Polion d.o.o.
Obrtnička 12
32100 Vinkovci

t: 032 332 784
f: 032 332 784
e: info@polion.hr

OIB: 26195613045
IBAN: HR2223400091100164230
www.polion.hr

ISO 9001:2015; ISO 14001:2015
Cro Cert

POLITIKA SIGURNOSTI INFORMATIČKE INFRASTRUKTURE

SADRŽAJ

Oznaka dokumenta: ZOP 4.0

Verzija: 1

Datum publiciranja: 25.5.2018.

Datum slijedeće revizije: 25.5.2023.

Vlasnik dokumenta: Voditelj informatičkog odjela, ugovorni suradnik poduzeća Polion d.o.o., Vinkovci, Obrtnička 12, OIB: 26195613045

UVOD

1.1. Svrha

Ovaj dokument pod nazivom Politika sigurnosti informatičke infrastrukture za cilj ima definirati sigurnosne zahtjeve koji osiguravaju pravilnu i sigurnu upotrebu informatičke infrastrukture u poduzeću Polion d.o.o.. Cilj ovog dokumenta je definirati pravila kojima se štiti poduzeće Polion d.o.o. i svi korisnici, u najvećoj mogućoj mjeri, od sigurnosnih prijetnji koje bi mogle ugroziti integritet privatnost njezinih zaposlenika, suradnika te ugled poduzeća Polion d.o.o.. Ova politika propisanim pravilima osigurava najoptimalniju razinu zaštite osobnih podataka povjerenih na obradu poduzeću Polion d.o.o., a u skladu sa zahtjevima opće Uredbe o zaštiti osobnih podataka (u daljnjem tekstu Uredba).
Pod pojmom „Informatička infrastruktura“ u ovoj Politici podrazumijeva se i hardverska i programska infrastruktura.

1.2. Djelokrug

Ovaj dokument odnosi se na sve korisnike informatičke infrastrukture poduzeća Polion d.o.o., uključujući i privremene korisnike (gosti, vanjski suradnici) koji imaju privremeni pristup uslugama informatičke infrastrukture te partnere s ograničenim ili neograničenim vremenom pristupa uslugama informatičke infrastrukture. Politika zahtjeva i pretpostavlja usklađenost svih korisnika usluga informatičke infrastrukture Poduzeća Polion d.o.o. s propisanom politikom.

1.3. Odgovornosti

Uloga	Odgovornosti
Voditelj informatičkog odjela	• Odgovoran za sve aspekte informacijske sigurnosti • Odgovoran za sigurnost informatičke infrastrukture • Planira aktivnosti koje umanjuju i otklanjaju sigurnosne prijetnje • Provodi i revidira Politiku informacijske sigurnosti • Provodi programe edukacije o sigurnosti informatičke infrastrukture • Osigurava usklađenost politike informatičke sigurnosti i infrastrukture • Reagira na incidente vezane uz povredu informacijske sigurnosti u dijelu informatičke infrastrukture • Provodi i pomaže u provođenju planova za oporavak od katastrofe • Osigurava kontinuitet poslovanja • Upravlja informatičkom sigurnošću i implementira poboljšanja u skladu s razvojem tehnologije • Primjenjuje i omogućava prava pristupa podacima i resursima • Djeluje u skladu s prihvaćenom Politikom privatnosti Poduzeća Polion d.o.o.
Osobe odgovorne za podatke	• Daju prijedloge za unaprjeđenje sigurnosti podataka na njihovom specifičnom području • Daju prijedloge za dodjeljivanje prava pristupa podacima u njihovom specifičnom području
Korisnici	• Upoznati i prihvatiti politiku sigurnosti informatičke infrastrukture

	• Prijavljuju bilo kakav pokušaj povrede sigurnosti

1.4. Opće politike

1. Svaki izuzetak od pravila definiranih u bilo kojem dijelu ovog dokumenta može odobriti samo voditelj informatičkog odjela u dogovoru s direktorom.
2. Svaki puta kada se odstupa od pravila propisanih ovom politikom, odstupanje se evidentira zapisnikom, evidentirajući vrijeme, opis, razlog odstupanja te način upravljanja rizikom.
3. Sve usluge koje omogućuje informatička infrastruktura moraju se koristiti isključivo u skladu s tehničkim i sigurnosnim zahtjevima definiranim u ovoj politici.
4. Svako kršenje prihvaćene Politike sigurnosti informatičke infrastrukture mogu dovesti do disciplinskih postupaka opisanih u Disciplinskoj politici Poduzeća Polion d.o.o. .

