eDelivery Network for Croatian Crafts

POLITIKA INFORMACIJSKE SIGURNOSTI

Inačica dokumenta: 1.0
Datum dokumenta: 15. ožujka 2022.
Dokument izradili: Sanja Želinski Matunec, Sanja Martinovsky, Branko Zubak, Dražen Barić
Dokument odobrio: Darko Glujić
Vlasnik dokumenta: direktor DB informatike d.o.o.
Razina povjerljivosti: JAVNO

SADRŽAJ

1. Namjena

Ovaj dokument se primjenjuje na svu dokumentaciju i aktivnosti unutar sustava elektroničke preporučene dostave "eDelivery Network for Croatian Crafts".
Informacije čine ključnu imovinu DB informatike d.o.o. (dalje u tekstu DB informatika). Korištenje pravodobnih, točnih i potpunih informacija, s obzirom na njihov utjecaj na poslovanje i upravljačko odlučivanje, ključni su za ostvarivanje poslovnih ciljeva DB informatike. Svjesni njihova značaja, DB informatika kontinuirano upravlja svim rizicima kojima je izložena, a u cilju ispunjenja temeljnih načela informacijske sigurnosti, posebice onim rizicima koji se odnose na informatičku tehnologiju i druge pridružene tehnologije te rizicima koji proizlaze iz korištenja informacijskog sustava.
Namjena ovog dokumenta je uspostaviti okvir za sustav upravljanja informacijskom sigurnošću s konačnim ciljem osiguranja kontinuiteta poslovnih procesa DB informatike.
Način provođenja pojedinih aktivnosti koji proizlaze iz ovdje definiranih odredbi propisani su u dodatnim dokumentima u formi pravilnika, politika, metodologija, obrazaca, planova, uputa itd.

2. Pojmovnik

"**informacija**" znači svaki podatak u fizičkom ili elektroničkom obliku koji se kreira, obrađuje, pohranjuje, prenosi, štiti i uništava u okviru informacijskog sustava.
Informacije čine imovinu koja je, kao i druga važna poslovna imovina, bitna za poslovanje DB informatike te ju je stoga potrebno primjereno zaštititi. Informacije se mogu pohraniti u različitim oblicima: digitalnom (npr. datoteke pohranjene na elektroničkom ili optičkom mediju), fizičkom (npr. na papiru) ili kao skrivene informacije u obliku znanja zaposlenika. Informacije se mogu prenositi različitim sredstvima prijenosa uključujući fizičku, elektroničku ili verbalnu komunikaciju. Bez obzira na njenu formu ili način prijenosa, informaciju treba uvijek odgovarajuće zaštiti.
U današnje vrijeme informacije su ovisne o informacijskoj i komunikacijskoj tehnologiji. Ova tehnologija često je bitan faktor koji olakšava kreiranje, obradu, pohranu, prijenos, zaštitu i uništavanje informacija.;
"**informacijska imovina**" uključuje podatke u bazama podataka, datoteke s podacima, programski kôd, sistemsku i aplikacijsku dokumentaciju, korisničke priručnike, planove, interne akte i slično;

