podatkov iz opreme, se nosilce varno shraniti. Kadar nosilcev ni mogoče odstraniti, je postopek vzdrževanja nadzorovan. Tudi pri selitvi opreme se zagotovi varnost podatkov.

Evidentirana je vsa računalniška oprema, ki eventuelno mora zaradi vzdrževanja zapustiti prostore podjetja.

Opremo se vzdržuje in čisti v skladu s priporočili proizvajalca. Vsa čiščenja občutljive opreme, razen zaslonov tipkovnic in površinskega čiščenja ohišij neobčutljivih naprav, opravljajo pooblašteni izvajalci. V varovana območja sme osebje za čiščenje vstopati le pod nadzorom. Kritične opreme praviloma ne čistimo med obratovanjem, razen, če proizvajalec opreme ne priporoča drugače.

Vodi in vzdržuje se dokumentacija in navodila o opremi. Za vso opremo obstajata dokumentacija, ki je dostopna zaposlenim, ki opremo vzdržujejo.

Vzpostavljena in vzdrževana je evidenca računalniške opreme v sektorju za informatiko. Opremljena je s podatki o uporabi, vzdrževanju in varovanju.

Posebno pomembno je varovanje prenosne opreme za rabo izven organizacije na službeni poti.

Varno uničenje in odpis opreme

Na opremi, ki se odpiše, se predhodno varno odstraniti podatke. Podatke brišemo šele, ko so preneseni na drug sistem. Za ustrezno brisanje podatkov se uporablja namenska programska oprema ali pa se nosilci podatkov komisijsko fizično uničijo.

	VARNOSTNA POLITIKA	
	POLITIKA FIZIČNEGA VAROVANJA	
	Oznaka: VP 07-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 6/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Pri zamenjavi in odpisu opreme za varnostno kopiranje podatkov, se zagotovi, da nova oprema lahko bere stare varnostne kopije, ali pa je potrebno prepisati kopije na nov sistem, stare kopije pa uničiti.

5. UVELJAVLJANJE POLITIKE

Kadar se Mariborski vodovod odloča za obnovo, nakup ali najem poslovnih prostorov, morajo odgovorne službe, kadar gre za zagotavljanje informacijske varnosti, upoštevati vse v tem dokumentu navedene zahteve.

Direktor in vodje služb Mariborskega vodovoda skrbijo, da delavci, ki so pod njihovim nadzorom, upoštevajo varnostne mere navedene v tej politiki.

Odgovornost vseh zaposlenih in drugih pooblaščenih izvajalcev (tretje osebe) je, da se ravna skladno s politikami opisanimi v 4. točki tega dokumenta. Vsi uporabniki so dolžni o incidentih in morebitnih zlorabah poročati svojim vodjem in/ali sektorju za informatiko. Pooblaščen uporabniki varovanih območij so dolžni, da preverijo vsako nepooblaščen oseb, ki se nahaja v varovanem območju.

Vsak zaposleni podjetja, na katerega se nanaša ta politika, ki je identificiran in je ugotovljeno, da je prekršil to politiko, je glede na obseg in vsebino kršitve lahko podvržen sankcioniranju in ustreznim disciplinskim ukrepom podjetja.

Dobavitelji, ki kršijo to politiko so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

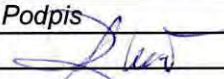
- ISO/IEC 27001-2013 poglavja:
 - A.11.1.1 Varovanje fizičnih meja območja
 - A.11.1.2 Kontrole fizičnega pristopa
 - A.11.1.4 Zaščita pred zunanjimi in okoljskimi grožnjami
 - A.11.1.5 Delo na varovanih območjih»
- Politika je v soodvisnosti z VP_07_02_Politika čiste mize in čistega zaslona, kontrola A.11.1.3«

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VP_05_01_politika FizičnegaVarovanja	VP_07_01_PolitikaFizicnegaVarovanja.doc	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Bojan Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	VARNOSTNA POLITIKA	
	POLITIKA FIZIČNEGA VAROVANJA	
	Oznaka: VP 07-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 7/7
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

	<i>Ime</i>	<i>Podpis</i>
<i>Direktor:</i>	Danilo Burnač	
<i>Sprejet na Forumu varovanja informacij, dne:</i>	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA ČISTE MIZE IN ZASLONA	
	Oznaka: VP 07-02	Datum izdaje: 14.05.2018
	Verzija: 1	Stran: 1/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
5. UVELJAVLJANJE POLITIKE	3
6. REFERENCE	3
7. ZGODOVINA	3

	VARNOSTNA POLITIKA	
	POLITIKA ČISTE MIZE IN ZASLONA	
	Oznaka: VP 07-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Namen politike čiste mize in zaslona je vzpostavitev kulture varovanja informacij in zaupanja med vsemi zaposlenimi v podjetju Mariborski vodovod. Učinkovito izvajanje politike čiste mize in zaslona se odraža v sodelovanju vseh zaposlenih podjetja. Zaposleni varujejo tako elektronske, kakor tudi papirne dokumente, ki vsebujejo podatke o strankah, partnerjih, dobaviteljih in ostale pomembne podatke podjetja. Vsi zaposleni morajo poznati vsebino te varnostne politike. Posebna občutljivost velja za **Osebne podatke**.

Osnovni nameni uveljavljanja politike so:

- Čista in urejena miza vpliva na pozitivno podobo, ki si jo stranke ni partnerji ustvarijo ob vstopu v naše prostore.
- Zmanjša nevarnost in varnostna tveganja pred izgubo ali razkritjem zaupnih podatkov.

Zaupne in občutljive dokumente, ki so odloženi na mizi, lahko nepooblaščen oseba odtuji.

2. OBSEG

S to politiko so seznanjeni in jo morajo spoštovati vsi zaposleni podjetja in ostali uporabniki, ki se srečujejo s podatki podjetja.

Politika se nanaša na vse podatke in informacijske informacije ne glede na medij na katerem se nahajajo.

3. POJMI

- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, dobavitelji in ostali delavci.
- **Zaupne informacije:** skladno s Pravilnikom o varovanju poslovne skrivnosti.
- **Osebni podatki:** skladno s Pravilnikom o varovanju osebnih podatkov.
- **Podatki in informacije:** se nahajajo bodisi na elektronskih medijih, papirni obliki, zvočnih medijih ali so tudi ustne.

4. POLITIKA

V primeru, ko se za dalj časa oddaljite od vaše pisalne mize (npr. malica, sestanki,...), je potrebno fizično dokumentacijo, ki vsebuje zaupne informacije, shraniti v predalnik ali omaro, ki jo je možno zakleniti. Na osebnem računalniku vključite ohranjevalnik zaslona z zaklepanjem (uporabniško geslo).

Po koncu delovnega dneva se pričakuje, da zaposleni pospravijo svojo delovno mizo in odstranijo z miz vse zaupne dokumente. Podjetje zagotavlja zaposlenim predalnike in omare, ki jih je možno zakleniti. Osební računalnik moramo zakleniti oz. vključiti ohranjevalnik zaslona z geslom.

	VARNOSTNA POLITIKA	
	POLITIKA ČISTE MIZE IN ZASLONA	
	Oznaka: VP 07-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Priporočamo naslednje aktivnosti:

- Načrtujte čas vnaprej, da boste lahko uredili tudi svojo papirno dokumentacijo.
- V primeru daljše odsotnosti je potrebno vedno pospraviti in urediti delovni prostor.
- Sodelavcem, ki nas nadomeščajo, posredujemo navodila.
- Nepotrebno papirno dokumentacijo uničimo v skladu z *VP 03-02 Politika primerne rabe informacijske tehnologije*.
- Po potrebi papirno dokumentacijo skeniramo in pretvorimo v elektronsko obliko. V kolikor je mogoče, izvajamo poslovne procese v elektronski obliki.
- Po koncu delovnega dneva obvezno zaklenimo predalnike in omare, kjer hranimo takšne informacije.
- Prenosne računalniške naprave, kot so prenosniki in tablice, shranjujemo v zaklenjene predalnike ali omare, kadar jih ne uporabljamo.
- Naprave za hrambo podatkov, kot so npr. CD romi, DVD ji, USB ključi, diski, idr. moramo prav tako hraniti v zaklenjenih predalnikih ali omarah.

5. UVELJAVLJANJE POLITIKE

V kolikor uporabnik krši določila te politike, bo njegovo ravnanje podvrženo ukrepom po Zakonu o delovnih razmerjih, ki lahko vodijo tudi do prenehanja delovnega razmerja.

Dobavitelji, ki kršijo to politiko, so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

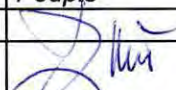
- Uporabljena nadzorstva ISO/IEC 27001:2013,
 - A.11.1.3 varovanje pisarn, sob in naprav
 - A.11.2.8 Nenadzorovana uporabniška oprema
 - A.11.2.9 Politika čiste mize in praznega zaslona
- Politika je v soodvisnosti s politikami:
 - VP 03-02 Primerna raba informacijske tehnologije
 - VP 02-01 Politika mobilnih naprav
- Pravilniki:
 - Pravilnik o varovanju osebnih podatkov
 - Pravilnik o varovanju poslovne skrivnosti

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	Apr.2018	Dodane spr.	VP_07_02_CistaMiza.doc	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Bojan Erker
3		Dodane spr.		Uredil:

	VARNOSTNA POLITIKA	
	POLITIKA ČISTE MIZE IN ZASLONA	
	Oznaka: VP 07-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

	<i>Ime</i>	<i>Podpis</i>
<i>Direktor:</i>	Danilo Burnač	
<i>Sprejet na Forumu varovanja informacij, dne:</i>	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA OPERACIJ	
	Oznaka: VP 08-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 1/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1. Fizično varovanje in zaščita okolja.....	2
4.2. Dostop do sistemov.....	3
4.3. Postopki in odgovornosti produkcije	3
4.4. Preprečevanje zlonamerne kode	4
4.5. Varnostno kopiranje	4
4.6. Spremembe in prevzem informacijske dobrine.....	4
4.7. Sinhronizacija ure.....	5
4.8. Nadzor sistemskih aktivnosti.....	5
4.9. Projektni nadzor	5
5. UVELJAVLJANJE POLITIKE	6
6. REFERENCE	6
7. ZGODOVINA.....	6

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA OPERACIJ	
	Oznaka: VP 08-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Politika upravljanja produkcije informacijskega sistema opredeljuje postopke, kako se uporabljajo in upravljajo sistemi za procesiranje informacij z namenom zaščite informacij in storitev. Opredeljuje standardne postopke produkcije IS in odgovornosti skrbnikov, za delovanje ključnih sistemov za končne uporabnike informacijskega sistema v normalnih pogojih. Vpeljuje ločeno dodeljevanje nalog osebju, ki posreduje ali upravlja z občutljivimi podatki, t.i. skrbništvo s ciljem boljšega nadzora nad delom. Politika vključuje pravila za posege v produkcijsko okolje in migracije iz razvojnega v produkcijsko okolje.

2. OBSEG

Politika zajema vse produkcijske informacijske vire v Mariborskem vodovodu. S politiko so seznanjeni vsi v zaposleni v sektorju za informatiko.

3. POJMI

Uporabniki: so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, dobavitelji in ostali delavci.

Produkcija IS: se nanaša na informacijske vire (najpogostejše strežniki, ostala systemska in aplikativna programska oprema,...), na katerih tečejo »živi podatki« za končne uporabnike.

Informacijska dobrina: opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema,...)

Skrbnik: (*ang. Administrator*) upravljalec informacijskega vira s posebnimi pooblastili.

4. POLITIKA

4.1. Fizično varovanje in zaščita okolja

Področja in pisarne, kjer se procesirajo občutljive informacije zahtevajo določen nivo fizičnega varovanja in pristopne kontrole. Avtorizirano osebje, ki dostopa do teh prostorov mora biti seznanjeno z varnostnimi tveganji in ukrepi za njihovo obvladovanje.

Visoko kritični sistemi	Srednje kritični sistemi	Nizko kritični sistemi
Zaklenjeni prostori z pristopno kontrolo.	Zaklenjeni prostori.	Običajni prostori-pisarne.

Kritičnost sistemov je opredeljena v dokumentu: **seznam_kriticnih_it_sistemov.doc**

Varovanje občutljive opreme je opredeljeno v VP 07-01 Politika fizičnega varovanja in VP 05-01 Politika nadzora dostopa, za vse uporabnike.

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA OPERACIJ	
	Oznaka: VP 08-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.2. Dostop do sistemov

Skrbniški dostop do sistemov zahteva varen (kriptiran) proces prijave. Za visoko tvegane sisteme je morda smiselno omejiti čas dneva in, ali lokacijo dostopa.

Splošne in skrbniške zahteve dostopa do sistemov opredeljuje *VP 05-01 Politika nadzora dostopa*.

Politika skrbniških gesel je opredeljena v *VP 05-02 Politika uporabe gesel*.

4.3. Postopki in odgovornosti produkcije

Dokumentiranje delovnih postopkov in opravil: Zaposleni, skladno z organizacijo sektorja za informatiko so odgovorni za dokumentiranje postopkov in opravil, ki jih izvaja sektor. Dokumentacija je v obliki »Sistemskih postopkov« in »Sistemskih navodil«,... in je odobrena z stani vodje sektorja informatike, ter na razpolago samo tistim zaposlenim, ki jih pri svojem delu potrebujejo.

Upravljanje sistemov in poslovnih aplikacij, vključno z uporabo sistemskih orodij v Mariborskem vodovodu upravlja pooblaščen in ustrezno usposobljeno osebje, ki nadzoruje dnevno razpoložljivost in skrbi za varnost in integriteto v sodelovanju z ostalimi skrbniki sistemov. Sodelavec, ki odgovoren za sisteme je ustrezno seznanjen s tematiko sistemske informacijske varnosti.

Vsak sistem je evidentiran in ima jasno opredeljeno sistemsko skrbništvo, ki je lahko individualno ali skupinsko, informacije pa morajo biti ažurne. Minimalen nabor informacij je:

- Inventarna številka
- kontaktna oseba(skrbnik), namestnika kontaktne osebe (namestnik skrbnika)
- osnovne podatke o strojni in sistemski programski opremi,

Vsi navedeni podatki so del ocene tveganj in so ažurirani v tabeli **VP-OT_viri.xls**

Ločevanje nalog: Znotraj sektorja za informatiko so vloge, področja in odgovornosti zaposlenih omejene z namenom omejitve namerne ali nenamerne spremembe ali zlorabe informacij ali storitev.

- V informatiziranem okolju je ločena sistemska administracija od uporabniških aktivnosti.
- Vloga sistema skrbnika osebnih računalnikov, kakor strežniških kapacitet je (glede na majhnost podjetja) dodeljena eni osebi. Strokovno podporno nudijo tudi zunanji izvajalci (outsourcing), v skadu s pogodbo.
- Vloga skrbnika podatkovnih baz zaradi majhnosti podjetja ni ločena od vloge sistema skrbnika računalnikov. Strokovno podporno nudijo tudi zunanji izvajalci (outsourcing), v skadu s pogodbo.
- Vloge skrbnika omrežja zaradi majhnosti podjetja niso ločene od skrbnika računalnikov. Strokovno podporno nudijo tudi zunanji izvajalci (outsourcing), v skadu s pogodbo.