2. POLITIKA INFORMATIČKE INFRASTRUKTURE

2.1. Svrha

Odjeljak propisuje uvjete za pravilno i sigurno rukovanje svim informatičkim sredstvima u Poduzeću Polion d.o.o.

2.2. Djelokrug

Pravila opisana u ovom odjeljku odnose se na stolna računala, prijenosna računala, pisače i drugu infrastrukturu, aplikacije i softver te na bilo koga tko upotrebljava tu imovinu, uključujući interne korisnike, privremene zaposlenike, posjetitelje i vanjske suradnike, te sve ostale fizičke i pravne osobe koje rade za i u ime Poduzeća Polion d.o.o.

2.3. Opis politike

1. Sva informatička infrastruktura može se koristiti isključivo u poslovnim aktivnostima za koje je namijenjena
2. Sva informatička infrastruktura mora biti svrstana u jednu od sigurnosnih kategorija definiranih u Poduzeću Polion d.o.o., u skladu s trenutnom poslovnom funkcijom kojoj je dodijeljena
3. Svaki korisnik je odgovoran za očuvanje i ispravnu upotrebu informatičke infrastrukture koja mu je dana na korištenje
4. Sva informatička infrastruktura mora biti na mjestima s ograničenim pristupom. Razina pristupa definirana je u skladu sa sigurnosnim kategorijama Poduzeća Polion d.o.o.
5. Aktivna radna površina i prijenosna računala moraju biti osigurana ukoliko nisu pod nadzorom. Kada je god moguće, spomenuto pravilo mora se provoditi automatski.
6. Pristup infrastrukturi nije dozvoljen neovlaštenim osobama. Dodjeljivanje pristupa informatičkoj infrastrukturi i računalnim mrežama mora se obaviti putem odobrenih i prihvaćenih postupaka za upravljanje uslugama informatičke infrastrukture i nadziranim upravljanjem pristupom.
7. Svo osoblje koje koristi informatičku infrastrukturu mora proći odgovarajuću obuku za korištenje informatičke infrastrukture.
8. Korisnici se moraju prema infrastrukturi, koja im je povjerena na korištenje, odnositi s punom pažnjom, održavati ju čistu te s njom pažljivo rukovati te izbjegavati nepravilno korištenje.
9. Pristup informatičkoj infrastrukturi instaliranoj u Poduzeću Polion d.o.o. mora biti ograničen, u skladu s odobrenim pravima, odobren u skladu s politikama sigurnosti i privatnosti. Prijenosna računala tvrtke, tableti, pametni telefoni i ostala infrastruktura koja se koristi na izdvojenim lokacijama mora se periodički održavati i provjeravati.

10. Informatički odjel jedini je odgovoran za održavanje, nadogradnju i konfiguriranje informatičke infrastrukture. Niti jedan drugi korisnik nije i ne može biti odgovoran i ovlašten za održavanje i nadogradnju infrastrukture. To uključuje izmjenu hardvera ili instaliranje softvera.
11. Posebna se pažnja mora posvetiti zaštiti prijenosnih računala, tableta, pametnih telefona i drugih prijenosnih uređaja od krađe ili gubitka. Također, u obzir treba uzeti druge rizike oštećenja infrastrukture te oštećenja koji mogu rezultirati povredom ili gubitkom podataka kao što su ekstremne temperature, magnetska polja ili padovi.
12. Prilikom putovanja (avionom) prijenosna oprema poput prijenosnih računala, tableta ili pametnih telefona, mora ostati u posjedu korisnika kao ručna prtljaga
13. Uvijek kada je moguće, neophodno je koristiti tehnologiju šifriranja i brisanja u slučaju gubitka ili krađe prijenosne infrastrukture.
14. Sva prijenosna oprema koja se koristi u poslovanju Poduzeća Polion d.o.o. mora biti zaštićena tehnologijom kriptiranja. Oprema koja nema tu mogućnost ne može se koristiti izvan prostora Poduzeća Polion d.o.o..
15. Gubitak, krađa, oštećenje, neovlašteno korištenje ili drugi incidenti moraju se, što prije od trenutka spoznaje, prijaviti voditelju informatičkog odjela.
16. Zbrinjavanje imovine koja se više ne koristi mora se izvršiti u skladu s posebnim postupcima zbrinjavanja informatičkog otpada, uzimajući u obzir zaštitu svih informacija koji su predmet takvog oblika obrade. Imovina koja pohranjuje povjerljive podatke mora biti uništena u prisustvu člana tima za informacijsku sigurnost. Sredstva za čuvanje osjetljivih informacija moraju se prije odlaganja u potpunosti izbrisati u nazočnosti člana tima za informacijsku sigurnost