"**informacijska sigurnost**" znači očuvanje povjerljivosti, integriteta i raspoloživosti informacija. Dodatno, u značenje se mogu obuhvatiti i druga svojstva, poput autentičnosti, neporecivosti, dokazivosti i pouzdanosti.
Informacijska sigurnost uključuje primjenu i upravljanje odgovarajućim kontrolama koje uključuju razmatranje širokog spektra prijetnji s ciljem osiguranja kontinuiteta poslovanja, te ublažavanja posljedica incidenata informacijske sigurnosti.
Informacijska sigurnost postiže se provedbom niza mjera, odabranih kroz proces upravljanja rizikom i sustavom upravljanja informacijskom sigurnošću, uključujući politike, procese, postupke, organizaciju, softver i hardver za zaštitu identificirane informacijske imovine. Te se mjere moraju definirati, provoditi, pratiti, pregledavati i unapređivati prema potrebi kako bi se osiguralo da se zadovolje zahtjevi informacijske sigurnosti i poslovni ciljevi organizacije. Očekuje se da se mjere informacijske sigurnosti učinkovito integriraju u poslovne procese organizacije.;
"**informacijski sustav**" znači sveobuhvatnost tehnološke infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima. Informacijski sustav moguće je definirati i kao međudjelovanje informacijske tehnologije, podataka i postupaka za procesiranje podataka te ljudi koji prikupljaju navedene podatke i njima se koriste;
"**korisnici informacijskog sustava**" su sve osobe koje se koriste informacijskim sustavom;
"**povjerljivost**" znači svojstvo informacija (podataka) da nisu dostupne ili otkrivene neovlaštenim subjektima;
"**integritet**" znači svojstvo informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani;
"**raspoloživost**" znači svojstvo informacija i procesa koje omogućuje pristup tim informacijama i procesima te njihovu upotrebljivost, tj. njihovu dostupnost na zahtjev ovlaštenog subjekta;
"**autentičnost**" znači svojstvo koje osigurava da je identitet subjekta zaista onaj za koji se tvrdi da jest;
"**neporecivost**" znači svojstvo koje osigurava nemogućnost poricanja izvršene aktivnosti ili primitka informacije (podatka);
"**dokazivost**" znači svojstvo koje osigurava da aktivnosti subjekta mogu biti praćene jedinstveno do samog subjekta;

"**pouzdanost**" znači svojstvo dosljednoga, očekivanog ponašanja i rezultata;
"**resursi informacijskog sustava**" uključuju računalne aplikacije, infrastrukturu, informacije i ljude;
"**rizik informacijskog sustava**" znači rizik koji proizlazi iz korištenja informacijske tehnologije odnosno informacijskog sustava;
"**sustav upravljanja informacijskom sigurnošću**" znači upravljački okvir za sustavni pristup uspostavi, provedbi, radu, praćenju, nadzoru, održavanju i unapređivanju informacijske sigurnosti koji uključuje organizaciju, pravila, odgovornosti, planove, procese i resurse informacijskog sustava;
"**temeljna načela informacijskog sustava**" znači, ovisno o kontekstu, jedno ili kombinaciju načela povjerljivosti, integriteta, raspoloživosti, neporecivosti, dokazivosti, autentičnosti i pouzdanosti;
"**neželjeni događaj (incident**)" znači bilo koji događaj koji može uzrokovati neželjene ili neočekivane posljedice i možebitne izravne ili neizravne materijalne, financijske i druge štete;
"**vlasnik informacije**" znači osoba u okviru čijeg djelovanja je određena informacija nastala. Ovom politikom pod vlasnikom informacije smatra se vlasnik procesa odnosno voditelj organizacijske jedinice, koji je odgovoran za klasifikaciju informacija, odobravanje i ukidanje pristupa informacijama ili određivanje potrebnih mjera zaštite informacija.

3. Uvodne odredbe

Članak 1.

Ovom Politikom direktor DB informatike (dalje u tekstu Direktor) uspostavlja sustav te propisuje osnovna načela upravljanja informacijskom sigurnošću (dalje: Sustav upravljanja informacijskom sigurnošću), ponajprije na sljedeće načine:

- Usvajanjem ove Politike, Direktor izražava svoju obvezu zaštite informacijske sigurnosti i uspostavlja okvir za upravljanje informacijskim sustavom DB informatike;
- Uspostavom adekvatne organizacijske strukture, imenovanjem ključnih funkcija i odbora odgovornih za upravljanje sustavom informacijske sigurnosti;
- Osiguranjem prikladnog broja izvršitelja potrebnih vještina te osiguranjem potrebnog proračuna;