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA OPERACIJ	
	Oznaka: VP 08-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Vloge so opredeljene v tabeli *VP-OT_viri.xls*. Tabela opredeljuje skrbnika in namestnika skrbnika za posamezen informacijska dobrina (npr. strežnik) in skrbnika ali podrobneje skrbnika in namestnika za posamezen del na viru (servis na strežniku).

Ločevanje za programsko opremo je prav tako zapisan v tabeli *VP-OT_viri.xls*.

4.4. Preprečevanje zlonamerne kode

Preprečevanje zlonamerne kode opredeljuje VP 08-03 Politika zaščite pred zlonamerno programsko opremo.

4.5. Varnostno kopiranje

Varovanje podatkov opredeljuje VP 08-02 Politika varnostnega kopiranja.

4.6. Spremembe in prevzem informacijske dobrine

Vse spremembe v produkcijskem okolju informacijskega sistema je potrebno nadzorovati, da se zagotovi trajno skladnost z informacijsko varnostjo. Konfiguracija operacijskega sistema in aplikativna programska oprema morata biti pod strogo kontrolo sprememb, ki zajema:

- identifikacija in zapis bistvenih sprememb,
- planiranje in testiranje sprememb,
- potencialni varnostni vplivi,
- formalizirani postopek potrjevanja predlaganih sprememb,
- postopek vrnitve v prvotno stanje.

Spremembe na produkcijskih dobrinah IS zahtevajo potrditev:

Visoko kritični sistemi	Srednje kritični sistemi	Nizko kritični sistemi
Dokumentirane spremembe potrjujejo vodja SI, obveščen pa je tudi direktor	Dokumentirane spremembe potrjuje vodja SI	Dokumentirane spremembe potrjujejo skrbniki dobrin

Razvojne in testne zmogljivosti visoko kritičnih sistemov, morajo biti ločene od produkcijskih zmogljivosti, da se prepreči neavtorizirani pristop ali nenadzorovana sprememba. Pri tem se upošteva:

- pravila prenosa programske opreme od razvojnega okolja, do produkcije, ki naj bodo dokumentirana,
- razvojna in produkcijska verzija naj tečeta na identični vendar ločeni opremi (fizično ali logično drug strežnik, ločena domena ali ločene mape...)
- razvojna orodja (compiler, editor,...) naj ne bodo nameščena na produkcijski opremi, če niso nujno potrebna
- občutljivi podatki produkcije se naj ne prenašajo v testno ali razvojno okolje

Postopki za **srednje in nizko kritične sisteme** so lahko poenostavljeni, a kljub temu nadzorovani.

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA OPERACIJ	
	Oznaka: VP 08-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 5/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Kritičnost sistemov je opredeljena v sistemskem postopku:

seznam_kriticnih_it_sistemov.doc

Kriteriji sprejemljivosti: Z namenom minimiranja tveganj sistemskih napak na **visoko kritičnih sistemih**, se oblikujejo kriteriji sprejemljivosti za nov informacijski sistem, nadgradnjo oz. novo različico že med razvojem, pred testiranjem in potrditvijo. Med testiranjem se lahko koristijo sistemska orodja »tuning and monitoring«, za doseg izboljšanja razpoložljivosti in učinkovitosti sistema. Naredi naj se projekcija zahtevanih procesnih, pomnilniških, in komunikacijskih kapacitet za prihodnost ob upoštevanju predvidenih poslovnih zahtev.

4.7. Sinhronizacija ure

Pravilna nastavitev ure in časa na vseh računalnikih, je bistvenega pomena, da se zagotovi točnost revizijskih dnevnikov, ki je lahko potrebna, če se preučuje problem ali kot dokaz v sodnih ali disciplinskih postopkih.

Sistemske ure se morajo redno sinhronizirati med vsemi sistemi in računalniki podjetja!

4.8. Nadzor sistemskih aktivnosti

Zmogljivosti računalniških sistemov, ki podpirajo produkcijske poslovne procese se spremlja z namenom opazovanja trenda zmogljivosti procesorske moči, pomnilniških in omrežnih zmogljivosti.

Oseba odgovorna za sisteme izvaja nadzor nad sistemi po vnaprej izdelani listi preverjanj (ang. *Check list*) **SN_06_02_CheckList.xls**.

Vsi dostopi do informacijskih storitev se beležijo in spremljajo z namenom identifikacije potencialne zlorabe (revizijska sled).

Varnostni, sistemski, operativni dnevniki se redno pregledujejo s strani usposobljenega osebja. Zmogljivosti za beleženje dnevnikov je zaščiteno pred nepooblaščenim spreminjanjem s pomočjo varnostnega kopiranja.

V »IT podpori« se beležijo okvare sistemov, z zapiski analize in sprejetimi ukrepi.

Dostop do privilegiranih funkcij operacijskega sistema je omejen na osebe, ki so pooblašcene za izvajanje vodstvenih funkcij s strani vodje SI. Te funkcije se dodatno logirajo in nadzorujejo.

4.9. Projektni nadzor

Mariborski vodovod ima vzpostavljene postopke za nadzor razvojne in produkcijske programske opreme. Vsi sistemi razviti znotraj ali zunaj Mariborskega vodovoda upoštevajo formalen proces razvoja. Zunanji razvoj je opredeljen v posamezni pogodbi. Testni podatki so izbrani pazljivo, zaščiteni in nadzorovani. Dostop do programske izvirne kode je strogo omejen.

	VARNOSTNA POLITIKA	
	POLITIKA VAROVANJA OPERACIJ	
	Oznaka: VP 08-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 6/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

5. UVELJAVLJANJE POLITIKE

Vsak zaposleni, na katerega se nanaša ta politika, ki je identificiran in je ugotovljeno, da je prekršil to politiko, je glede na obseg in vsebino kršitve lahko podvržen sankcioniranju in ustreznim disciplinskim ukrepom podjetja.

Tretje osebe, ki kršijo to politiko so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

- Uporabljena nadzorstva ISO/IEC 27001-2013 poglavja:
 - A.12 Varnost operacij
 - A.12.1 Operativni postopki in odgovornosti
 - A.12.4 Beleženje in spremljanje
 - A.12.5 Nadzor operativne programske opreme
 - A.12.6 Upravljanje tehničnih ranljivosti
- Politika je v soodvisnosti z politikami:
 - VP 05-01 Politika nadzora dostopa
 - VP 05-02 Politika uporabe gesel
 - VP 07-01 Politika fizičnega varovanja
 - VP 08-02 Politika varnostnega kopiranja
 - VP 08-03 Politika zaščite pred zlonamerno prog. opremo
- Soodvisni dokumenti:
 - Informacijska tabela vzdrževalcev VP-OT_viri.xls
 - Seznam za vzdrževanje programov VP-OT_viri.xls
 - Klasifikacija kritičnih informacijskih sistemov: **seznam_kriticnih_it_sistemov.doc**

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VO_06_02_UpravljanjeProdukcije	VP_08_01_VarovanjeOperacij.doc	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Dodal: Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTNEGA KOPIRANJA	
	Oznaka: VP 08-02	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 1/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1. Osnovna pravila	2
4.2. Zahteve vezane na varnostno kopiranje podatkov in informacij	3
4.3. Sistemska administracija	3
4.4. Organizacijski ukrepi	3
5. UVELJAVLJANJE POLITIKE	4
6. REFERENCE	4
7. ZGODOVINA	4

	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTNEGA KOPIRANJA	
	Oznaka: VP 08-02	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 2/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Mariborski vodovod je življenjsko odvisen od podatkov in informacij. Zaradi tega mora vse podatke in informacije s katerimi upravlja ustrezno varovati. Varovanje se izvaja z organizacijskimi in tehničnimi ukrepi. Koncept varnostnih kopij za podatke in informacije zagotavlja, da so podatki in informacije dostopne v vsakem trenutku, ko je to potrebno. Cilj te politike je definirati varnostne zahteve, ki jih ima podjetje z varnostno hrambo podatkov in informacij. Vsi podatki in informacije, ki so last podjetja morajo biti varovani pred izgubo.

2. OBSEG

Politika vključuje vse podatke in informacije, ki so ključnega pomena za Mariborski vodovod. Obsega informacijske dobrine na katerih se ti podatki nahajajo in sodelavcem v sistemski službi, sodelavcu sektorja informatike - administratorju, kakor tudi poslovnim lastnikom podatkov.

3. POJMI

- **Pooblaščen delavec:** zaposleni, ki imajo reden dostop do varovanih prostorov (npr. sistemski skrbnik)
- **Pooblaščen oseba:** pooblaščen delavec ali varnostnik, ki lahko pospremi tretjo osebo do varovanih prostorov
- **Dobavitelj:** pravne in fizične osebe, ki sodelujejo z Mariborskim vodovodom in imajo dostop do IT dobrin,
- **Administrator:** sistemski skrbnik, oz. tip uporabnika s posebnimi pooblastili
- **Poslovni lastnik:** je posameznik (uporabnik), ki mu je vodstvo odobrilo uporabo informacijske dobrine. Izraz ne pomeni, da ima ta oseba dejansko lastniško pravico nad tem sredstvom.

4. POLITIKA

4.1. Osnovna pravila

Operativni postopek izvajanja varnostnih kopij je opisan v posebnem dokumentu (**Sistemsko navodilo varnostnega kopiranja SN_08_01_Varnostno kopiranje**). Varnostno kopiranje se izvaja skladno s tem predpisom. V sistemskem navodilu so definirane kontaktne osebe, odgovornosti, intervali varnostnih kopiranj.

V primeru, da varnostno kopiranje izvajajo zunanji izvajalci ima podjetje pravico, v vsakem trenutku, preveri postopke izvajanja varnostnega kopiranja pri zunanjem izvajalcu.

Sistemi za varnostno kopiranje je postavljeni varovan informacijski prostor. Zagotovljen ima nadzorovan fizični in logični dostop. Dostop do teh prostorov je dovoljen samo pooblaščenim delavcem -administratorjem ali tretjim osebam, ki imajo dovoljen dostop do teh prostorov na osnovi pogodb (Politika fizičnega varovanja).

	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTNEGA KOPIRANJA	
	Oznaka: VP 08-02	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 3/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.2. Zahteve vezane na varnostno kopiranje podatkov in informacij

- Varnostno kopiranje sistema
Varnostno kopiranje sistema mora biti realizirano takoj po prvi instalaciji. Spremembe v sistemski konfiguraciji morajo biti varnostno kopirane takoj, ki je bila sprememba implementirana.
- Varnostno kopiranje podatkovne baze
Vse podatke in informacijske dobrine, je treba varnostno kopirati takoj po prvi inicializaciji. Vse spremembe poslovno kritičnih dobrin morajo biti hranjene v transakcijskih logih. Te loge je treba dnevno kopirati na varnostne medije.
- Varnostno kopiranje nosilcev informacij v pisarnah – osebni računalniki
Nosilce informacij, ki jih ni možno varnostno kopirati preko centralnega sistema, so dolžni varovati uporabniki sami. V to kategorijo spadajo lokalni trdi diski, dlančniki, mobilne naprave in vse naprave, ki niso varovane preko centralnega varnostnega sistema. Vsi uporabniki, ki uporabljajo take naprave so dolžni sami poskrbeti za varovanje podatkov in informacij (tudi pred tatvinami). Le to realizirajo z ustreznim kopiranjem podatkov in informacij na mrežno mapo dogovorjenega srežnika. To opredeljuje politika primerne rabe.
- Varovanje podatkov in informacij prenosnih računalnikov
Za podatke na prenosnih računalnikih velja enako kot za osebne računalnike v pisarnah - gornja alineja.
- Katastrofična situacija
Varnostne kopije poslovno kritičnih podatkov in informacij so hranjene na ločeni lokaciji od izvora informacij (strežniki). Oddaljenost, na kateri se hranjene varnostne kopije zagotavlja, da podatke pridobimo tudi v primeru katastrofičnega dogodka (požar, poplava,...).

4.3. Sistemska administracija

- Za vsak sistem morata biti na razpolago nadomestni administrator z istim nivojem znanja obnove,
- administratorji morajo imeti na razpolago dovolj časa za upravljanje s sistemi za izdelavo varnostnih kopij (pregled in nadzor),
- administratorji morajo imajo izdelane plane za testiranje obnove varnostnih kopij in te teste morajo v praksi tudi izvajati.,
- administratorji so ozaveščeni o pomembnosti varnostnega kopiranja in o pomembnosti njihovega dela.
- Sistemski administrator izvaja nadzor nad uspešnostjo izvedbe varnostnih kopij (SN_06_02_CheckList.xls)

4.4. Organizacijski ukrepi

Ustrezno dimenzionirani sistemi za varnostno kopiranje, so fizično ločeni od izvornih sistemov (strežniški sistemi).

Strategija varnostnega kopiranja mora biti jasno določena v sistemskem navodilu izvajanja varnostnega kopiranja.

Ob planiranju projektov informacijske narave je potrebno vsakič preveriti potrebo po varnostnem kopiranju podatkov ali informacij. Ob ugotovljeni potrebi po varnostnem kopiranju informacij se izdelajo postopki varnostnega kopiranja in jih implementirati v prakso.

	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTNEGA KOPIRANJA	
	Oznaka: VP 08-02	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 4/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Vsaj enkrat letno je potrebno izvesti testiranje povrnitve varnostnih kopij. Postopek in rezultati se dokumentirajo in predajo forumu varovanja informacij. Ugotovljene pomanjkljivosti morajo biti odpravljene v najkrajšem možnem roku. Ta rok določi forum.

5. UVELJAVLJANJE POLITIKE

Vsak zaposleni, na katerega se nanaša ta politika, ki je identificiran in je ugotovljeno, da je prekršil to politiko, je glede na obseg in vsebino kršitve lahko podvržen sankcioniranju in ustreznim disciplinskim ukrepom podjetja.

Tretje osebe, ki kršijo to politiko so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

- Uporabljeno nadzorstvo ISO/IEC 27001 ,
A.12.3.1 Varnostno kopiranje
- Navezuje se na dokumente:
VP_03_02_PrimernaRaba
SN_08_01_Varnostno kopiranje
SN_06_02_CheckList.xls

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	15.02.2018	Osnutek	VP_08_02_VarnostnoKopiranje.docx	Pripravil: Bojan Erker
2	12.2019	Dodane spr.		Uredil: Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO	
	Oznaka: VP 08-03	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 1/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
5. UVELJAVLJANJE POLITIKE	3
6. REFERENCE	3
7. ZGODOVINA	3

	VARNOSTNA POLITIKA	
	POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO	
	Oznaka: VP 08-03	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Zlonamerna programska koda, kot so virusi, trojanci, vohunski program, mobilna koda (znotraj brskalnikov), itd., lahko bistveno prizadenejo zaupnost, neoporečnost ali razpoložljivost informacijskih dobrin Mariborskega vodovoda. V informacijski sistem se lahko vsilijo iz različnih tipov datotek, vtičnikov,... iz različnih virov, internet, elektronska pošta, izmenljivi mediji (CD, USB ključ) ali v omrežje vključenega prenosnega računalnika.

Cilj politike je zaščititi celovitost programske opreme in informacij pred takšno kodo.

2. OBSEG

Vsi uporabniki informacijskih storitev so seznanjeni s priporočenimi postopki za preprečevanje in odkrivanje zlonamerne programske opreme.

3. POJMI

Uporabniki: so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, dobavitelji in ostali delavci.