3. POLITIKA KONTROLE PRISTUPA

3.1. Svrha

Odjeljak „Politika kontrole pristupa“ određuje uvjete za pravilnu kontrolu pristupa informatičkim uslugama i informatičkoj infrastrukturi u Poduzeću Polion d.o.o..

3.2. Djelokrug

Politika kontrole pristupa odnosi se na sve korisnike informatičke infrastrukture u Poduzeću Polion d.o.o., uključujući i privremene korisnike (gosti, posjetitelji, vanjski suradnici) koji imaju privremeni pristup informatičkih uslugama te partnere s ograničenim ili neograničenim vremenom pristupa uslugama koje pruža informatička infrastruktura. Politika zahtjeva i pretpostavlja usklađenost svih korisnika informatičkih usluga Poduzeća Polion d.o.o. s propisanom politikom.

3.3. Opis politike

1. Svaki sustav koji obrađuje podatke mora biti zaštićen sustavnom kontrole pristupa koji se temelji na lozinki
2. Svaki sustav koji obrađuje povjerljive podatke mora biti zaštićen dvostupanjskim sustavom kontrole pristupa.
3. Minimalno jednom godišnje potrebno je provesti kontrolu i reviziju dodijeljenih prava pristupa
4. Pristup podacima treba biti dodijeljen za grupe korisnika a ne za korisnika pojedinačno. Svaka iznimka mora biti posebno odobrena i evidentirana.
5. Pristup podacima odobrava se u skladu s načelom „manje povlastice“, tj. svakom se korisniku dodjeljuju minimalna prava pristupa resursima koji su im potrebni za uspješno obavljanje poslovnih funkcija.
6. Kada je god moguće, pristup se odobrava sa centralne lokacije
7. Svi bi se korisnici trebali suzdržavati od pokušaja manipuliranja ili izbjegavanja kontrole pristupa kako bi dobili veća prava pristupa od onih koja su im dodijeljena.

8. Sustav mora uključivati automatsku kontrolu, bilježenje i sprečavanje pokušaja neovlaštenih pristupa kako bi se otkrili svi pokušaji zaobilaženja sustava kontrole i nadzora sigurnosti informatičkog sustava

4. POLITIKA KONTROLE LOZINKI

4.1. Svrha

Odjeljak pod nazivom „Politika kontrole lozinki“ definira uvjete za pravilno i sigurno upravljanje lozinkama u Poduzeću Polion d.o.o..

4.2. Djelokrug

Politika kontrole pristupa odnosi se na sve korisnike informatičke infrastrukture u Poduzeću Polion d.o.o., uključujući i privremene korisnike (gosti, posjetitelji, vanjski suradnici) koji imaju privremeni pristup informatičkim uslugama te partnere s ograničenim ili neograničenim vremenom pristupa informatičkim uslugama. Politika zahtjeva i pretpostavlja usklađenost svih korisnika informatičkih usluga Poduzeća Polion d.o.o. s propisanom politikom.