- Usvajanjem dodatnih internih akata kojima se detaljnije reguliraju pojedina područja Sustava upravljanja informacijskom sigurnošću;
- Usvajanjem okvira za upravljanje rizicima informacijske sigurnosti;
- Primjenom odgovarajućih upravljačkih, logičkih i fizičkih mjera zaštite informacijskih resursa;
- Kontinuiranom edukacijom zaposlenika o važnosti informacijske sigurnosti;

Ovom Politikom Direktor izjavljuje i potvrđuje da je ciljeve informacijske sigurnosti prihvatio jednako odgovorno i svjesno kao i ostale ciljeve te da ih promatra u cjelini s ostalim poslovnim ciljevima.

Članak 2.

Svrha ove Politike je uspostaviti upravljački okvir i definirati načela upravljanja informacijskom sigurnošću u kontekstu očuvanja integriteta, povjerljivosti i raspoloživosti informacijske imovine, te pravnih i poslovnih interesa DB informatike.
Zajedno s "Politikom zaštite pojedinaca u vezi s obradom osobnih podataka", "Općim pravilima pružanja usluge elektroničke preporučene dostave" i "Uvjetima i odredbama usluge elektroničke preporučene dostave" ova Politika definira okvir za uspostavljanje upravljačkih, logičkih i fizičkih mjera zaštite resursa informacijskog sustava zasnovane na pristupu upravljanja rizicima, a u skladu s mjerama koje proizlaze iz dobre prakse.

Članak 3.

Ova Politika primjenjuje se na cjelokupni informacijski sustav DB informatike (informacijsku imovinu, tehnologiju, organizaciju, ljudske resurse i postupke za prikupljanje, obradu, pohranu, prijenos, zaštitu i zbrinjavanje informacija) uključivo eksternalizirane usluge i sve njegove korisnike (zaposlenike DB informatike na neodređeno ili određeno vrijeme, poslovne suradnike i druge osobe koji su na bilo koji način uključene u proslovne procese DB informatike, članove Uprave, vanjske dobavljače/pružatelje usluga i njihove zaposlenike te korisnike usluga DB informatike i zaposlenike korisnika usluga ako su pravne osobe).
Svi korisnici informacijskog sustava DB informatike trebaju biti upoznati s odredbama ove Politike i pridržavati ih se.

Članak 4.

Ova Politika temeljni je okvir za upravljanje informacijskom sigurnošću i odražava prihvaćena načela sigurnosti.

Direktor donosi i druge interne akte radi zaštite informacijske imovine i sustava u skladu s poslovnim potrebama i sigurnosnim zahtjevima.

4. Sustav upravljanja informacijskom sigurnosti

Članak 5.

Sustav upravljanja informacijskom sigurnošću skup je pravila, procedura, smjernica, aktivnosti i povezanih resursa kojima DB informatika upravlja u cilju zaštite "resursa informacijskog sustava" i poslovnih procesa DB informatike. DB informatika na taj način ostvaruje sustavni pristup uspostavi, radu, nadzoru, održavanju i unapređivanju informacijske sigurnosti u svrhu ostvarivanja poslovnih ciljeva i zaštite temeljnih načela informacijskog sustava.

Članak 6.

Direktor uspostavlja ovom Politikom organizacijski i upravljački okvir.

Ključne funkcije u upravljanju informacijskom sigurnošću čine Direktor, Voditelj sigurnosti informacijskog sustava i voditelji organizacijskih dijelova DB informatike.

Odgovornosti ključnih funkcija i ostalih uloga u sustavu upravljanja informacijskom sigurnošću definirane su sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Članak 7.