Zlonamerna programska koda: t.i. virusi, trojanski konji, črvi, vohunski program, mobilna koda in ostale oblike

4. POLITIKA

Mariborski vodovod sprejema sledeče postopke za zaščito pred zlonamerno kodo:

- Sektor za informatiko zagotavlja vsem uporabnikom ažurno varnostno programsko opremo.
- Vedno uporablja varnostno programsko opremo, znanega proizvajalca in je na voljo na strežniku podjetja. Uporablja najnovejšo različico, ter jo posodablja takoj ko je posodobitev na voljo.
- Privzeto je samodejno skeniranje priponk elektronske pošte, skeniranje datotečnih sistemov.
- Na internetnih brskalnikih je omejeno izvajanje mobilne kode.
- Datoteke namenjene sistemom, ki podpirajo ključne poslovne procese se najprej prenese ali kako drugače kopira v varno (testno) okolje, skenirati na zlonamerno programsko kodo, ter šele nato preseliti v njihovo končno (produkcijsko) okolje.

Uporabnikom se priporoča, da:

- Nikoli ne odpirajo kakršnih koli datotek ali makrov pripetih k elektronski pošti neznanega, sumljivega pošiljatelja ali vira, ki mu ne zaupajo. Ta sporočila naj takoj izbrišejo ter ponovno izpraznijo koš.
- Izbrišejo SPAM, verižna in ostala nezaželena sporočila. Pošiljanje verižnih pisem v skladu s to politiko podjetja ni dovoljeno!
- Nikoli naj ne snemajo datotek iz neznanih ali sumljivih virov.

	VARNOSTNA POLITIKA	
	POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO	
	Oznaka: VP 08-03	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- Izogibajo se tveganim spletnim stranem (igre na srečo, zabava, posredovalnice za stike...)
- Izogibajo naj se direktni skupni uporabi diskov z bralno/zapisovalnim dostopom razen v primeru, da je to absolutno potrebno za potrebe poslovanja.
- Medije (CD, DVD, USB) pred uporabo naj vedno preiščejo s protivirusnim programom.
- Redno naj izdelujejo varnostne kopije pomembnih podatkov ter jih shranjujejo na varna mesta skladno s politiko primerne rabe.
- V kolikor protivirusna zaščita ovira razvojno testiranje, se lahko ob zagotovitvi, da na sistemu ni virusov, začasno ustavi protivirusno zaščito, in izvedite teste. Po končanem testiranju se protivirusna zaščito spet zažene in preveri sistem. Medtem ko je protivirusni sistem onemogočen naj ne uporabljajo aplikacije, ki bi lahko prinesle zlonamerno kodo.

V primeru vprašanj, suma ali zaznave incidentov naj o tem obvestijo IT podpora na tel. 261 ali na elektronski naslov it.podpora@mb-vodovod.si

5. UVELJAVLJANJE POLITIKE

Vsak zaposleni, na katerega se nanaša ta politika, ki je identificiran in je ugotovljeno, da je prekršil to politiko, je glede na obseg in vsebino kršitve lahko podvržen sankcioniranju in ustreznim disciplinskim ukrepom podjetja.

Tretje osebe, ki kršijo to politiko so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

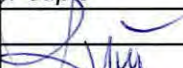
- Uporabljena nadzorstva ISO/IEC 27001, A.12.2.1 Kontrole proti zlonamerni programski opremi

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VP_06_01_ZlonamernaKoda	VP_08_03_ZlonamernaProgramskaOprema.doc	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	VARNOSTNA POLITIKA	
	POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO	
	Oznaka: VP 08-03	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

	<i>Ime</i>	<i>Podpis</i>
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	



	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTI KOMUNIKACIJ	
	Oznaka: VP 09-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 1/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
5. UVELJAVLJANJE POLITIKE	5
6. REFERENCE	5
7. ZGODOVINA	5

	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTI KOMUNIKACIJ	
	Oznaka: VP 09-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Politika varnosti komunikacij določa, kako so zasnovana omrežja in sistemi povezani z njimi. Vsebuje zahteve za ustrezne tehnične in postopkovne kontrole za zmanjševanje tveganj.

Omrežja so običajno razdeljena tudi z vidika različnih varnostnih zahtev, s komunikacijskimi kontrolnimi točkami se preprečuje nepotreben promet med njimi. Posebno pozornost posvečamo zaščiti teh komunikacijskih dobrin pred nepooblaščenim dostopom.

Politika opredeljuje tudi možnost in zahteve oddaljenega dostopa.

2. OBSEG

Politika se nanaša gradnike omrežja, aktivne mrežne naprave (stikala, usmerjevalnike, požarne pregrade, IDS, IPS, VPN sisteme, idr.), ki sestavljajo LAN, WAN omrežje v domeni upravljanja Mariborskega vodovoda.

S politiko so seznanjeni zaposleni v Službi informatike, skrbniki omrežja in sistemski skrbniki in ostali uporabniki, ki vključujejo v omrežje naprave ali storitve (dobavitelji).

3. POJMI

- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, dobavitelji in ostali delavci.
- **Sistemski skrbnik:** (*ang. Sistem Administrator*) upravljalec informacijske dobrine s posebnimi pooblastili.
- **Skrbnik omrežja:** upravljalec komunikacijskega informacijske dobrine s posebnimi pooblastili.
- **Komunikacijska kontrolna točka:** je komunikacijska informacijska dobrina, kot je: stikalo, usmerjevalnik, požarna pregrada, IDS, IPS, VPN sistem, idr.
- **Informacijska dobrina:** opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema, ...).
- **VPN:** (*ang. Virtual Private Network*) navidežno zasebno omrežje.
- **VLAN:** navidežno lokalno omrežje.

4. POLITIKA

4.1 Konfiguracija omrežja

Omrežje je zasnovano in konfigurirano za visoko zmogljivost in zanesljivost, ki je potrebna za zadovoljevanje komunikacijskih potreb podjetja, hkrati pa zagotavlja visoko stopnjo nadzora dostopa in omejitev privilegijev.

Omrežje je segmentirano na posamezna področja (logične domene), znotraj katerih so določene skupine uporabnikov in računalnikov:

- Vzpostavljena je segmentacija omrežja (OSI L3),

	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTI KOMUNIKACIJ	
	Oznaka: VP 09-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- omogoča ločevanje virov glede na vrednost in tip,
- poskrbi za večnivojsko zaščito bolj pomembnih virov,
- vključuje tudi uporabo naslavljanja NAT/PAT.

Nad področji je vzpostavljen nadzor dostopa in usmerjanja. Stopnja nadzora mora biti sorazmerna z zahtevami pomembnosti dobrin (virov).

Konfiguracija omrežij neposredno vpliva na njihovo delovanje, na njihovo stabilnost in varnost informacij.

Varnostni vidiki omrežij, ki jih je treba upoštevati:

- nestabilnost omrežja lahko ogroža poslovanje podjetja,
- neprimeren nadzor nad dostopom do omrežja lahko ogrozi zaupnost in celovitost podatkov,
- neustrezne zmogljivosti omrežij lahko otežijo ali celo onemogočajo delovanje,
- počasni ali neustrezni odzivni časi sistemov lahko ovirajo poslovno obdelavo.

4.2 Kontrola dostopa do omrežja

Dostop do omrežnih storitev je na nivoju posameznega uporabnika in računalnika. Postopek dostopne kontrole se izvaja ob pomoči močne identifikacije in avtentifikacije.

V osnovi imajo uporabniki dostop zgolj do informacijskih storitev za katere so avtorizirani. Po potrebi se lahko na omrežju omogočijo kontrole in omejitve posameznim uporabnikom ali skupinam, če to zahteva politika dostopa do posameznih aplikacij.

Politiko dostopa do informacijskih sistemov (operacijski sistem, aplikacije,...) opredeljuje VP 05-01 *Politika nadzora dostopa*.

Nezaščitena diagnostična vrata (porti), »out of the band« in upravljalna vrata, »in band« (SNMP ali web vmesnik na usmerjevalnikih) predstavljajo tveganje nepooblaščenega dostopa. Logičen dostop do vrat, ki niso potrebna za diagnostiko ali konfiguracijo je onemogočen, vsi potrebni dostopi do vrat pa so omejeni na avtorizirano skrbniško osebje. To opredeljuje VP 05-02 *Politika uporabe gesel*, poglavje *Skrbniška gesla*.

Vsi skrbniški dostopi do komunikacijskih informacijskih dobrin se beležijo z namenom zagotavljanja revizijske sledi.

4.3 Nadzor oddaljenega dostopa do omrežja (VPN)

Napravam, ki niso v popolnem nadzoru Mariborskega vodovoda, je onemogočen nepooblaščen dostop do omrežnih storitev in aplikacij.

Pooblaščen oddaljeni uporabniki, bodisi od doma ali na poslovnih potovanjih ipd., lahko neposredno komunicirajo z informacijskim sistemom podjetja za sprejem/pošiljanje podatkov in posodobitve. Ti fizično oddaljeni uporabniki se pogosto povezujejo preko javnih omrežij, kar povečuje tveganje za nedovoljen dostop.

	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTI KOMUNIKACIJ	
	Oznaka: VP 09-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

V kolikor obstaja poslovna potreba po takšnem povezovanju, je le to možno zgolj ob preverjanju pristnosti naprave in uporabo ustreznega avtentifikacijskega in avtorizacijskega mehanizma.

Oddaljena povezava z omrežjem podjetja je dovoljena le, kadar je pooblaščen uporabnik potrjen, podatki pri prenosu so šifrirani. V praksi se ti uporabniki na daljavo (od doma, na službeni poti, idr) povezujejo na informacijski sistem podjetja preko navideznega privatnega omrežja (VPN).

Zahteve in odgovornosti uporabnikov, ki jim je omogočen oddaljen dostop do omrežja podjetja opredeljuje *VP 02-02 Politika dela na daljavo*.

4.4 Upravljanje omrežja

Z omrežjem Mariborskega vodovoda upravlja pooblaščen in ustrezno usposobljeno osebje, ki nadzoruje dnevno razpoložljivost in skrbi za varnost in integriteto v sodelovanju z ostalimi skrbniki sistemov in dobavitelji. Osebje je ustrezno usposobljeno za tematiko mrežne informacijske varnosti.

Premike, menjave in spremembe konfiguracijskih nastavitev in uporabnikov, ter dostopnih (kontrolnih) točk do omrežja sme izvajati samo ustrezno usposobljeno in pooblaščen osebje v Službi informatike in dobavitelj, ki vodi popolno evidenco vseh sprememb.

Spremembe na komunikacijskih virih zahtevajo potrditev nadrejenih:

Visoko kritične dobrine	Srednje kritične dobrine	Nizko kritični dobrine
Dokumentirane spremembe potrjuje vodja Službe informatike, ki je zastopan v varnostnem forumu (požarna pregrada, glavna stikala, VPN,...)	Dokumentirane spremembe lahko izvaja skrbnik omrežja ob podpori dobavitelja. (rec. dostopna stikala)	Izvaja skrbnik omrežja

Posodobitve programske opreme komunikacijskih informacijskih virov (firmware) mora biti skrbno načrtovano in vodeno, da se minimizirajo varnostna tveganja, vzpostavljena pa morata biti tudi postopkovni in tehnični nadzor.

Za vse spremembe na kritičnih sistemih omrežja morajo biti vpeljeni formalni postopki za kontrolo sprememb in zagotovljena revizijska sled. Vse spremembe na kritičnih sistemih morajo biti predhodno preizkušene in odobrene pred selitvijo v živo okolje.

4.5 Fizična varnost in integriteta

Omrežna in komunikacijska infrastruktura, vključno s kabli in komunikacijskimi omarami, mora zagotavljati dobro varnost pred fizičnim napadom in nepooblaščenim vdorom.

Področja, kjer se nahajajo komunikacijsko informacijske dobrine zahtevajo določen nivo fizičnega varovanja in pristopne kontrole. Avtorizirano osebje, ki dostopa do teh prostorov, mora biti seznanjeno z varnostnimi tveganji in ukrepi za njihovo obvladovanje.

	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTI KOMUNIKACIJ	
	Oznaka: VP 09-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 5/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Visoko kritične dobrine	Srednje kritične dobrine	Nizko kritične dobrine
Izključno v podatkovnem centru. Pristop je nadzorovan. (požarna pregrada, glavna stikala, VPN,..)	Zaklenjeni prostori z pristopno kontrolo. Pristop je pod kontrolo. (dostopna stikala)	Običajni prostori podjetja.

Fizično varovanje občutljive opreme je opredeljeno v *VP 05-01 Politika nadzora dostopa*

Fizični in logični dostop do omrežnih dobrin je strogo nadzorovan z namenom, da se prepreči nepooblaščen dostop. **Fizični in logični dostop do omrežnih naprav je prepovedan vsem, razen avtoriziranemu osebju.** Nepooblaščenim uporabnikom pomeni je prepovedano skeniranje portov, servisov, ipd...

5. UVELJAVLJANJE POLITIKE

V kolikor uporabnik krši določila te politike, bo njegovo ravnanje podvrženo ukrepom po Zakonu o delovnih razmerjih, ki lahko vodijo tudi do prenehanja delovnega razmerja.

Dobavitelji, ki kršijo to politiko, so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

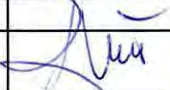
- Uporabljena nadzorstva ISO/IEC 27001-2013:
 - A.9.1.1 Dostop do omrežij in omrežnih storitev
 - A.13.1.1 Omrežne kontrole
 - A.13.1.2 Varovanje omrežnih storitev
 - A.13.1.3 Ločevanje v omrežjih
- Politika je v soodvisnosti s politikami:
 - VP 05-01 Politika nadzora dostopa
 - VP 05-02 Politika uporabe gesel
 - VP 02-02 Politika dela na daljavo
 - VP 08-01 Politika varovanja operacij

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	Apr.2018	Nova	VP_09_01_VarnostKomunikacij.doc	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Erker
3		Dodane spr.		Uredil:

	VARNOSTNA POLITIKA	
	POLITIKA VARNOSTI KOMUNIKACIJ	
	Oznaka: VP 09-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 6/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

	<i>Ime</i>	<i>Podpis</i>
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 1/11
	Datum zadnje revizije: 12.02.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	3
4.1. Splošne zahteve politike	3
4.2. Primerna raba	4
4.3. Omejena zasebna raba	4
4.4. Raba tretjih oseb	5
4.5. Dostop do elektronske pošte	5
4.6. Uporaba priponk	6
4.7. Prepovedana uporaba	6
4.8. Zaščita in varovanje elektronske pošte	7
4.9. Velikost poštnega nabiralnika (mailboxa)	7
4.10. Nadzor nad elektronsko pošto	7
4.10.1. Nadzor nad vsebino službenih elektronskih poštnih sporočil	8
4.10.2. Vpogled v službene e- poštne predale za namene vzdrževanja	8
4.10.3. Nadzor nad zasebno elektronsko pošto	9
4.10.4. Nadzor nad službeno elektronsko pošto, ki se izmenjuje preko »info« poštnega predala	9
4.11. Pravno obvestilo – izjava o omejitvi odgovornosti	9
5. UVELJAVLJANJE POLITIKE	10
6. REFERENCE	10
7. ZGODOVINA	10
8. PRILOGA	11

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Elektronska pošta je postala razširjen način komuniciranja v Mariborskem vodovodu. Je nenadomestljivo poslovno orodje, ki olajša komuniciranje, pospešuje tok dela, povečuje produktivnost in služi tudi drugim poslovnim funkcijam. Podjetje podpira uporabo elektronske pošte v poslovne namene, pri čemer pa pričakuje od uporabnikov vestno, učinkovito in odgovorno rabo vseh sistemov za elektronsko pošto.