4.3. Opis politike

1. Svaki sustav koji obrađuje podatke mora biti zaštićen sustavnom kontrole pristupa koji se temelji na lozinki.
2. Svaki korisnik mora imati zasebni privatni identitet za pristup mrežnim uslugama
3. Identiteti moraju biti centralno kreirani i upravljani.
4. Svaki identitet mora imati jaku, privatnu alfanumeričku lozinku za pristup uslugama informatičkog sustava. Lozinke moraju imati minimalno 8 znakova.
5. Lozinke moraju biti sastavljene od kombinacije slova, brojeva i posebnih znakova (interpunkcijskih oznaka i simbola).
6. Lozinke moraju imati kombinaciju velikih i malih slova.
7. Lozinke se ne bi trebale sadržavati očiti slijed znakova na tipkovnici (npr qwertz ili 12345)
8. Lozinke ne smiju sadržavati pogodne podatke kao što su osobni podaci o sebi, članovima obitelji, kućnim ljubimcima, vašoj djeci, rođendanima, adresama, telefonskim brojevima, lokacijama i sl.
9. Dozvoljava se zamjena brojeva za slova npr. 3 se može koristiti kao E, 4 kao A ili 0 kao O.
10. Pamćenje lozinki ne mora biti teško. Dozvoljeno je korištenje kratkih rečenica kao lozinki (npr MojaMam4najb0ljeKuha!)
11. Svaki redoviti korisnik istu lozinku može koristiti najviše 90 dana, ne manje od 3 dana. Istu lozinku ne smije koristiti barem godinu dana.
12. Ne preporuča se korištenje iste lozinke za pristup različitim sustavima.
13. Voditelji nisu ovlašteni tražiti, prikupljati i pohranjivati lozinke zaposlenika.
14. Ukoliko se odrede neki identiteti kojima se lozinke ne mijenjaju, lozinka u tom slučaju mora sadržavati najmanje 15 znakova.
15. Neprihvatljivo je korištenje administrativne lozinke za neadministrativni rad. Administrator(i) informatičke infrastrukture mora(ju) imati odvojene lozinke za administrativni i neadministrativni rad.
16. Strogo je zabranjeno dijeljenje lozinki. Lozinke se ne smiju otkrivati ili javno prikazivati.
17. Zabranjeno je slanje lozinki elektroničkom poštom.
18. Uvijek kada se lozinka smatra kompromitiranom, odmah se mora promijeniti.
19. Za kritične obrade podataka, a kada je god to moguće, potrebno je koristiti digitalne certifikate i višestruku autentifikaciju pomoću smart kartica.

5. POLITIKA ELEKTRONIČKE POŠTE

5.1. Svrha

Odjeljak pod nazivom „Politika elektroničke pošte“ definira uvjete za pravilnu i sigurnu upotrebu elektroničke pošte u Poduzeću Polion d.o.o..

5.2. Djelokrug

Politika elektroničke pošte odnosi se na sve korisnike elektroničke pošte u Poduzeću Polion d.o.o., neovisno radi li se o privatnim ili služenim adresama elektroničke pošte.

5.3. Opis politike

1. Sve dodijeljene adrese elektroničke pošte i mjesta za pohranu pošte moraju se koristiti isključivo u poslovne svrhe u interesu Poduzeća Polion d.o.o.. Povremeno korištenje osobne e-mail adrese na internetu za osobnu namjenu može biti dopušteno ako korištenje ne uzrokuje vidljivu potrošnju resursa Poduzeća Polion d.o.o. i ne utječe na produktivnost rada.
2. Strogo je zabranjeno korištenje resursa poduzeća za neovlašteno oglašavanje, neželjenu elektroničku poštu, političke kampanje i drugo korištenje koje nije povezano s poslovanjem Poduzeća Polion d.o.o..
3. Ni na koji način se resursi i adrese elektroničke pošte ne smiju koristiti za otkrivanje povjerljivih ili osjetljivih informacija koje posjeduje Poduzeće Polion d.o.o., osim u slučaju otkrivanja podataka ovlaštenim osobama i na autorizirane adrese elektroničke pošte.
4. Korištenje resursa i adresa elektroničke pošte Poduzeća Polion d.o.o. za širenje poruka koje se smatraju uvredljivima, rasističkim ili na bilo koji način protivnih zakonu i etici Poduzeća Polion d.o.o., apsolutno se zabranjuju.
5. Elektronička pošta Poduzeća Polion d.o.o. koristi se samo u mjeri koja je potrebna za obavljanje poslovnih zadaća. Kada korisnik i Poduzeće Polion d.o.o. prekinu poslovni odnos, elektronička pošta mora biti deaktivirana.
6. Korisnici moraju imati privatni identitet da bi pristupili vlastitoj elektroničkoj pošti i resursima za pohranu elektroničke pošte osim u slučajevima posebnim slučajevima kada pristupaju elektroničkoj pošti dodijeljenoj grupi djelatnika.
7. Privatnost nije zajamčena. Ukoliko se pojave posebni zahtjevi povjerljivosti, vjerodostojnosti i integriteta, omogućiti će se korištenje elektronički potpisanih poruka.
8. Samo Voditelj informatičkog odjela u poduzeću Polion d.o.o. u dogovoru s direktorom može odobriti presretanje i otkrivanje poruka.
9. Identiteti za pristup korporativnoj elektroničkoj pošti moraju biti zaštićeni jakim lozinkama. Složenost i trajanje lozinki definirano je ovom politikom. Dijeljenje lozinki nije dozvoljeno. Korisnici ne smiju lažno predstavljati drugog korisnika.
10. Izlazne poruke korporativnih e-mail adresa trebaju imati odobrene potpise na kraju poruke.
11. Prilozi moraju biti ograničeni veličinom u skladu s posebnim postupcima Poduzeća Polion d.o.o.. Kada god je to moguće, ograničenja se moraju provoditi automatski.
12. Antivirusna zaštita i zaštita od zlonamjernih programa mora biti postavljena na svakom klijentskom računalu i na poslužiteljima, kako bi se osigurala maksimalna zaštita od zlonamjerne dolazne i odlazne pošte.
13. Sigurnosni incidenti moraju se prijaviti i obraditi što je prije moguće u skladu s procesima upravljanja informacijskom sigurnošću, korisnici ne bi trebali sami odgovarati na sigurnosne napade.
14. Sadržaj korporativne elektroničke pošte treba pohranjivati centralno na mjestima koja se mogu sigurnosno kopirati i s kojima se može upravljati i skladu s procesima u tvrtci. Čišćenje, sigurnosno kopiranje i povrat moraju se upravljati u skladu s prihvaćeni postupcima upravljanja kontinuitetom poslovanja.