Sustav upravljanja informacijskom sigurnošću DB informatike zasniva se na sljedećim načelima koja su nužna za njegovu uspješnu implementaciju:

- Upravljački okvir
  DB informatika će uspostaviti adekvatnu organizacijsku strukturu, poslovne funkcije, odbore i procese za primjereno upravljanje informacijskom sigurnošću te definirati njihove odgovornosti.
- Pristup zasnovan na upravljanju rizicima
  DB informatika identificira, određuje prioritete i adresira rizike koji proizlaze iz ko-

rištenja informacijskih tehnologija na dosljedan i učinkovit način te primijeniti odgovarajuće mjere za zaštitu informacijske imovine i sustava i ublažavanje rizika na prihvatljivu razinu.

- Zaštita informacijske imovine
  DB informatika štiti povjerljivost, cjelovitost i integritet informacija tijekom obrade, u prijenosu i pohrani. Pritom se treba voditi načelima zabrane svih radnji koje nisu eksplicitno dopuštene i dodjele minimalnih ovlasti koje omogućuju djelotvorno poslovanje.
- Prevencija, otkrivanje, odgovor, oporavak
  DB informatika primjenjuje zaštitne mjere koje će osigurati učinkovitu prevenciju, otkrivanje, odgovor i oporavak informacijskog sustava u slučaju neželjenog događaja. Preventivnim mjerama se izbjegavaju ili odvraćaju pojave neželjenog događaja, mjerama nadzora ih pravovremeno identificiramo, učinkovitim odgovorom zaustavljamo i ograničavamo štetu, a mjerama oporavka osiguravamo obnovu povjerljivosti, cjelovitosti i dostupnosti informacijskog sustava u očekivano stanje.
- Edukacija korisnika
  DB informatika će kontinuirano educirati korisnike informacijskog sustava kako bi osigurala da njihova znanja i kompetencije prate promjene u informacijskom sustavu, sigurnosne zahtjeve te vanjske utjecaje koji bi mogli utjecati na sigurnost informacijskog sustava.
- Dokazivost i neporecivost
  DB informatika će osigurati dokazivost i neporecivost radnji korisnika informacijskog sustava kako bi bila u mogućnosti rekonstruirati njihove aktivnosti i utvrditi osobnu odgovornost.
- Kontinuirano praćenje i unapređivanje informacijske sigurnosti
  DB informatika će uspostaviti kontinuirani proces praćenja i unapređivanja efikasnosti informacijske sigurnosti kako bi se prilagođavala promjenama u okruženju i tehnologiji. Mjere zaštite trebaju biti periodički procjenjivane kako bi se osigurala njihova učinkovitost i ispunila svrha njihove primjene.

- Upravljanje kontinuitetom poslovanja
  DB informatika će uspostaviti poslovno-upravljački sustav s ciljem osiguranja kontinuiranog procesa uspostave i unaprjeđenja mogućnosti da strateški planira i spremno dočekuje prekide u poslovanju, minimizira negativan učinak te brzo i efikasno oporavi kritične poslovne aktivnosti na prihvatljivu razinu.
- Revizija
  DB informatika će omogućiti neovisnu i objektivnu provjeru adekvatnosti upravljanja informacijskom sigurnošću i sustavom.

Članak 8.

Imovinu informacijskog sustava mora identificirati te izraditi i održavati njen popis ažurnim i usklađenim s drugim evidencijama. Imovini informacijskog sustava mora dodijeliti vlasnika. DB informatika upravlja imovinom informacijskog sustava tijekom njenog životnog vijeka na način kako je definirano sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.
Korisnici informacijskog sustava smiju koristiti softversku i hardversku imovinu na način propisan u zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Članak 9.

DB informatika klasificira informacijsku imovinu u smislu zakonskih zahtjeva, vrijednosti, kritičnosti i osjetljivosti na neovlašteno otkrivanje, promjenu ili nedostupnost, na način kako je definirano sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Članak 10.