Namen te politike je:

- zagotovitev varne in primerne uporabe sistema elektronske pošte s strani uporabnikov,
- preprečevanje omadeževanja podobe podjetja, do katerega lahko pride zaradi napačnega tolmačenja vsebine elektronske pošte s strani naslovnika oz. prejemnika elektronskega sporočila,
- seznanitev uporabnikov s tveganji, povezanimi z uporabo elektronske pošte,
- opredelitev ukrepov za zaščito informacij pred nepooblaščenim razkritjem ali zlorabo.

Ko elektronsko sporočilo zapusti okolje podjetja, lahko javnost njegovo vsebino razume kot uradno stališče ali mnenje Mariborskega vodovoda.

Mariborski vodovod zagotavlja svojim zaposlenim in drugim uporabnikom (zunanjim sodelavcem in pogodbenim partnerjem, ki uporabljajo internetno povezavo podjetja) možnost uporabe sistema elektronske pošte predvsem zaradi zahtev sodobnega poslovanja in učinkovitejšega izpolnjevanja delovnih obveznosti.

2. OBSEG

Politika določa smernice za uporabo elektronske pošte, v kateri se na mestu pošiljatelja pojavi elektronski naslov z domeno Mariborskega vodovoda (@mb-vodovod.si) in opredeljuje način zasebne rabe na infrastrukturi podjetja.

Velja za vse zaposlene, za vse zunanje sodelavce in pogodbene partnerje, ki uporabljajo sistem elektronske pošte (v nadaljevanju: uporabniki).

3. POJMI

- **Informacijska dobrina:** opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema, poljuben nosilec informacij...)
- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, dobavitelji in ostali delavci.
- **Dobavitelji:** pravne in fizične osebe, ki sodelujejo z Mariborskim vodovodom in imajo dostop do IT dobrin,
- **Lastnik:** posameznik (uporabnik), kateremu je vodstvo odobrilo odgovornost za uporabo, nadzorovanje, razvoj, vzdrževanje in varovanje informacijske dobrine. Izraz "lastnik" ne pomeni, da ima ta oseba dejanske lastniške pravice v zvezi z tem informacijsko dobrino.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4. POLITIKA

4.1. Splošne zahteve politike

Uporabniki elektronski naslov na spletni domeni Mariborski vodovod (npr. ime.priimek@mb-vodovod.si) uporabljajo za izvrševanje nalog na delovnem mestu, za osebne potrebe pa lahko v omejenem obsegu in v skladu s pravili te politike uporabljajo storitve komercialnih ponudnikov elektronske pošte (gmail, yahoo, hotmail, idr.).

Vse informacije ustvarjene, poslane ali prejele prek sistema elektronske pošte z izjemo mape "ZASEBNO" so last podjetja Mariborskega vodovoda. Te informacije se ne štejejo kot zasebne, vključno s sporočili elektronske pošte in pripetimi datotekami (pripisanimi) poslanimi in/ ali prejetimi preko sistema elektronske pošte podjetja.

Mariborski vodovod terja od uporabnikov posebno natančnost pri pisanju pravih elektronskih naslovov. Od uporabnikov se pričakuje, da upoštevajo pravila omrežnega vedenja, ki so podana tudi v politiki uporabe interneta. Sporočila naj bodo primerne vsebine in oblike, napisana v spoštljivem tonu do naslovnika ter slovnično pravilna.

Vsako sporočilo ali datoteka, ki je poslana po elektronski pošti mora biti podpisana z imenom in priimkom pošiljatelja.

Pošiljatelji za pošiljanje elektronskih sporočil službene narave v razmerju do naslovnikov ne smejo uporabljati lastnih e-poštnih računov komercialnih ponudnikov (npr. gmail, yahoo, hotmail, ipd.). Uporaba takšnih računov za pošiljanje in prejemanje elektronske pošte je dovoljena le v izjemnih primerih, ko je pošiljanje ali prejemanje elektronskih sporočil nujno potrebno za nemoteno delovanje Mariborskega vodovoda ali za nemoteno opravljanje del uporabnikov, pa je poštni sistem podjetja v okvari ali ga ni mogoče uporabljati zaradi tehnično - varnostnih razlogov. Nedelovanje elektronskega sporočilnega sistema je mogoče preveriti na podpori uporabnikom "IT.podpora" na tel. 261.

Mariborski vodovod si bo z vsemi dovoljenimi in z zakonodajo skladnimi tehničnimi in organizacijskimi postopki in ukrepi prizadeval omejiti možnosti za nepooblaščen dostop do sistema elektronske pošte, vsakršno nepooblaščen spremembo informacij ali preprečevanje storitve ter zagotoviti splošno zanesljivost in dostopnost storitve.

Sistem je organiziran tako, da ves čas njegove uporabe omogoča sledljivost pošiljanja informacij po elektronski pošti in s tem preprečitev možnosti zlorabe sistema, obenem pa je uveden nadzor dostopa do sistema za oddaljene uporabnike elektronske pošte (owa,pop,smtp?).

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.2. Primerna raba

Uporabnik je dolžan uporabljati sistem elektronske pošte odgovorno in etično ter skladno s to politiko in drugimi internimi predpisi ali navodili.

Vse informacije o strankah in poslovanju Mariborskega vodovoda so zaupne narave (razen informacije javnega značaja). Tako se od uporabnika pričakuje enako ravnanje z zaupnimi informacijami v elektronski obliki, kot z zaupnimi papirnimi dokumenti. Nikakor jih ne smemo razkrivati nepooblaščenim osebam.

Kadar uporabnik prenaša občutljive podatke preko elektronske pošte, morata obe strani, kjer je to mogoče, overiti identiteto pošiljatelja, z uporabo elektronskega podpisa. Le tako lahko zagotovimo tudi nespremenjenost in nezatajivost elektronskega sporočila. Informacije v glavi prejetega sporočila, ki vsebuje podatke o pošiljatelju, nikakor niso zadostne za overitev identitete pošiljatelja.

Uporabniki elektronske pošte se morajo zavedati, da je kljub skrbi za varnost skrbnikov sistema, elektronska sporočila možno, glede na tehnologijo, posredovati drugim, jo prestrezati, shranjevati in tiskati. Pri prenosu zaupnih podatkov (npr. osebni podatki) preko elektronske pošte, mora uporabnik uporabljati mehanizme šifriranja, ki omogočajo prebiranje sporočila samo želenim prejemnikom.

Uporabnik mora periodično brisati iz svojega poštnega predala, vsa sporočila, ki jih več ne potrebuje v službene namene, ali na zahtevo skrbnika sistema elektronske pošte. Uporabniki so dolžni racionalno razpolagati s prostorom poštnega predala, tako se naj izogibajo shranjevanju velikih datotek v multimedijskih formatih.

Vsako elektronsko sporočilo, ki zapusti omrežje podjetja, naj bo opremljeno z nogo ki vsebuje pravno obvestilo – izjavo o omejitvi odgovornosti, ki je priloga politike.

Uporabnik poštnega nabiralnika mora biti posebej previden pri odpiranju prejetih elektronskih sporočil, če je pošiljatelj neznan ali nepreverjen, če je naslov e- sporočila sumljiv in predvsem, če e-sporočilo vsebuje tudi priponko.

V primerih, ko uporabniki zaznajo takšna elektronska sporočila, so dolžni o tem nemudoma obvestiti podporo uporabnikom »IT.podpora« podjetja. V kolikor pa sami presodijo, da gre za neželeno pošto (SPAM) ali za pošto, ki bi lahko kakorkoli ogrozila računalniški sistem podjetja, pa so takšna sporočila dolžni izbrisati ali jih preusmeriti v koš za sporočila.

Mariborski vodovod z ustreznimi strojnimi in programskimi orodji sicer filtrira nezaželeno e-pošto, vendar ne more zagotoviti popolne zapore zaradi vedno novega pojavljanja žarišč takšne pošte.

4.3. Omejena zasebna raba

Elektronska pošta je v osnovi namenjena poslovni rabi. Mariborski vodovod dovoljuje omejeno zasebno rabo, vendar le v kolikor to ne ogroža delovnega procesa ali informacijske infrastrukture ter v kolikor ne posega v pravice ostalih uporabnikov.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 5/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Uporabniki je dolžan zagotoviti, da osebna rabe:

- ne ovira dela in delavčevih delovnih obveznosti,
- ne sme predstavljati ali zastopati poslovnih vidikov,
- je omejena na ožji krog prejemnikov,
- ne sme povzročati nobenih neupravičenih stroškov,
- ne sme imeti nikakršnega negativnega vpliva na podjetje.

Zaradi izključitve varnostnih tveganj in hkratnega upoštevanja zasebnosti, morajo biti zasebna sporočila (domene @mb-vodovod.si) in vse datoteke, povezane z njimi, shranjena v mapi "ZASEBNO", ločeno od sporočil, povezanih z izpolnjevanjem delovnih obveznosti. Vsebina zasebne mape v sistemu elektronske pošte ne sme presegati 500 MB podatkov. Podjetje se zavezuje, da bo spoštovala zasebnost uporabnika izključno znotraj te mape.

Ob upoštevanju zgornjih zahtev je omejeno dovoljena tudi raba zasebnih elektronskih računov komercialnih ponudnikov (gmail, yahoo, hotmail).

4.4. Raba tretjih oseb

Pogodbeni delavci in drugi partnerji smejo uporabljati elektronsko pošto Mariborskega vodovoda, samo če so za to avtorizirani z razlogom, da je taka raba potrebna za doseg pričakovanih rezultatov njihovega dela v podjetju.

Vsak tak uporabnik mora biti seznanjen in mora delovati skladno s to politiko.

4.5. Dostop do elektronske pošte

Uporabniki, ki uporabljajo sistem elektronske pošte v podjetju, morajo imeti za to ustrezno pooblastilo vodje organizacijske enote.

Uporabnik sistema elektronske pošte lahko v primeru odsotnosti izzven podjetja, do svojega poštnega predala dostopa na daljavo, pri čemer pa za takšen dostop veljajo pogoji in zahteve, določene v tej politiki, politiki interneta in z njo povezano politiko oddaljenega dostopa.

V primeru, ko posamezniku preneha delovno razmerje z Mariborskim vodovodom je njegov naslednik na tem delovnem mestu ali na drugem delovnem mestu z enakim ali podobnim opisom delovnih nalog (v primeru, da se prejšnje delovno mesto ukine) upravičen do uporabe elektronskih sporočil, ki so bila shranjena v elektronskem poštnem predalu njegovega predhodnika, če:

- je to potrebno za kontinuiteto opravljanja delovnih nalog in za nemoten proces dela in
- če to predhodno odobri njegov nadrejeni.

Za dostop do elektronske pošte je dovoljeno uporabljati samo tipe in verzije programske opreme, ki so odobreni s strani sektorja za informatiko. Vse namestitve potrebne programske opreme, popravkov in vse spremembe nastavitev izvaja sektor za informatiko.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 6/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.6. Uporaba priponk

Pošiljanje in sprejemanje priponk v elektronskih sporočilih je dovoljeno, pri tem pa so uporabniki dolžni upoštevati naslednje omejitve:

1. Največja velikost priponke je omejena. Velikost priponk določa sektor za informatiko podjetja, skladno z razpoložljivimi strežniškimi kapacitetami in skladno z razpoložljivo pasovno širino internetne povezave.
2. Priponke z določenimi končnicami se iz varnostnih razlogov filtrirajo. Takšnih priponk ni mogoče pošiljati in/ ali sprejemati, zaradi potencialne nevarnosti okužbe z virusi oz. drugimi programi, ki bi lahko škodili računalniškemu sistemu podjetja.
3. Priponke se pred prejemom in/ ali pošiljanjem avtomatsko preverjajo pred zlonamerno programsko kodo.

Ni dovoljeno razpošiljati elektronska sporočila s sumljivo vsebino oz. takšna, za katera je že na prvi pogled očitno, da lahko kakorkoli ogrozijo varnost računalniškega sistema. Prav tako je nepooblaščenim osebam izrecno prepovedano razpošiljanje elektronskih sporočil s priponkami, ki vsebujejo dokumente ali podatke, ki so poslovna skrivnost (npr. osebni podatki po ZVOP-u).

4.7. Prepovedana uporaba

Uporabnikom je prepovedano uporabljati elektronsko pošto za:

1. Kakršenkoli napad na osebnost naslovnika (žalitve, grožnje, nasilno vedenje, ipd.);
2. Izmenjavo vsebin povezanih s spolnostjo, vsebin teroristične ali vohunske narave ter vsebin, povezanih s krajo in drogami;
3. Posredovanje verižnih sporočil;
4. Podpiranje rasne, spolne, nacionalne, verske, starostne diskriminacije ali diskriminacije oseb s posebnimi potrebami (izražanje žaljivih in grozečih izjav ali uporaba takega jezika, vključno z izjavami, ki merijo na rasno, versko, nacionalno pripadnost, spolno orientacijo, starost in telesne pomanjkljivosti posameznikov);
5. Versko ali politično propagando;
6. Oglaševanje izdelkov ali storitev v osebni interesu;
7. Razpošiljanje neželenih sporočil (SPAM-a);
8. Sodelovanje v igrah na srečo;
9. Osebno finančno okoriščenje;
10. Posredovanje osebnih podatkov nepooblaščenim uporabnikom ali tretjim osebam;
11. Nepooblaščen posredovanje poslovno občutljivih in tajnih podatkov ter informacij;
12. Omalovaževanje podjetja in njegovih uslužbencev;
13. Razpošiljanje materialov, ki so avtorsko ali intelektualno zaščiteni, vključno s članki in programsko opremo, avdio-vizualne vsebine ipd..;
14. Pošiljanje, prejemanje, tiskanje ali drugačno širjenje podatkov, ki so last podjetja, poslovnih skrivnosti ali drugih zaupnih informacij, kar predstavlja kršenje politik podjetja ali drugih pisnih dogovorov;
15. Vodenje lastnega podjetja, prevzemanje poslovnih priložnosti, pridobivanje denarja za lastne potrebe ali iskanje novega delovnega mesta;
16. Neetične aktivnosti ali vsebine, ki lahko očrnijo profesionalni ugled podjetja;

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 7/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

17. Kakršnekoli druge nezakonite dejavnosti.

Ugotovitev katerekoli od zgoraj navedenih prepovedanih aktivnosti, pomeni podlago za uvedbo nadzora nad elektronsko pošto zaposlenega s strani odgovornih oseb v Mariborskem vodovodu. O nadzoru so skladno z določili te politike uporabniki v podjetju vnaprej pisno obveščeni.

Uporaba elektronske pošte za namene, ki so v nasprotju s poslovnimi interesi podjetja, ali kršijo predpise o zaupnosti informacij, je izrecno prepovedana.

Prepovedano je pošiljanje informacij z oznako »zaupno« in »strogo zaupno«, izven podjetja, če dostop do njih ni zaščiten z zadostno stopnjo enkripcije (šifriranja).