6. POLITIKA KORIŠTENJA INTERNETA

6.1. Svrha

Odjeljak pod nazivom „Politika korištenja interneta“ definira uvjete za pravilan i siguran pristup internetu.

6.2. Djelokrug

Politika korištenja interneta odnosi se na sve korisnike interneta u poduzeću Polion d.o.o., uključujući i privremene korisnike (gosti, posjetitelji, vanjski suradnici) koji imaju privremeni pristup internetu te partnere s ograničenim ili neograničenim vremenom pristupa internetu. Politika zahtjeva i pretpostavlja usklađenost svih korisnika interneta Poduzeća Polion d.o.o. s propisanom politikom.

6.3. Opis politike

1. Za sve korisnike interneta dopušten je ograničen pristup.
2. Strogo je zabranjen pristup pornografskim web stranicama i svim drugim rizičnim stranicama.
3. Preuzimanje sadržaja dozvoljeno je samo nekim korisnicima i može biti dodatno odobreno na zahtjev.
4. Pristup internetu uglavnom je predviđen za osobnu namjenu. Dopušten je ograničen pristup internetu u osobne svrhe uz uvjet da se vidljivo ne troše resursi Poduzeća Polion d.o.o. i ne utječe na produktivnost rada. Obeshrabruje se svako korištenje interneta za osobne svrhe tijekom radnog vremena.
5. Ulazni i izlazni promet kontroliraju se i ograničavaju pomoću vatrozida.
6. Pri pristupanju internetu, korisnici se moraju ponašati u skladu s pravilima koja osiguravaju ugled.
7. Internet promet treba biti ograničen vatrozidom. Svaki napad treba biti zabilježen, a ovisno o tipu napada i prijavljen voditelju informatičkog odjela.
8. Potrebno je poduzeti razumne mjere za otkrivanje, sprečavanje i pohranu informacija o napadima na servere i radne stanice.

7. POLITIKA ANTIVIRUSNE ZAŠTITE

7.1. Svrha

Odjeljak pod nazivom „Politika antivirusne zaštite“ definira uvjete za pravilnu primjenu antivirusnih i drugih oblika zaštite u Poduzeću Polion d.o.o.

7.2. Djelokrug

Pravila opisana u ovoj politici odnose se na poslužitelje, radne stanice i infrastrukturu u Poduzeću Polion d.o.o., uključujući prijenosna računala i tablete koji mogu biti korišteni izvan poduzeća. Neka od navedenih pravila odnose se i na uređaje koji pristupaju resursima Poduzeća Polion d.o.o..