Pristup informacijama korisnicima informacijskog sustava se odobrava u skladu s poslovnim zahtjevima, samo do razine koja omogućava izvršavanje radnih zadataka korisnika, skladno njegovoj ulozi i klasifikaciji informacija.
Za utvrđivanje jedinstvenog identiteta korisnika informacijskog sustava provodi se procedura registracije i de-registracije korisnika te provjere autentičnosti korisnika koja može, ovisno o osjetljivosti informacija kojima se pristupa, uključivati više elemenata autentifikacije. Proces registracije i de-registracije korisnika, kao i upravljanje i zaštita elemenata autentifikacije, provodi se na način propisan u zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Korisnicima s pravom povlaštenog pristupa komponentama informacijskog sustava DB informatike potrebno je uvesti dodatne kontrole koje umanjuju rizik od namjerne ili nenamjerne zlouporabe sustava. Razgraničenje dužnosti korisnika s pravom povlaštenog pristupa provodi se tamo gdje je to moguće.
Udaljeni pristup informacijskom sustavu DB informatike propisuje se sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Članak 11.

DB informatika provodi mjere fizičke sigurnosti radi zaštite resursa informacijskog sustava od neovlaštenog pristupa i opasnosti povezanih s okolišem. Uređaji za obradu podataka smješteni su u sigurnim područjima, fizički zaštićenima od neovlaštenog pristupa, oštećenja i ometanja. Uspostavljene su slojevite unutarnje i vanjske sigurnosne kontrole kako bi se spriječio neovlašteni pristup resursima informacijskog sustava i zaštitila temeljna načela informacijskog sustava.

Članak 12.

Direktor uspostavlja sveobuhvatan okvir upravljanja rizikom informacijskog sustava. Sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi definiran je proces, uloge, odgovornosti i ciljevi upravljanja rizicima informacijskog sustava, a proces je integriran u životni ciklus upravljanja informacijskim sustavom.
Procjena sigurnosnog rizika se provodi s ciljem identifikacije specifičnih prijetnji informacijskom sustavu i njegovih ranjivosti. Procjena sigurnosnog rizika provodi se periodički kako bi se ustanovile promjene u oblicima prijetnji prema informacijskom sustavu i promjene u organizacijskim prioritetima.
Voditelj sigurnosti je odgovoran za pokretanje i provedbu postupka procjene sigurnosnih rizika.
Rezultati procjene sigurnosnog rizika odrediti će prioritete mjera i akcija koje moraju biti provedene u provedbi sustava zaštite.
Troškovi primjene mjera sigurnosti moraju biti razmjerni s osjetljivošću i vrijednošću informacije koje se takvim mjerama štite.

Članak 13.

Direktor uspostavlja okvir za upravljanje kontinuitetom poslovanja kao jednim od ključnih elemenata upravljanja sigurnošću poslovanja i smanjenja operativnih rizika. Sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi definiran je proces, uloge, odgovornosti i ciljevi upravljanja kontinuitetom poslovanja, a proces je integriran u životni ciklus upravljanja informacijskim sustavom.
U okviru procesa upravljanja kontinuitetom poslovanja, DB informatika priprema, redovito usklađuje i testira planove kontinuiteta poslovanja i oporavka informacijskog sustava DB informatike.

Članak 14.

Direktor uspostavlja okvir za upravljanje incidentima i povredama načela informacijske sigurnosti s ciljem pravovremenog i učinkovitog odgovora na neplanirane događaje koji mogu ugroziti temeljna načela informacijske sigurnosti DB informatike. Proces, uloge, odgovornosti i ciljevi upravljanja povredama informacijske sigurnosti definiraju se sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.
Svi korisnici informacijskog sustava DB informatike dužni su prijaviti svaki događaj za koji sumnjaju da predstavlja povredu načela informacijske sigurnosti.

Članak 15.

Svaka promjena na sustavu mora biti planirana, izvođenje promjena odobreno, a rezultati promjene dokumentirani. Prije provođenja promjene većeg obima mora se obaviti analiza utjecaja promjene na sigurnost informacijskog sustava i dokumentirati sigurnosne zahtjeve i mjere neophodne za siguran rad sustava.
Upravljanje promjenama informacijskog sustava DB informatike propisuje se sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Članak 16.