4.8. Zaščita in varovanje elektronske pošte

Na poštnem strežniku se elektronska pošta pregleduje izključno s programsko opremo za odkrivanje zlonamerne programske kode, prav tako pa se izvaja odstranjevanje izvršljivih in ostalih nevarnih datotek, ki so bile del sporočila (npr. v obliki priponk).

Na poštnem strežniku se izvaja zaščita pred neželenimi elektronskimi sporočili (antispam), ki omejuje pretok (označevanje, filtracija in blokiranje) takšnih sporočil do uporabnikov elektronske pošte.

Arhiviranje (varnostno kopiranje) vsebine poštnih predalov se izvaja dnevno, samodejno na medije za shranjevanje podatkov. Pooblastila za dostop do prostorov in do podatkov so omejena.

Vsak uporabnik elektronskega poštnega nabiralnika je dolžan sproti urejati svojo pošto korespondenco.

4.9. Velikost poštnega nabiralnika (mailboxa)

Velikost poštnega nabiralnika določa sektor za informatiko glede na zahteve uporabnika in skladno z zmogljivimi - razpoložljivimi strežniškimi kapacitetami.

V kolikor je velikost obstoječega nabiralnika za posameznega uporabnika premajhna in zaradi tega prihaja do težav pri prejemu sporočil, je ta dolžan s pisno utemeljitvijo o tem zakaj je prišlo do prezasedenosti poštnega predala nemudoma obvestiti sektor za informatiko.

4.10. Nadzor nad elektronsko pošto

Mariborski vodovod se zavezuje, da bo pri nadzoru nad uporabo sredstev informacijske tehnologije (in tako tudi interneta, elektronska pošte) upoštevala načela sorazmernosti, zakonitosti in ustavne dopustnosti.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 8/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.10.1. Nadzor nad vsebino službenih elektronskih poštinih sporočil

Mariborski vodovod si zaradi organizacije dela pridružuje pravico, da pregleda vso službeno korespondenco oz. komunikacijo uporabnikov prek elektronske pošte, če je to potrebno, za kar pričakuje privolitev uporabnika. To nikakor ne velja za zasebno korespondenco, shranjeno v mapi »ZASEBNO«. Podjetje si ob tem pridružuje tudi pravico vpogleda v elektronska sporočila, ki so bila že izbrisana (s strani pošiljatelja ali naslovnika).

Mariborski vodovod o možnosti vpogleda elektronskih sporočil in datotek službene narave uporabnike pisno obvesti pred začetkom takšnega nadzora. Z obvestilom jih seznani kdaj in v kakšnih primerih bo nadzorovala elektronska sporočila in datoteke službene narave.

Razlogi za nadzor morajo biti utemeljeni. Na primer, izgubljena korespondenca, obremenjevanje omrežja zaradi posredovanja večje količine podatkov, negativni odzivi tretjih oseb na sporočila poslana s strani uporabnikov, počasno ali kakorkoli drugače ovirano delovanje omrežja zaradi pošiljanja slikovnih ali zvočnih datotek, povečano število virusov, odtekanje podatkov zaupne narave, ugotovitev drugih prepovedanih aktivnosti, navedenih v tej politiki.

Dostop do službenih elektronskih sporočil je mogoč po sklepu direktorja podjetja, s katerim se določi posameznika(e), katerega korespondenca bo pregledana in komisijo, ki bo prisotna pri takšnem nadzoru.

Komisija je sestavljena iz treh oseb:

1. oseba, ki je dala navodilo za pregled v elektronsko pošto uporabnika (vodja področja ali direktor)
2. oseba iz IT področja, ki je pooblaščen za tehnično omogočanje pregleda
3. oseba s statusom priče (ki ni nujno delavec, na katerega se pregled nanaša)

Samo tako sestavljena komisija sme dostopati do posameznih uporabniških poštinih predalov oz. opraviti vpogled v vsebino ali/ in izpis vsebine ustreznih uporabniških poštinih predalov. O opravljenem komisijskem pregledu se sestavi zapisnik, ki ga podpišejo vsi prisotni.

Mariborski vodovod se zavezuje, da bo pri nadzoru nad uporabo sredstev informacijske tehnologije – elektronske pošte upošteval načela sorazmernosti, zakonitosti in ustavne dopustnosti.

Mariborski vodovod lahko razkrije tekstovni ali slikovni material službene narave uradnim organom ali drugim tretjim osebam, ki imajo za to pooblastilo v zakonu ali v odredbi sodišča, brez pristanka uporabnika, prav tako pa ga o takšnem razkritju ni dolžna obvestiti.

4.10.2. Vpogled v službene e- poštne predale za namene vzdrževanja

Zapisano v točki 4.10.1 pa ne velja v celoti za izredno vzdrževanje poštinih predalov s strani pooblaščenih oseb v Sektorju za informatiko, ki so pri opravljanju svojih delovnih obveznosti dolžni skrbeti za nemoteno delovanje poštnega sistema.

Ti smejo vpogledati v poštne predale uporabnikov izključno za namene vzdrževanja poštnega sistema, ko je takšna intervencija nujna za zagotavljanje nemotene delovanja informacijskega sistema. Za tovrstne vpogleds nista potrebna sklep direktorja podjetja in sklic komisije iz prejšnje točke.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 9/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Razloge za vsako posamezno intervencijo, ki vključuje tudi vpogled v poštni predal posameznega ali več uporabnikov, so dolžni zabeležiti v dnevnik, kakor tudi datum vpogleda ter ime in priimek uporabnika, v čigar poštni predal so pri takšni intervenciji vpogledali, ter pisno obvestiti direktorja podjetja.

Za vse ostalo se uporabljajo določila točke 4.10.1.

4.10.3. Nadzor nad zasebno elektronsko pošto

Mariborski vodovod v nobenem primeru ne bo nadzoroval vsebine elektronskih sporočil in datotek (priponk), ki so zasebne narave (mapa ZASEBNO) in jih posamezni uporabniki službene strojne opreme in interneta skladno s to politiko in v omejenem obsegu prejemajo in/ali pošiljajo v delovnem času prek službenega elektronskega naslova ali svojih elektronskih naslovov komercialnih ponudnikov (npr. gmail, yahoo, hotmail, idr.).

V primeru, da podjetje utemeljeno sumi, da v delovnem času posamezni uporabnik službene strojne opreme in interneta prek svojega zasebnega elektronskega naslova s službene strojne opreme nepooblaščen pošilja zunanjemu ali notranjemu naslovniku poslovne skrivnosti ali druge zaupne podatke podjetja, si ta pridržuje pravico, da s tehničnimi sredstvi takšnemu posamezniku začasno omeji uporabo storitev komercialnih ponudnikov elektronske pošte na službeni strojni opremi.

4.10.4. Nadzor nad službeno elektronsko pošto, ki se izmenjuje preko »info« poštnega predala

Mariborski vodovod lahko kadarkoli, brez vnaprejšnjega opozorila pregleda splošne, univerzalne e- poštne predale (npr. info@mb-vodovod.si, it.podpora@mb-vodovod.si in podobne), ki niso vezani na posameznega uporabnika sistema elektronske pošte podjetja in so namenjeni predvsem komuniciranju z njenimi strankami ali partnerji o splošnih zadevah in ponavadi služijo prvemu kontaktu podjetja z njimi.

4.11. Pravno obvestilo – izjava o omejitvi odgovornosti

Vsa izhodna elektronska sporočila, ki jih uporabniki sistema elektronske pošte pošiljajo naslovnikom, so samodejno opremljena s pravnim obvestilom, ki naslovnika opozarja na to, da bo njegov odgovor na prejeto elektronsko sporočilo, v skladu s to politiko, obravnavan kot službena korespondenca, ki bo lahko podvržena tudi pregledu s strani pooblaščenih oseb podjetja v primerih, določenih s to politiko. Obvestilo vsebuje tudi opozorilo naslovnika o tem, da glede vsebine poslanega elektronskega sporočila ne more pričakovati tolikšne ravni zasebnosti, kot če bi pošiljatelju poslal elektronsko sporočilo na njegov zasebni elektronski naslov komercialnega ponudnika (npr. gmail, yahoo, hotmail, idr.).

Besedilo pravnega obvestila, ki se samodejno vključi v elektronska sporočila, ki jih uporabniki pošiljajo naslovnikom je v slovenskem in angleškem jeziku – priloga politike.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 10/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

5. UVELJAVLJANJE POLITIKE

Vsi uporabniki elektronskega poštne sistema Mariborskega vodovoda so odgovorni za izvajanje določil te politike.

Vsak uporabnik, ki ugotovi kršitev te politike, je dolžan o tem obvestiti svojega nadrejenega in/ali vodstvo sektorja za informatiko.

Če uporabnik krši določila te politike ali nepravilno uporablja elektronsko pošto, je njegovo ravnanje lahko predmet disciplinskih postopkov, ki lahko vodijo tudi do prenehanja delovnega razmerja.

6. REFERENCE

- Uporabljena nadzorstva ISO/IEC 27001-2013 poglavja:
 - A.7.2.2 Ozaveščenost...
 - A.8.1.3 Sprejemljiva uporaba dobrin
 - A.13.2 Prenos informacij
 - A.13.1.2 Varovanje omrežnih storitev
- Nadzor in zasebnost v informacijski družini, Matej Kovačič, FDV 2006, poglavje: Zasebnost na delovnem mestu.
- Izjava o omejitvi odgovornosti

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VP_04_03_P olitika elektronske pošte	VP_09_02_ElektronskaPo sta.doc	Pripravil: Bojan Erker
2		Dodane spr.		Dodal:
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE ELEKTRONSKE POŠTE	
	Oznaka: VP 09-02	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 11/11
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

8. PRILOGA

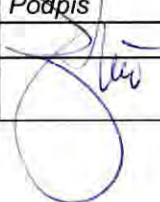
Izjava o omejitvi odgovornosti

Slovenska različica:

»Izjava o omejitvi odgovornosti. To elektronsko sporočilo in vse njegove morebitne priloge lahko vsebujejo zaupne in/ali privilegirane informacije in so last podjetja Mariborski vodovod d.d. ter namenjene izključno naslovniku. Če ste sporočilo prejeli pomotoma, Vas prosimo, da o tem obvestite pošiljatelja, sporočilo pa takoj uničite. Kakršnokoli nepooblaščenno razkritje, distribucija ali kopiranje vsebine sporočila je izrecno prepovedano. Mnenja vsebovana v tem elektronskem sporočilu ne odražajo nujno tudi stališča podjetja Mariborski vodovod j.p., d.d.. Elektronsko sporočilo je pregledano s protivirusnim programom. Odgovor na to elektronsko sporočilo, bo v skladu s politiko uporabe elektronske pošte v Mariborskem vodovodu d.d. obravnavan kot službena korespondenca in bo lahko podvržen pregledu s strani pooblaščenih oseb podjetja, v primerih in pod pogoji, določenimi s politiko.«

Angleška različica:

»Legal disclaimer statement. This e-mail and any attachments may contain confidential and/or privileged information and is a property of Mariborski vodovod j.p., d.d. and intended solely for the addressee. If you are not the intended recipient (or have received this e-mail by mistake), please notify the sender immediately and delete this e-mail. Any unauthorized reproduction, disclosure or distribution of the material in this e-mail is strictly forbidden. Opinions contained in this e-mail do not necessarily reflect the opinions of Mariborski vodovod j.p., d.d. This e-mail message is being scanned by Anti-Virus Software. In accordance to the company's e-mail usage policy, a reply to this e-mail will be treated as a business correspondence and may be, in certain cases, the object of inspection, done by the authorized persons within the Mariborski vodovod d.d. and under conditions, defined in the company's e-mail usage policy.«

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE INTERNETA	
	Oznaka: VP 09-03	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 1/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1. Splošne zahteve politike	2
4.2. Dovoljena uporaba internetnega dostopa (socialna omrežja)	3
4.3. Omejena zasebna raba internetnega dostopa	3
4.4. Raba tretjih oseb	3
4.5. Prepovedana uporaba internetnega dostopa	3
4.6. Odgovornost uporabnikov	4
4.7. Nadzor	5
5. UVELJAVLJANJE POLITIKE	5
6. REFERENCE	6
7. ZGODOVINA	6

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE INTERNETA	
	Oznaka: VP 09-03	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Internet je lahko učinkovito poslovno orodje, katerega uporaba pa je za podjetje lahko tudi tvegana. Ključni razlogi za skrbno rabo internet na delovnem mestu so:

- Zagotavljanje varnosti informacijskega sistema .
- Komunikacijske povezave predstavljajo realne stroške.
- Prekomerna raba znižuje produktivnost zaposlenih in učinkovitost dela.
- Neprimerna raba povzroča potencialne zakonske odgovornosti in negativno reklamo.
- Nepooblaščen dostop zunanjih uporabnikov lahko povzroči razkritje občutljivih podatkov, zakonsko odgovornost ali izgubo ugleda podjetja.

Namen te politike je določitev pravil za učinkovito in varno uporabo interneta v mariborskem vodovodu.

2. OBSEG

Politika določa smernice za uporabo interneta v Mariborskem vodovodu. Velja, za vse zaposlene, zunanje sodelavce in pogodbene partnerje, ki uporabljajo internetno povezavo podjetja (v nadaljevanju: uporabniki).

3. POJMI

- **Informacijska dobrina:** opredmeteno ali neopredmeteno (osnovno) sredstvo informacijske tehnologije (primer: računalnik, programska oprema, podatkovna baza, podatki, komunikacijska oprema, poljuben nosilec informacij...)
- **Uporabniki:** so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, tretje osebe in ostali delavci.
- **Dobavitelji:** pravne in fizične osebe, ki sodelujejo z Mariborskim vodovodom in imajo dostop do IT dobrin,
- **Lastnik:** izraz pomeni posameznika (uporabnika), ki mu je vodstvo odobrilo odgovornost za uporabo, nadzorovanje, razvoj, vzdrževanja in varovanje informacijske dobrine. Izraz "lastnik" ne pomeni, da ima ta oseba dejanske lastniške pravice v zvezi z tem informacijsko dobrino.

4. POLITIKA

4.1. Splošne zahteve politike

Mariborski vodovod v svojih prostorih in na svoji strojni ter programski opremi uporabnikom omogoča dostop do interneta.

Uporabniki lahko dostopajo do interneta tudi z mobilnih enot, katerih lastnik je Mariborski vodovod in ki se ne nahajajo nujno v prostorih podjetja.

Uporabniki lahko internet uporabljajo prvenstveno za izvrševanje nalog na delovnem mestu, za zasebne potrebe pa med delovnim časom le v omejenem obsegu in izključno v skladu s pravili te politike.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE INTERNETA	
	Oznaka: VP 09-03	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Pravila in dovoljeni obseg uporabe interneta za pogodbene partnerje morajo biti del pogodbe, ki jo ima partner z Mariborskim vodovodom.

Za občasne zunanje sodelavce (npr. študente) veljajo enaka pravila pri uporabi interneta kot za ostale uporabnike. V kolikor teh pravil ni mogoče zagotoviti, ti uporabniki ne smejo uporabljati interneta, oziroma polno odgovornost za uporabo prevzame vodja sektorja v katerem posamezni zunanji sodelavec dela.