7.3. Opis politike

1. Sva računala i uređaji koji pristupaju mreži Poduzeća Polion d.o.o. moraju imati instaliranu antivirusnu zaštitu u skladu s najvišim standardima zaštite resursa i informacija u Poduzeću Polion d.o.o..
2. Svi poslužitelji i radne stanice u vlasništvu Poduzeća Polion d.o.o. ili trajno korišteni uređaji, moraju imati odobreni, centralno upravljani antivirusni program. Ovo pravilo se odnosi i na prijenosna računala koja se redovito povezuju s mrežom Poduzeća Polion d.o.o. ili kojima se internetom upravlja putem sigurnih kanala.

3. Računala Poduzeća Polion d.o.o. koja rade u mreži drugih poduzeće mogu biti izuzeta od prethodnog pravila ako to zahtijevaju sigurnosna pravila druge poduzeća, pod uvjetom da su ta računala također zaštićena.
4. Prijenosna računala koja se rijetko povezuju s mrežom Poduzeća Polion d.o.o., mogu imati instaliran odobreni antivirusni program koji je upravljan lokalno (ne centralno).
5. Svi instalirani antivirusni programi moraju se automatski ažurirati te se ažuriranje mora nadgledati kako bi se osiguralo uspješno ažuriranje.
6. Svi uređaji gostiju, posjetitelja i ostala privatna infrastruktura nad kojom Poduzeće Polion d.o.o. nema nadzor mogu se spojiti samo na izdvojenu, za takve potrebe predviđenu internetsku mrežu. Nije omogućeno spajanje na glavnu mrežu Poduzeća Polion d.o.o..

8. POLITIKA KLASIFICIRANJA INFORMACIJA

8.1. Svrha

Politika klasificiranja informacija definira okvir za klasificiranje informacija prema važnosti i rizicima koji su uključeni. Cilj je osigurati odgovarajući integritet, povjerljivost i dostupnost podataka Poduzeća Polion d.o.o..

8.2. Djelokrug

Pravila opisna u ovoj politici odnose se na sve informacije koje su kreirane, u vlasništvu ili kojima upravlja Poduzeće Polion d.o.o., uključujući one pohranjene u elektroničkom obliku i one tiskane na papiru.

8.3. Opis politike

1. Poduzeće Polion d.o.o. mora osigurati sigurnost svih podataka koje posjeduje, neovisno o načinu stjecanja, i osigurati sigurnost sustava koji upravlja podacima u skladu s ovom politikom i svim ostalim relevantnim politikama prihvaćenim u Poduzeću Polion d.o.o., a naročito Politikom zaštite podataka Poduzeća Polion d.o.o..
2. Uprava Poduzeća Polion d.o.o. odgovorna je za osiguranje i raspodjelu resursa i zadataka koji osiguravaju povjerljivost, cjelovitost i dostupnost informacija, podataka i informatičkih usluga Poduzeća Polion d.o.o..
3. Svaka povreda sigurnosti podataka odmah mora biti prijavljena voditelju informatičkog odjela, direktoru Poduzeća Polion d.o.o. i službeniku za zaštitu osobnih podataka. Ukoliko je potrebno, moraju se aktivirati odgovarajuće protumjere kako bi se procijenila i kontrolirala eventualno nastala šteta i postupilo u skladu s ostalim prihvaćenim relevantnim politikama, pravilima i procedurama.
4. Informacije u Poduzeću Polion d.o.o. razvrstavaju se u skladu s njihovim učinkom na sigurnost. Dijele se na 5 kategorija i to: povjerljive, osjetljive, zajedničke, javne i privatne.
5. Informacije definirane kao povjerljive imaju najvišu razinu sigurnosti. Samo ograničeni broj osoba može imati pristup tim informacijama. Upravljanje, pristup i odgovornosti vezane uz povjerljive informacije moraju se definirati posebnim postupcima informacijske sigurnosti.
6. Informacije koje su definirane kao osjetljive mogu biti obrađivane od strane većeg broja osoba. Potrebne su za svakodnevno obavljanje poslova, ali se ne smiju dijeliti izvan dosega potrebnog za obavljanje odgovarajuće funkcije.
7. Informacije definirane kao zajedničke, mogu se dijeliti izvan Poduzeća Polion d.o.o., za one klijente, poduzeća, korisnike koji imaju pravo im pristupati.
8. Informacije definirane kao javne mogu se javno dijeliti, npr. sadržaj na internetskim stranicama Poduzeća Polion d.o.o..
9. Informacije koje se smatraju privatnima pripadaju pojedincima koji su odgovorni za njihovo čuvanje i sigurnosno kopiranje.
10. Informacije se klasificiraju zajednički od strane voditelja informatičkog odjela, direktora i službenika za zaštitu osobnih podataka Poduzeća Polion d.o.o..