Potrebno je redovito izrađivati zaštitne kopije produkcijskih podataka. Zaštitne kopije moraju biti izrađene i pohranjene na primjeren način, u dovoljnom broju kopija, a prema potrebi i na lokaciji dovoljno udaljenoj od lokacije na kojoj su izrađene.
Potrebno je periodično uvježbavati postupak obnove podataka sa zaštitnih kopija.

Upravljanje pričuvnom pohranom informacijskog sustava DB informatike propisuje se sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Članak 17.

Na aktivnoj opremi informacijskog sustava moraju se provoditi mjere zaštite od virusa i drugih malicioznih programa.
Upravljanje zaštitom od malicioznog koda informacijskog sustava Zaklade propisuje se sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Članak 18.

Kibernetička sigurnost obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada tome značajno pridonosi.
Potrebno je kontinuirano provoditi mjere kako bi razina zaštite u svakom području bila proporcionalna s povezanim rizicima i mogućnostima ograničavanja prijetnji koje ih uzrokuju.
Upravljanje kibernetičkom sigurnošću informacijskog sustava DB informatike propisuje se sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Članak 19.

Razvoj ili unapređivanje informacijskog sustava mora uzeti u obzir sigurnosne zahtjeve.
Upravljanje razvojem informacijskog sustava DB informatike propisuje se sukladno zahtjevima za pružatelja usluge povjerenja prema eIDAS uredbi.

Članak 20.

Direktor uspostavlja kontinuirani proces kojim se informira, osvješćuje i educira korisnike informacijskog sustava o promjenama funkcionalnosti i sigurnosnih obilježja informacijskog sustava DB informatike te prijetnjama informacijskoj sigurnosti i primjerenim načinima zaštite.
Program obrazovanja utvrđuje Voditelj sigurnosti informacijskog sustava u suradnji s Direktorom. Pritom, edukacija treba:

- Obuhvatiti sve korisnike informacijskog sustava DB informatike, uključivo vanjske korisnike te zaposlenike tvrtki dobavljača/isporučitelja;

- Razviti i održavati znanja i vještine korisnika na primjerenoj razini kako bi mogli obavljati poslovne zadatke na djelotvoran i siguran način;
- Upoznati korisnike s internim politikama, procedurama i ostalim postupcima kojih se moraju pridržavati kako bi se točno utvrdili zadaci, opseg djelovanja i osobna odgovornost svakog korisnika;
- Uspostaviti i unapređivati svijest o potrebi zaštite resursa informacijskog sustava DB informatike;
- Razviti i održavati znanja potrebna da bi se funkcionalnost i sigurnost informacijskog sustava zadržale na zadovoljavajućoj razini tijekom cijelog životnog ciklusa informacijskog sustava.

Edukaciju je moguće provoditi putem informiranja ili organiziranim složenijim edukacijama. Opseg, detaljnost, trajanje i način provođenja edukacije trebaju biti u skladu s potrebama ciljane grupe korisnika te opsežnosti i kompleksnosti tematike.

5. Završne odredbe

Članak 21.

Ova Politika ili pojedini njeni dijelovi mogu se objaviti na mrežnoj stranici DB informatike. Politika se mora pregledati redovito, najmanje jednom godišnje, ili u slučaju kada se dogode značajne promjene sustava upravljanja informacijskom sigurnošću kako bi se osigurala trajna prikladnost, primjerenost i djelotvornost.

Članak 22.

Povreda odredbi Politike sigurnosti informacijskog sustava predstavlja tešku povredu ugovora o radu i može biti razlog izvanrednog otkaza ugovora o radu ili otkazivanja ugovorene usluge vanjskim dobavljačima.

Članak 23.

Ova Politika stupa na snagu i primjenjuje se danom donošenja.