4.2. Dovoljena uporaba internetnega dostopa (socialna omrežja)

- Dostop do informacij v spletu, ki ga uporabniki potrebujejo za svoje delo;
- Pošiljanje in prejemanje elektronske pošte;
- Komunikacija z ostalimi zaposlenimi podjetja, z javnimi organi (občina, država) ali drugimi organizacijami, s katerimi Mariborski vodovod sodeluje;
- Prenos podatkov ali datotek s spleta, ki jih zaposleni potrebujejo pri svojem delu;
- Posredovanje datotek, podatkov, elektronskih dokumentov zunanjim uporabnikom, s katerimi Mariborski vodovod sodeluje ali ki so od podjetja upravičeni zahtevati nekatere podatke ali dokumente;
- Izobraževanje in izpopolnjevanje uporabnikov, če je le- to v interesu in v korist podjetja.

4.3. Omejena zasebna raba internetnega dostopa

Internetni dostop, ki ga Mariborski vodovod zagotavlja svojim zaposlenim na delovnem mestu, je namenjen prvenstveno službeni uporabi.

Občasna uporaba interneta za zasebne namene je dovoljena v omejenem obsegu, v razumnih mejah in če ni moteča pri izvajanju delovnih nalog in odgovornosti posameznega zaposlenega in njegovih sodelavcev.

4.4. Raba tretjih oseb

Pogodbeni delavci in drugi partnerji smejo uporabljati internet podjetja, samo če so za to avtorizirani z razlogom, da je taka raba potrebna za doseg pričakovanih rezultatov njihovega dela v podjetju. Vsak tak uporabnik mora biti seznanjen in mora delovati skladno s to politiko.

4.5. Prepovedana uporaba internetnega dostopa

Uporabniki na delovnem mestu ne smejo uporabljati internetnega dostopa za pregledovanje, prenos (download), hranjenje ali posredovanje naslednjih materialov in vsebin:

1. Izmenjavo vsebin povezanih s spolnostjo ali vsebin teroristične, vohunske narave ter vsebin povezanih s krajo in drogami.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE INTERNETA	
	Oznaka: VP 09-03	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

2. Posredovanje verižnih ali drugih neželenih e- sporočil (SPAM-a).
3. Širjenje rasne, spolne, nacionalne, verske, starostne diskriminacije ali diskriminacije oseb s posebnimi potrebami. Prepovedano je izražanje žaljivih in grozečih izjav ali uporaba takega jezika, vključno z izjavami, ki merijo na rasno, versko, nacionalno pripadnost, spolno orientacijo, starost in telesne pomanjkljivosti posameznikov.
4. Verska ali politična propaganda.
5. Oglaševanje izdelkov ali storitev v osebni interesu.
6. Sodelovanje v igrah na srečo.
7. Osebno finančno okoriščenje.
8. Posredovanje osebnih podatkov nepooblaščenim uporabnikom ali tretjim osebam.
9. Nepooblaščen posredovanje poslovno občutljivih in tajnih podatkov ter informacij.
10. Omalovaževanje Mariborskega vodovoda in njenih uslužbencev.
11. Prenos programske opreme ali njenih delov brez dovoljenja skrbnika sistema.
12. Prenos materialov, ki so avtorsko zaščiteni, patentirani ali druge intelektualne lastnine vključno s članki, programsko opremo, avdio-vizualne vsebine, ipd...
13. Pošiljanje, prejemanje, tiskanje ali drugačno širjenje podatkov, ki so last Mariborskega vodovoda, poslovnih skrivnosti ali drugih zaupnih informacij, kar predstavlja kršenje politike podjetja ali drugih pisnih dogovorov.
14. Vodenje lastnega podjetja, prevzemanje poslovnih priložnosti, pridobivanje denarja za lastne potrebe ali iskanje novega delovnega mesta.
15. Neetične aktivnosti ali vsebine, ki lahko očrni profesionalni ugled podjetja.
16. Kakršnekoli druge nezakonite dejavnosti.

Ugotovitev katerekoli od zgoraj navedenih prepovedanih aktivnosti, pomeni podlago za uvedbo nadzora nad uporabo interneta zaposlenega s strani odgovornih oseb v podjetju. O nadzoru so skladno z določili te politike zaposleni v Mariborskem vodovodu vnaprej pisno obveščeni.

Podjetje si pridržuje pravico blokade dostopa do določenih spletnih strani, če bi bilo to potrebno za zagotovitev učinkovitejšega delovnega procesa, varnosti informacijskega sistema ter zaščite pravic uporabnikov interneta.

4.6. Odgovornost uporabnikov

- Uporabniki interneta v Mariborskem vodovodu so dolžni spoštovati in upoštevati določila te politike in z njo povezanih politik.
- Uporabniki interneta v Mariborskem vodovodu so dolžni poskrbeti za minimiziranje nepotrebnega omrežnega prometa, ki ovira ostale zaposlene pri učinkoviti uporabi omrežja.
- Uporabniki interneta v Mariborskem vodovodu ne smejo preobremenjevati računalniškega omrežja s prekomerno količino podatkov, ki bi jih bilo sicer mogoče prenašati s pomočjo druge, primernejše opreme (optičnih medijev, prenosnih trdih diskov, ipd.).
- Uporabniki interneta v Mariborskem vodovodu morajo s tehnično opremo ravnati pazljivo, skladno z uporabniško tehnično dokumentacijo, politiko primerne rabe informacijske tehnologije ter v skladu z navodili in napotki pooblaščenih oseb v sektorju za informatiko.

V primeru vprašanj se uporabniki lahko obrnejo na »Help desk« na int. telefon 261 ali na elektronski naslov it.podpora@mb-vodovod.si !

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE INTERNETA	
	Oznaka: VP 09-03	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 5/6
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.7. Nadzor

Mariborski vodovod razpolaga z tehnično opremo za zaščito uporabnikov in podjetja pred okužbami, krajo podatkov, krajo identitete, spletnimi goljufijami, itd. Tehnična oprema beleži tudi vse dostope do internetnih strani in spletnih storitev. Beleženje sledljivosti je namenjena izključno vzdrževanju, zagotavljanju zaščite uporabnika in podjetja, ter zagotavljanje zakonitosti delovanja.

Tehnična oprema nikakor ni namenjena nadzoru posameznega uporabnika, vendar si podjetje pridržuje pravico, da v izjemnih okoliščinah, ko smatra, da je ogrožena njena integriteta ali integriteta uporabnikov dostopa do podatkov o sledljivosti.

Mariborski vodovod se zavezuje, da bo pri nadzoru nad uporabo sredstev informacijske tehnologije - interneta upošteval načela sorazmernosti, zakonitosti in ustavne dopustnosti.

V kolikor smatra, da je potreben nadzor nad sledljivimi podatki posameznega uporabnika ga o tem obvesti in pričakuje njegovo privolitvev.

Dostop do sledljivih podatkov o posameznem uporabniku je mogoč po sklepu direktorja, s katerim se določi utemeljen razlog nadzora in uporabnik, ki bo predmet nadzora ter komisijo, ki bo prisotna pri takšnem nadzoru.

Komisija je sestavljena iz treh oseb:
predlagatelj iz Sektorja za informacijsko tehnologijo,
oseba, ki je nadrejena posameznemu uporabniku (direktor, vodja sektorja ali član vodstva),
oseba s statusom prič (ki ni nujno delavec, na katerega se pregled nanaša).

Samo tako sestavljena komisija sme izvajati nadzor nad sledljivimi podatki uporabnika posameznika. O opravljenem komisijskem pregledu se sestavi zapisnik, ki ga podpišejo vsi prisotni.

Podjetje Mariborski vodovod nikakor ne bo dostopala do vsebine podatkov shranjenih na osebem računalniku posameznega uporabnika, ki so zasebne narave, shranjeni v mapi »ZASEBNO«.

Mariborski vodovod lahko razkrije beležene podatke uradnim organom ali drugim tretjim osebam, ki imajo za to pooblastilo v zakonu ali v odredbi sodišča, brez pristanka uporabnika, prav tako pa ga o takšnem razkritju ni dolžna obvestiti.

5. UVELJAVLJANJE POLITIKE

Vsi zaposleni in drugi uporabniki interneta v Mariborskem vodovodu so odgovorni za izvajanje določil te politike.

Vsak uporabnik interneta in drug zaposleni, ki ugotovi kršitev te politike, je dolžan o tem obvestiti svojega nadrejenega in/ali sektor za informatiko Mariborskega vodovoda.

	VARNOSTNA POLITIKA	
	POLITIKA UPORABE INTERNETA	
	Oznaka: VP 09-03	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 6/6
Datum zadnje revizije: 02.12.2019		Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Če uporabnik interneta krši določila te politike ali nepravilno uporablja internet, bo njegovo ravnanje predmet disciplinskih postopkov, ki lahko vodijo tudi do prenehanja delovnega razmerja oz. pogodbe o sodelovanju.

Tretje osebe, ki kršijo to politiko so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

Uporabljena nadzorstva ISO/IEC 27001-2013:

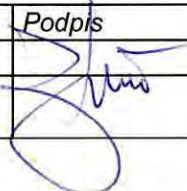
A.7.2.2 Ozaveščenost...

A.8.1.3 Sprejemljiva uporaba dobrin

A.13.1.2 Varovanje omrežnih storitev

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VP_04_02_U poraba Interneta	VP_09_03_UporabaInterneta.doc	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	

	VARNOSTNA POLITIKA	
	POLITIKA VARNEGA E-POSLOVANJA	
	Oznaka: VP 09-04	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 1/6
	Datum zadnje revizije: 12-2019	Datum nove revizije: 2020

Klasifikacija: **INTERNO**

Vsebina:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1 Obveznosti uporabnikov	2
4.1.1. Internet	3
4.1.2 Uporaba digitalnih potrdil (certifikatov)	3
4.1.3 Elektronska pošta	3
4.1.4 Prenos datotek preko protokola FTP	4
4.1.5 Družabna omrežja	4
4.1.6 Storitve v oblaku	4
4.1.7 Varnost telefonskih pogovorov	4
4.1.8 Varnost pri (video)konferenčnih klicih	4
4.1.9 Varno rokovanje s faks napravami	5
4.2 Odgovornost Službe za informatiko	5
5. UVELJAVLJANJE POLITIKE	6
6. REFERENCE	6
7. ZGODOVINA	6

	VARNOSTNA POLITIKA	
	POLITIKA VARNEGA E-POSLOVANJA	
	Oznaka: VP 09-04	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/6
	Datum zadnje revizije: 12-2019	Datum nove revizije: 2020

Klasifikacija: **INTERNO**

1. NAMEN

Politika varnega e-poslovanja je namenjena varovanju poslovno občutljivih informacij pri izvajanju poslovnih procesov preko interneta in komunikacij z ostalimi udeleženci.

Cilj politike je zagotavljanje zaupnosti in neoporečnosti nejavnih, to je vseh poslovno občutljivih informacij.

2. OBSEG

S politiko so seznanjeni vsi uporabniki informacijskega sistema podjetja Mariborski vodovod d.d., ki pri svojem delu uporabljajo internet in druge komunikacije za izvajanje poslovnih procesov, kakor tudi tehnično osebje v Službi informatike.

3. POJMI

- **E- poslovanje:** izvajanje poslovnih procesov preko interneta in drugih komunikacij
- **Ostali udeleženci:** javne in državne institucije, zasebni ponudniki storitev ter ostale pravne in fizične osebe.
- **Poslovno občutljive informacije:** so vse informacije, ki niso označene kot javne. Gre za interne in zaupne informacije podjetja, **ter osebne podatke**.
- **Spletni brskalnik:** programi kot Internet Explorer, MS Edge, Chrome, Opera...

4. POLITIKA

4.1 Obveznosti uporabnikov

Pred pošiljanjem občutljivih informacij mora biti uporabnik prepričan, da je prejemnik pooblaščen za prejem takšnih informacij.

V kolikor je prejemnik informacij pravna oseba, s katero ima podjetje Mariborski vodovod sklenjeno naročilnico in/ali pogodbo o poslovnem sodelovanju je potrebno upoštevati tudi politiko *VP 02-01 Politika do tretjih oseb*.

Pred pošiljanjem se uporabnik prepriča v avtentičnost prejemnika informacij:

- Avtentičnost spletnih strani je razvidna ob vzpostavitvi varne povezave (<https://>) – strežniški javni ključ.
- Avtentičnost poštnega predala je na prvi pogled razvidna iz naziva (ime, priimek, funkcija) in domene (podjetje) elektronske pošte ime.priimek@podjetje.si. V kolikor uporabnik prvič posluje s tem udeležencem se priporoča vzpostavitev telefonskega kontakta. Pošiljanje informacij na elektronske naslove zasebnih ponudnikov (gmail, hotmail,...) predstavlja varnostno tveganje in se odsvetuje brez predhodnega posvetovanja.

Uporabnik lahko poslovno občutljive informacije posreduje samo na varen komunikacijski način!

	VARNOSTNA POLITIKA	
	POLITIKA VARNEGA E-POSLOVANJA	
	Oznaka: VP 09-04	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/6
	Datum zadnje revizije: 12-2019	Datum nove revizije: 2020

Klasifikacija: **INTERNO**

4.1.1. Internet

Na spletu (www) se lahko izvede varna prijava z uporabniškim imenom in geslom, šele če je zagotovljena varna (s-ang. *secure*) povezava <https://www.primer.si>.

Uporabnik sme vnašati poslovno občutljive informacije v spletno aplikacijo v kolikor je vzpostavljena varna povezava https ves čas.

Glej tudi VP 04-02 Politika uporabe interneta.

4.1.2 Uporaba digitalnih potrdil (certifikatov)

Nekatere spletne storitve (državne institucije, agencije, banke,...) omogočajo višji nivo varovanja dostopa in zaupnosti ter neoporečnosti prenosa informacij ob pomoči t.i. asimetrične kriptografije. Dostop do teh storitev je mogoč le ob uporabi digitalnega potrdila, ki ga je izdala zaupanja vredna certifikatska agencija (SigenCa, PoštarCa, Halcom CA, NLB CA, ..., tuje agencije).

- V kolikor je digitalno potrdilo izdano osebno na zaposlenega, tega potrdila ne smejo uporabljati druge osebe (Zakon o elektronskem poslovanju in elektronskem podpisu: "elektronskemu podpisu priznava enako veljavo, kot jo ima v papirnatem svetu lastnoročni podpis").
- V kolikor več oseb potrebuje dostop do iste storitve z digitalnim potrdilom mora imeti vsak uporabnik svoje potrdilo.
- Digitalno potrdilo s uporabnikovim zasebnim ključem se namesti ob pomoči tehničnega osebja Službe informatike
- Uporabnikom se odsvetuje izvažanje digitalnih potrdil in izdelava kopij le the. Služba informatike skrbi za varne kopije digitalnih potrdil.

Glej tudi VP 06-05 Politika kriptografije

4.1.3 Elektronska pošta

Elektronska pošta znotraj domene družbe, t.j. med naslovi @mb-vodovod se smatra kot "varna" elektronska pošta, saj se usmerja znotraj varovanega omrežja.

Uporabnik se mora zavedati, da elektronska pošta na ostale naslove izven podjetja **ne velja za varno** povezavo. V kolikor se posredujejo poslovno občutljive informacije na naslove izven podjetja, je to dovoljeno le ob uporabi dodatnih mehanizmov varovanja. Uporabnik naj se za pomoč obrne na it.podpora@mb-vodovod.si.