9. POLITIKA UDALJENIH PRISTUPA

9.1. Svrha

Politika udaljenih pristupa definira uvjete za siguran daljinski pristup unutarnjim resursima poduzeća.

9.2. Djelokrug

Politika udaljenih pristupa odnosi se na korisnike koji pristupaju unutarnjim resursima Poduzeća Polion d.o.o. s udaljenih lokacija.

9.3. Opis politike

1. Da bi pristupili internim resursima Poduzeća Polion d.o.o. s udaljenih lokacija, korisnici moraju imati potrebna autorizacijska prava. Pristup zaposlenika s udaljenih lokacija može zatražiti samo njemu nadređena osoba, odobrava ga direktor, a omogućava voditelj informatičkog odjela ili djelatnik informatičkog odjela po nalogu voditelja informatičkog odjela.
2. Pristup s udaljenih lokacija mora biti omogućen samo sigurnim kanalima uz međusobnu provjeru autentičnosti između poslužitelja i klijenta. I poslužitelj i klijent moraju prepoznati međusobno pouzdane certifikate.
3. Nije dozvoljen pristup povjerljivim informacijama s udaljenih lokacija. Iznimka od ovog pravila može se odobriti samo u slučajevima u kojima je to strogo potrebno.
4. Korisnici se ne smiju povezivati s javnih računala osim ako se radi o pristupu javnom sadržaju (npr. web stranicama).

10. POLITIKA IZDVAJANJA POSLOVA (OUTSOURCINGA)

10.1. Svrha

Politika izdvajanja poslova definira zahtjeve koji su potrebni kako bi se smanjili rizici povezani s izdvajanjem poslova informatičkih usluga, funkcija i procesa.

10.2. Djelokrug

Pravila opisana Politikom izdvajanja poslova odnose se na Organizaciju Polion d.o.o., pružatelje usluga kojima se izdvajaju poslovi informatičkih usluga, funkcije i procesi, te sam proces izdvajanja poslova.

10.3. Opis politike

1. Prije izdvajanja poslova pružanja bilo kojih usluga, funkcija ili procesa, mora se obaviti procjena rizika izdvajanja poslova, ocijeniti utjecaj na obradu podataka te financijske učinke.
2. Kada je god moguće, treba objaviti natječaj za odabir između više pružatelja usluga.
3. Pružatelj usluge trebao bi biti odabran nakon procjene njegovog ugleda, iskustva u vrsti tražene usluge, ponudama i jamstvima.
4. Unaprijed je potrebno planirati revizije svih segmenata pruženih usluga kako bi se ocijenila kvaliteta izvedbe pružatelja usluge. Ukoliko poduzeće nema dovoljno znanja i resursa, treba angažirati specijalnu tvrtku koja se bavi revizijom iz segmenta ugovorene usluge.
5. Ugovori o pružanju usluga i definirane razine usluga moraju dogovaraju se između Poduzeća Polion d.o.o. i pružatelja usluge.
6. Pružatelj usluge mora dobiti odobrenje Poduzeća Polion d.o.o. ako namjerava angažirati treću stranu (podugovaratelja) na poslovima pružanja ugovorene usluge, funkcije ili procesa.

Polion d.o.o.
Obrtnička 12
32100 Vinkovci

t: 032 332 784
f: 032 332 784
e: info@polion.hr

OIB: 26195613045
IBAN: HR2223400091100164230
www.polion.hr

ISO 9001:2015; ISO 14001:2015
Cro Cert

Vlasništvo i odobrenje dokumenta

Voditelj informatičkog odjela, ugovorni suradnik Poduzeća Polion d.o.o.. Vlasnik dokumenta mora izvršiti reviziju informatičkog sustava sukladno prethodno navedenim zahtjevima. Trenutna verzija ovog dokumenta dostupna je svim djelatnicima Poduzeća Polion d.o.o. na lokaciji Obrtnička 12, Vinkovci te je javno objavljena na Internet stranicama na lokaciji www.polion.hr

Politiku je odobrila uprava Poduzeća Polion d.o.o. dana 25.05.2018.g.

Odobrio:

Evidencija povijesti promjena

R.br	Opis izmjene	Izmjenu odobrio	Datum izmjene