Uporabnikom se pri pošiljanju poslovno občutljivih informacij priporoča posebna pazljivost pri vpisovanju elektronskih naslovov in dodatno preverjanje vpisanega naslova pred pošiljanjem.

Uporabniki smejo uporabljati elektronsko pošto skladno s politiko VP 04-03 Politika elektronske pošte.

	VARNOSTNA POLITIKA	
	POLITIKA VARNEGA E-POSLOVANJA	
	Oznaka: VP 09-04	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/6
	Datum zadnje revizije: 12-2019	Datum nove revizije: 2020

Klasifikacija: **INTERNO**

4.1.4 Prenos datotek preko protokola FTP

Za vzpostavitev varnega prenosa poslovno občutljivih datotek (*ang. (Secure) File Transfer Protocol*) poskrbi in jo odobri Služba informatike.

Uporabnikom je prepovedana samodejna vzpostavitev FTP povezav za prenos občutljivih informacij, v kolikor ni odobrena s strani Služba informatike in je vpisana v spisek varnih povezav, ki je priloga tega dokumenta.

4.1.5 Družabna omrežja

Uporaba družabnih omrežij je dovoljena samo ob odobritvi vodstva in se lahko uporablja le v poslovne namene (npr. za predstavitev dejavnosti podjetja, komunikacijo z uporabniki storitev itd.). Uporaba javnih podatkov na družabnih omrežjih je dovoljena skrbnikom, ki skrbijo za uradne profile podjetja.

Uporaba poslovno občutljivih informacij na družabnih omrežjih (Facebook, LinkedIn, Google+, Xing, SnapChat,... ipd.) je v popolnosti prepovedana! Prav tako je prepovedana uporaba na družabnih omrežjih znotraj posameznih zaprtih skupin!

Posebno previdnost priporočamo uporabnikom, ki zasebno sodelujejo v družabnih omrežjih ob tem pa navajajo organizacijo, kjer so zaposleni in vlogo znotraj nje. Tak uporabnik je lahko posredna tarča z namenom zlorabe informacij podjetja Mariborski vodovod.

Uporabnikom se svetuje posebna previdnost pri uporabi javnih podatkov o podjetju na družabnih omrežjih, saj obstaja tveganje, da uporabnik nehoti objavi tudi občutljive podatke.

4.1.6 Storitve v oblaku

Uporaba poslovno občutljivih podatkov v oblčnih storitvah elektronske pošte, hrambe podatkov (Google email in Drive, Apple mail in iCloud, Dropbox, Microsoft 365 in OneDrive, SkyDrive, ZOHO,... ipd) je prepovedana v kolikor ni izrecno dovoljena in dodana na spisek v prilogi.

4.1.7 Varnost telefonskih pogovorov

Sogovornik mora biti identificiran, pooblaščen in opozorjen za sprejem poslovno občutljivih informacij. V kolikor sogovornika ni mogoče ustrezno identificirati (prepoznati), se poslovno občutljivih informacij ne sme razkriti!

Sodelujoča se morata zavedati, da telefon (govor preko klasičnega telefona, govor preko gsm in sms) ni primeren način komunikacije za poslovno občutljive informacije, saj je zaupnost informacij vprašljiva.

4.1.8 Varnost pri (video)konferenčnih klicih

Vsi sodelujoči v konferenčnih in videokonferenčnih klicih morajo biti pooblaščen in opozorjeni za sprejem poslovno občutljivih informacij.

- Če potrditev identitete ni možna lahko pride do zlorabe poslovno občutljivih informacij!

	VARNOSTNA POLITIKA	
	POLITIKA VARNEGA E-POSLOVANJA	
	Oznaka: VP 09-04	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 5/6
	Datum zadnje revizije: 12-2019	Datum nove revizije: 2020

Klasifikacija: **INTERNO**

- Sodelujoči so vnaprej obveščeni o poslovni občutljivosti informacij.
- Konference se lahko zaradi sledljivosti snemajo in/ali se vodi ustrezen zapisnik.
- Komunikacijski kanal video-konferenčnih klicov mora biti ustrezno tehnično varovan.

4.1.9 Varno rokovanje s faks napravami

Pošiljanje faks

Faks se ne smatra kot varen način prenosa za poslovno občutljive informacije. V kolikor je pošiljanje neizogibno se izvajajo sledeči ukrepi:

- Prejemnik mora biti identificiran, pooblaščen in opozorjen za sprejem poslovno občutljivih informacij.
- Preverjanje prisotnosti prejemnika faksa ob napravi po telefonu je nujno preden se pošlje faks.
- Faks mora biti označen z oznako zaupnosti.
- Zahteva se večkratno preverjanje pravilnosti telefonske številke pred pošiljanjem, da se prepreči zmotna napačnega usmerjanja in potencialnega razkritja.
- Pošiljanje se izvaja z obvezno zahtevano potrditvijo uspešnosti prenosa.
- Original se po pošiljanju nemudoma odstrani in hrani na varno mesto oz. uniči.

Prejemanje faks

- Nepričakovani faksi se obravnavajo previdno, dokler ni potrjena identiteta pošiljatelja.
- V primeru prejema poslovno občutljivih podatkov je potrebno takšen dokument dostaviti navedenemu prejemniku na varen način.
- Nezaželeni faksi (ang. "junk", reklame) so pogosti, vsebina se prezre. Pošiljatelja se ne obvešča, saj gre morda za t.i. "sondiranje" – preverjanje informacijskih lukenj.
- V kolikor je prišlo do napačnega usmerjanja in uporabnik ni pooblaščen prejemnik faksa se obvesti pošiljatelja, dokument pa se varno uniči.

V kolikor je uporabnik v kakršnem koli dvomu glede posredovanja poslovno občutljivih informacij, avtentičnosti prejemnika, vzpostavitvi varne povezave ali ima druga vprašanja, se naj obrne na podporo uporabnikom tel. int. 261 ali na elektronski naslov it.podpora@mb-vodovod.si, preden posreduje občutljive informacije!

4.2 Odgovornost Službe za informatiko

Tehnično osebje Službe informatike skrbi za učinkovito podporo uporabnikom pri zagotavljanju varnega e-poslovanja.

Služba v rednih časovnih intervalih 2 x letno preverja varnost elektronskih povezav uporabnikov in skrbi za ažurnost spiska, ki je priloga te politike. Služba za informatiko v ta namen pošilja ostalim službam vprašalnik, ki ga le te ustrezno dopolnijo.

Tehnično osebje Službe za informatiko lahko izvaja praktična testiranja ustreznosti spletnih komunikacij.

Služba skrbi, da imajo uporabniki na voljo varne in posodobljene spletne brskalnike in poskrbi za ustrezno zaščito v spletnih brskalnikih pred zlonamerno mobilno in aktivno kodo.

	VARNOSTNA POLITIKA	
	POLITIKA VARNEGA E-POSLOVANJA	
	Oznaka: VP 09-04	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 6/6
Datum zadnje revizije: 12-2019		Datum nove revizije: 2020

Klasifikacija: **INTERNO**

5. UVELJAVLJANJE POLITIKE

Vsi zaposleni in drugi uporabniki informacijske tehnologije Mariborskega vodovoda so odgovorni za izvajanje določil te politike.

Vsak zaposleni, ki ugotovi kršitev te politike, je dolžan o tem obvestiti Službo za informatiko Mariborskega vodovoda.

Če zaposleni krši določila te politike glede varovanja gesel, bo njegovo ravnanje predmet disciplinskih postopkov, ki lahko vodijo tudi do prenehanja delovnega razmerja.

6. REFERENCE

- ISO/IEC 27001 poglavja:
A.13.2 Prenosi informacij
- Politika se sklicuje tudi na:
VP 09-03 Politika uporabe interneta
VP 09-02 Politika elektronske pošte
VP 06-01 Politika kriptografije
VP 11-01 Odnosi z dobavitelji.
- Spisek varnih elektronskih povezav

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	15.06.2018	Dodane spr.		Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2015	

	VARNOSTNA POLITIKA	
	POLITIKA RAZVOJA IN VZDRŽEVANJA SISTEMOV	
	Oznaka: VP 10-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 1/5
Datum zadnje revizije: 02.12.2019		Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA

1.	NAMEN	2
2.	OBSEG	2
3.	POJMI	2
4.	POLITIKA	2
4.1	Varna razvojna politika	2
4.2	Postopki nadzora sprememb sistemov	3
4.3	Spremembe programskih paketov in omejitve	3
4.4	Varno razvojo okolje	4
4.5	Zunanje izvajanje razvoja	4
5.	UVELJAVLJANJE POLITIKE	4
6.	REFERENCE	4
7.	ZGODOVINA	5

	VARNOSTNA POLITIKA	
	POLITIKA RAZVOJA IN VZDRŽEVANJA SISTEMOV	
	Oznaka: VP 10-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Politika razvoja in vzdrževanja sistemov zagotavlja informacijsko varnost v celotnem ciklu od načrtovanja do obratovanja posamezne rešitve znotraj informacijskega sistema podjetja Mariborski vodovod.

2. OBSEG

Politika je namenjena vsem zaposlenim, ki so vključeni v načrtovanje, razvoj in vzdrževanje programske opreme, ter nameščanje le te v produkcijsko okolje podjetja.

3. POJMI

- **Sistem** – naprava za procesiranje ali hranjenje podatkov (največkrat strežnik, fizični računalnik z nameščenim operacijskim sistemom, tudi logični ali virtualni računalnik, diskovno polje, idr.), ki vključuje tudi programsko opremo
- **Skrbnik:** (*ang. Administrator*) upravitelj informacijske dobrine s posebnimi pooblastili - vzdrževalec.
- **Produkcija informacijskega sistema:** se nanaša na informacijske dobrine (strežniki, ostala sistemska in aplikativna programska oprema,...), do katerih dostopajo končni uporabniki in na katerih tečejo »živi podatki«.

4. POLITIKA

4.1 Varna razvojna politika

S poslovnimi aplikacijami upravlja ustrezno usposobljeno in kvalificirano osebje – skrbniki. Vsi skrbniki se ustrezno usposablajo na temo informacijske varnosti.

Nabavo in implementacijo nove programske opreme ali nadgradnjo obstoječe je potrebno skrbno načrtovati, razvoj programskih rešitev znotraj družbe pa mora slediti formaliziranemu procesu.

Informacijska tveganja, povezana s takšnimi projekti, je moč omiliti s kombinacijo procesnih in tehničnih kontrol, ki jih je potrebno dokumentirati.

Nov sistem, ki ni ustrezno preizkušen, lahko povzroči večjo škodo na poslovnih procesih in podatkih, ki se sklicujejo nanj. Posebno pozornost je potrebno posvetiti funkcionalnemu testiranju.

Poslovne zahteve za novo programsko opremo ali nadgradnjo obstoječe programske opreme morajo ustrezati specifikaciji varnostnih zahtev. Posebno pozornost je potrebno posvetiti integracijskemu testiranju.

Podjetje ščiti testne načrte in podatke. V kolikor so testni podatki zaupne narave (**osebni podatki**), se poskrbi za anonimizacijo.

	VARNOSTNA POLITIKA	
	POLITIKA RAZVOJA IN VZDRŽEVANJA SISTEMOV	
	Oznaka: VP 10-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Nezadovoljivo usposobljeni tehnični sodelavci in uporabniki lahko povzročijo napake na podatkih in procesih, to pa lahko vpliva tudi na druge sisteme. Izjemnega pomena je izobraževanje tako skrbnikov sistemov kakor tudi končnih uporabnikov.

4.2 Postopki nadzora sprememb sistemov

Podjetje ima s vpeljanim projektnim vodenjem uveden postopek upravljanja sprememb razvoja lastne programske opreme in sistemov, ki zagotavlja sledljivost od uporabniških zahtev, preko razvoja sprememb in nadgradenj produkta, do vpeljave v produkcijo.

Upravljanje sprememb opredeljuje:

- Način podajanja zahteve in njene lastnosti.
- Vloge udeležencev in odgovornosti v posameznih fazah (Projektni odbor, Projektni manager, Projektni vodja, Izvajalci).
- Delovni tok razvojnega procesa po fazah:
 - Analiza,
 - Razvoj podatkovnega modela,
 - Razvoj aplikacije,
 - Testiranje (uporabniško, integracijsko),
 - Uporaba – produkcija.
- Dokumentiranje in sledljivost.

4.3 Spremembe programskih paketov in omejitve

Spremembe na kupljenih programskih paketih (sistemih) se odsvetujejo. Dopustne so samo strogo nadzorovane in načrtovane spremembe.

Spremembe na ponudnikovi programski opreme (sistemih) lahko privedejo do nepredvidljivih varnostnih težav, morda šele po nadgradnji na novo verzijo. Takšni sistemi so povezani z ostalimi poslovnimi aplikacijami, s katerimi si izmenjujejo informacije. Ti procesi lahko močno ogrozijo integriteto podatkov.

Ta varnostna politika opozarja na naslednje spremembe:

- Nakup novih sistemov, katerih povezljivost na obstoječe sisteme deluje navidezno enostavno, lahko sproži težave povezljivosti z obstoječimi sistemi. Le-to lahko vodi do večjih zakasnitev ali celo do odstopa od projekta predvsem tam, kjer so potrebne kompleksne podatkovne manipulacije.
- programski vmesnik, ki formatira podatke v obliko za ciljni sistem predstavlja veliko tveganje za točnost (integriteto) podatkov,
- Spremembe sistemske programske opreme (operacijski sistem, podporna in vmesna prog. oprema – ang. *middleware*) lahko bistveno vpliva na informacijsko varnost. *Glej politika VP 08-01 Politika varovanja operacij, točka 4.3,*
- začasne datoteke, ki jih kreira vmesnik in shranjuje na začasne lokacije (temporary location) lahko vsebujejo občutljive podatke in predstavljajo tveganje zaupnosti podatkov.

	VARNOSTNA POLITIKA	
	POLITIKA RAZVOJA IN VZDRŽEVANJA SISTEMOV	
	Oznaka: VP 10-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/5
Datum zadnje revizije: 02.12.2019		Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.4 Varno razvojno okolje

- Podjetje ima vzpostavljeno varno razvojno okolje za kritične sisteme. Razvojne, testne in produkcijske zmogljivosti kritičnih sistemov so ločene. Glej *politika VP 08-01 Politika varovanja operacij, točka 4.3.*
- Celoten življenski cikel razvoja je opredeljen s *Projektnim vodenjem v družbi*.
- Kritičnost sistemov je opredeljena *Klasifikacija kritičnih informacijskih sistemov v MV d.d.*

4.5 Zunanje izvajanje razvoja

Podjetje spremlja in nadzoruje zunanji razvoj. Testiranja in prehod v produkcijo potekajo enako, kakor za lastno razvito programsko opremo v skladu s to in ostalimi politikami.

Glej tudi *VP 11-01 Politika odnosov do dobaviteljev*.

5. UVELJAVLJANJE POLITIKE

Zaposleni službe za informatiko in ostali sodelavci, ki sodelujejo razvoju so odgovorni za izvajanje določil te politike.

V kolikor uporabnik krši določila te politike, bo njegovo ravnanje podvrženo ukrepom po Zakonu o delovnih razmerjih, ki lahko vodijo tudi do prenehanja delovnega razmerja.

Dobavitelji, ki kršijo to politiko, so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

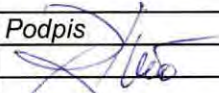
- ISO/IEC 27001-2013 poglavja:
 - A.14.1.1 Analiza in specifikacije informacijskih varnostnih zahtev
 - A.14.2 Varnost v procesih razvoja in podpore
 - A.14.3 Testni podatki
- Soodvisne politike:
 - VP 08-01 Politika varovanja operacij
 - VP 11-01 Politika odnosov z dobavitelji.
- Sistemski postopek: Klasifikacija kritičnih informacijskih sistemov v MV d.d.

	VARNOSTNA POLITIKA	
	POLITIKA RAZVOJA IN VZDRŽEVANJA SISTEMOV	
	Oznaka: VP 10-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 5/5
Datum zadnje revizije: 02.12.2019		Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	Apr.2018	Nova politika	VP_10_01_PolitikaRazvoj alnVzdrževanja.doc	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Erker
3		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3. 12. 2019.	

	VARNOSTNA POLITIKA	
	POLITIKA ODNOSA Z DOBAVITELJI	
	Oznaka: VP 11-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 1/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
5. UVELJAVLJANJE POLITIKE	3
6. REFERENCE	3
7. ZGODOVINA	4

	VARNOSTNA POLITIKA	
	POLITIKA ODNOSA Z DOBAVITELJI	
	Oznaka: VP 11-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 2/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Namen politike je ohranjanje varnosti informacijsko tehnoloških (v nadaljevanju IT) dobrin Mariborskega vodovoda, do katerih imajo dostop dobavitelji. Dostopnost IT dobrin s strani dobaviteljev mora biti nadzorovana. Tveganja dostopa do IT dobrin s strani dobaviteljev morajo biti ocenjena, implementirane pa morajo biti ustrezne varnostne kontrole.

Varnost IT sistemov v podjetju bi utegnila biti ogrožena v primeru dostopa s strani tretjih lokacij in neustreznem upravljanju varnosti. V kolikor obstaja poslovna potreba po takšnem povezovanju, se morajo analizirati tveganja glede na tip povezave, vrednost informacij, varnostnih zahtev do zaposlenih pri dobaviteljih in posledice dostopa za varnost IT infrastrukture.

Dostopa do IT dobrin s strani dobaviteljev se ne sme zagotoviti, dokler niso implementirani ustrezni protiukrepi in dokler ni podpisana pogodbeni zaveza.

2. OBSEG

Ta politika velja za vse dobavitelje - zunanje dobavitelja programske, strojne opreme in storitev, vse zunanje uporabnike IT storitev, ter skrbnike IT dobrin znotraj podjetja.

3. POJMI

- **Dobavitelji** – pravne in fizične osebe, ki sodelujejo z Mariborskim vodovodom in imajo dostop do IT dobrin
- **Outsourcing** – storitve v zunanjem izvajanju s strani tretjih oseb - dobaviteljev.

4. POLITIKA

Pogodbena zaveza

- Vsi dobavitelji, ki jim je odobren dostop do IT dobrin podjetja, ne glede na to ali so dobavitelj, stranka ali uporabnik so dolžni spoštovati informacijsko varnostno politiko podjetja. Pogodba o varovanju zaupnih podatkov vsebuje povzetek politike varovanja informacij (zaupni podatek), obveznosti pogodbenih strank, pooblaščen predstavnike, trajanje in kršitvene določbe. Pogodba mora biti podpisana preden jim je odobren dostop.
- Pogodba o varovanju zaupnih podatkov mora biti podpisana vedno v primeru, kadar bi lahko bile razkrite zaupne, občutljive ali druge vredne informacije.
- Pogodbe z zunanjimi dobavitelji in zunanjimi ponudniki storitev se morajo pregledovati in spremljati z namenom, da se zadovolji zahtevam po informacijski varnosti.

	VARNOSTNA POLITIKA	
	POLITIKA ODNOSA Z DOBAVITELJI	
	Oznaka: VP 11-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 3/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

Podpora in vzdrževanje s strani dobaviteljev

Oseba, ki je odgovorna za sklepanje vzdrževanja in podpore, mora zagotavljati, da bo podpisana pogodba v skladu z vsebino in duhom informacijske varnostne politike.

Razvoj s strani dobaviteljev

Osebe, odgovorne za dobavitelje zunanjega razvoja in storitev, so dolžne sodelovati zgolj z uglednimi podjetji, ki delujejo v skladu s standardi kakovosti in, ki bodo sledili informacijski varnosti politike naše podjetja, še posebej tiste, ki se nanašajo na razvoj aplikacij.

Upravljanje IT sredstev v zunanjem izvajanju (outsourcing)

Dobavitelj, s katero sodeluje Mariborski vodovod, mora biti sposobna dokazati skladnost delovanja z varnostno politiko podjetja, ter se pravno-formalno zavezuje k spoštovanju dogovorjenega nivoja kakovosti storitev in odpravi vseh morebitnih pomanjkljivosti.

5. UVELJAVLJANJE POLITIKE

Vsak zaposleni, na katerega se nanaša ta politika, ki je identificiran in je ugotovljeno, da je prekršil to politiko, je glede na obseg in vsebino kršitve lahko podvržen sankcioniranju in ustreznim disciplinskim ukrepom podjetja.

Dobavitelji, ki kršijo to politiko so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

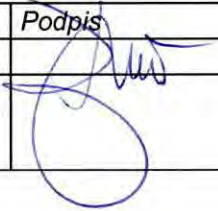
- Uporabljena nadzorstva ISO/IEC 27001-2013 poglavja:
A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.1.2
- Pogodba o varovanju zaupnih podatkov SN_02_01_Pogodba NDA.doc

	VARNOSTNA POLITIKA	
	POLITIKA ODNOSA Z DOBAVITELJI	
	Oznaka: VP 11-01	Datum izdaje: 15.06.2018
	Verzija: 1	Stran: 4/4
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	apr.2018	Nadomešča staro: VP_02_01_Odnosti do tretjih oseb	VP_11_01_Odnosi dobavitelji	z Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Erker
3		Dodane spr.		Uredil:
4		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3. 12. 2019	

PRILOGA

Je ločen dokument VP_02_01_Pogodba NDA.doc

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INCIDENTOV	
	Oznaka: VP 12-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 1/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

VSEBINA:

1. NAMEN	2
2. OBSEG	2
3. POJMI	2
4. POLITIKA	2
4.1. Varnostni incident.....	2
4.2. Postopek in odgovornost	3
4.3. Poročanje	3
4.4. Pregledovanje	4
5. UVELJAVLJANJE POLITIKE	4
6. REFERENCE	4
7. ZGODOVINA.....	5

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INCIDENTOV	
	Oznaka: VP 12-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 2/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

1. NAMEN

Varnostni incidenti so vsi dogodki, ki vplivajo na razpoložljivost, neoporečnost in zaupnost informacij in storitev. Predstavljajo kakršno koli tveganje za informacijo, informacijski sistem, dogodek povezan z nosilcem podatkov, ki je lahko bodisi ukraden, poškodovan ali uničen ali pa so poškodovani, uničeni, spremenjeni ali nedosegljivi podatki.

Cilj te varnostne politike je varovanje Mariborskega vodovoda pred škodo, ki lahko nastane zaradi varnostnih incidentov.

2. OBSEG

Politika je namenjena vsem zaposlenim, pogodbenikom, svetovalcem, začasno zaposlenim in vsem ostalim delavce Mariborskega vodovoda (v nadaljevanju: uporabniki).

Posebej morajo politiko upoštevati vodstveni delavci, sektor informatiko in njegov vodja .

3. POJMI

Uporabniki: so vsi zaposleni, začasno zaposleni, pogodbeniki, svetovalci, dobavitelji in ostali delavci.

Incident: varnostni dogodek ali varnostna slabost sistema ki vpliva na razpoložljivost, celovitost ali zaupnost informacij ali storitev.

Dobavitelji: pravne in fizične osebe, ki sodelujejo s podjetjem in imajo dostop do IT dobrin.

4. POLITIKA

4.1. Varnostni incident

Vzrok zaradi česar se varnostni incidenti zgodijo:

- grožnja, ki se je uresničila, vendar ni bila odkrita (nerazpoložljivost informacij ali storitev, ogrožena celovitost ali zaupnost informacij ali storitev)
- pomanjkljiva, neimplementirana ali neupoštevana varnostna politika,
- neustrezni preventivni ukrepi (tehnični ali netehnični) za identifikacijo in izogibanje varnostnim incidentom,
- itd.

V primeru incidenta, ni dovolj, da se incident zavede, označi kot »odkrit incident« in da se izvedejo vsi ukrepi za zmanjšanje škode, ki bi lahko zaradi incidenta nastala. Potrebno je analizirati vzroka nastanka incidenta in izvesti ukrepe, da do takega primera v prihodnje ne pride. Ob nastanku incidenta je vedno odgovornost vodstvenih delavcev, da sprožijo aktivnosti za odpravo posledic incidenta in zmanjšanje škode.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INCIDENTOV	
	Oznaka: VP 12-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 3/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

4.2. Postopek in odgovornost

V trenutku, ko uporabniki zaznajo sumljiv dogodek ali možnost incidenta, le to informacijo posredujejo na pomoč uporabnikom, ki to informacijo posredujejo ustrezni odgovorni osebi. V kolikor incident nastane izven delovnega časa uporabniške podpore, mora zaposleni informacijo posredovati svojemu nadrejenemu.

Mariborski vodovod ima vzpostavljeno enotno vstopno točko: »pomoč uporabnikom« int tel. 261 ali na elektronski naslov it.podpora@mb-vodovod.si, na katero so vsi uporabniki dolžni poročati o dogodkih v zvezi z varovanjem informacij, ter poročajo o vsaki opaženi ali sumljivi varnostni slabosti sistema ali storitve.

Vse okoliščine incidenta morajo biti podane iskreno in transparentno z namenom zmanjšanja oziroma preprečevanja škode.

Uslužbenec »pomoči uporabnikom« vse prijave in incidente (vsaka prijava še ni nujno incident) v zvezi z informacijsko varnostjo, nemudoma zabeleži in posreduje v sektor za informatiko.

S prijavi, ki kažejo na varnostnimi incidenti se obvesti vodjo sektorja za informatiko, ki sprejme naslednje ukrepe:

- takojšnji ukrepi za identifikacijo in omejevanje nastalega varnostnega incidenta na najmanjšo možno mero,
- takojšnji ukrepi za zmanjšanje posledic varnostnega incidenta, ki se je mogoče zgodil (takojšnje posredovanje informacij tudi v primeru, ko ni gotovo, da je incident nastal),
- takojšnji ukrepi za zmanjšanje posledic varnostnega incidenta, ki bi se lahko zgodil (odprava zaznanih pomanjkljivosti).

V primeru, da se je varnostni incident zgodil, je najpomembnejši dejavnik čas. Prej, ko varnostni incident odkrijemo, prej lahko ukrepamo in s tem zaustavimo nevarnost ali preprečimo njeno širjenje. Ob zgodnjem odkritju varnostnega incidenta so lahko posledice in škoda manjši.

Ob večjih varnostnih incidentih in eskalacijah, ki bi lahko povzročili finančno ali pravno škodo ali ogrozili ugled podjetja, vodja sektorja za informatiko nemudoma skliče varnostni forum, ki predlaga ustrezne ukrepe in seznani vodstvo Mariborskega vodovoda.

4.3. Poročanje

Ocena incidenta se vedno izvaja na osnovi predvidene škode, ki lahko nastane kot posledica incidenta. Zaznani dogodki, ki jih lahko ocenimo za incident, morajo biti nemudoma sporočeni kompetentni osebi, t.j. vodji sektorja informatiko, ki lahko sprejme odločitve o ravnanju v dani situaciji, ta pa po potrebi obvesti direktorja podjetja. Pri ocenjevanju incidenta morajo biti podani odgovori na naslednje kriterije:

- Klasifikacija IT dobrine (namizni računalnik, strežniški sistem, nosilec podatkov, programska oprema, podatkovne baze,...)
- tip škode (ali je prizadeta razpoložljivost, celovitost ali zaupnost),
- velikost škode (v kolikor je mogoče velikost nastale škode ali pričakovane škode oceniti),

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INCIDENTOV	
	Oznaka: VP 12-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 4/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

- razlog, povzročitelj incidenta (v kolikor je to možno),
- potencialna grožnja podjetju.

Prijave se dokumentirajo v elektronski obliki. Mariborski vodovod vodi evidenco v tabeli **prijave_it_incidentov.xls**.

Obveščanje o varnostnih incidentih je odvisno od kritičnosti incidenta oz. sistema na katerega ima ta vpliv:

Visoko kritični sistemi	Srednje kritični sistemi	Nizko kritični sistemi
Incidente in domnevne pomanjkljivosti se poroča vodji informatike in direktorju MV, ali drugemu članu, ki je zastopan v varnostnem forumu	Incidente in domnevne pomanjkljivosti se poroča vodji sektorja informatike in vodji OE	Incidente in domnevne pomanjkljivosti se poroča odgovornemu vodji OE – normalna situacija.

Kritičnost sistemov je opredeljena v sistemskem postopku: *Klasifikacija kritičnih informacijskih sistemov v MV d.d.*

4.4. Pregledovanje

Varnostni forum vsaj enkrat letno pregleda statistiko incidentov. Ob tem obravnava tudi preventivne ukrepe za zmanjšanje števila incidentov.

5. UVELJAVLJANJE POLITIKE

Vsi uporabniki informacijskega sistema Mariborskega vodovoda so odgovorni za izvajanje določil te politike. Vsi vodje OE morajo skrbeti, da zaposleni, ki so pod njihovim vodenjem, upoštevajo varnostne mere navedene v tej politiki.

Vsak zaposleni, na katerega se nanaša ta politika, ki je identificiran in je ugotovljeno, da je prekršil to politiko, je glede na obseg in vsebino kršitve lahko podvržen sankcioniranju in ustreznim disciplinskim ukrepom podjetja.

Tretje osebe, ki kršijo to politiko so lahko soočene s pogodbeno denarno kaznijo in v skrajnem primeru s prekinitvijo pogodbe.

6. REFERENCE

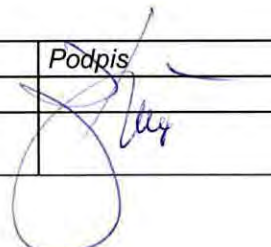
- Uporabljena nadzorstva ISO/IEC 27001-2013:
A.16.1 Upravljanje informacijskih varnostnih incidentov in izboljšave"
- Sistemski postopek: Klasifikacija kritičnih informacijskih sistemov v MV d.d.

	VARNOSTNA POLITIKA	
	POLITIKA UPRAVLJANJA INCIDENTOV	
	Oznaka: VP 12-01	Datum izdaje: 15.06.2018
	Verzija: 2	Stran: 5/5
	Datum zadnje revizije: 02.12.2019	Datum nove revizije: 2020

Klasifikacija: **ZA INTERNO UPORABO**

7. ZGODOVINA

Zap. št.	Datum	Opis	Ime datoteke	Opomba
1	2018	Nadomešča VP_09_01_P olitikaUpravlja njaIncidentov	VP_12_01_Upravljanje Incidentov.docx	Pripravil: Bojan Erker
2	12-2019	Dodane spr.		Uredil: Bojan Erker
3		Dodane spr.		Uredil:

	Ime	Podpis
Direktor:	Danilo Burnač	
Sprejet na Forumu varovanja informacij, dne:	3.12.2019	