POLITIKA
INFORMACIONE BEZBJEDNOSTI

Podgorica, mart 2024.

ISTORIJA DOKUMENTA

Verzija	Autor	Opis	Akcija*	Stranica/Poglavlje	Datum usvajanja
24.1		Inicijalna verzija			

(*) Akcija: C=Kreirano, I=Dodato, R=Zamijenjeno, D=Izbrisano

Sadržaj

Skraćenice

DP	Direktorat za plaćanja
IS	Informacioni sistem
IB	Informaciona bezbjednost
PIB	Politika informacione bezbjednosti
SIB	Savjetnik za informacionu bezbjednost
DIT	Direkcija za IT

Definicije pojmova

- ***Informacioni sistem (IS)*** je integrisani skup komponenti za sakupljanje, snimanje, čuvanje, obradu i prenošenje podataka.
- ***Informaciona bezbjednost*** (IB) podrazumijeva stanje povjerljivosti, cjelovitosti i dostupnosti podataka.
- ***Podatak*** je informacija, poruka i dokument sačinjen, poslat, primljen, zabilježen, skladišten ili prikazan elektronskim, optičkim ili sličnim sredstvom, uključujući prenos internetom i elektronsku poštu.
- ***Povjerljivost podatka*** podrazumijeva da je podatak dostupan samo licima koja su ovlašćena da ostvare pristup ili postupe sa tim podatkom.
- ***Cjelovitost (integritet) podatka*** podrazumijeva očuvanje postojanja, tačnosti i kompletnosti podatka, kao i zaštitu procesa ili programa koji sprječavaju neovlašćeno mijenjanje podatka.
- ***Dostupnost podatka*** podrazumijeva da ovlašćeni korisnici mogu da pristupe podatku uvijek kada za tim imaju potrebu.
- ***Resursi informacionog sistema***, osim ljudi i procesâ, uključuju:
  - **Hardverska imovina** – računari i računarska oprema, komunikaciona oprema, sistemi za skladištenje podataka kao i ostala tehnička oprema koja podržava rad informacionog sistema
  - **Softverska imovina** – operativni sistemi, programi za nadzor informacionog sistema, sigurnosni programi, korisnički programi, programi za upravljenje bazama podataka, alati za razvoj programa, uslužni programi i ostali programi koji se nalaze na informacionim sistemima.
  - **Informaciona imovina** – podaci u bazama podataka, dokumenta sa podacima, programski kod u tekstualnom obliku, dokumentacija o informacionim sistemima i programima, priručnici, planovi i usluge informacionog sistema.
- ***Informacione tehnologije (IT)*** su kombinacija softverske i hardverske imovine koja omogućava automatizovano generisanje, prikupljanje, obradu, čuvanje, prenos, prikazivanje i/ili korišćenje informacija.
- ***IT sistem*** je informaciona tehnologija uređena kao dio mehanizma ili međusobno povezane mreže koja pruža podršku poslovanju.

- ***IT servis*** je usluga koju IT sistem pruža unutrašnjim ili spoljnim korisnicima informacionog sistema.
- ***Incident*** je jedan ili više povezanih događaja koji nijesu planirani, a koji su ili će vjerovatno narušiti sigurnost ili funkcionalnost informacionog sistema.

Svrha i obuhvat PIB-a

Politika informacione bezbjednosti predstavlja krovni dokument u kome se definišu vodeća načela i odgovornosti potrebne za zaštitu informacionog sistema Direktorata za plaćanja (DP).

Svrha PIB-a je obezbjeđivanje bezbjednosnih okvira koji će osigurati zaštitu podataka DP od neovlašćenog pristupa, gubitka i oštećenja, kao i njihove zloupotrebe, dok će istovremeno podržavati potrebe za sigurnom razmjenom informacija.

PIB predstavlja namjeru i odlučnost rukovodstva DP da uspostavi i obezbijedi efikasan i siguran IS, kao i da osigura da upravljanje informacionom bezbjednošću bude integrisano sa ostalim procesima i cjelokupnom strukturom upravljanja te da bude uzeto u obzir pri projektovanju procesa, informacionih sistema i internih kontrola.

Područje primjene

PIB se odnosi na sve zaposlene u DP i na ostale pojedince i subjekte koji su na bilo koji način uključeni u poslovne procese na osnovu ugovorenih ili drugih obaveza i imaju odobren pristup podacima IS DP.

Svi gore navedeni dužni su potpisati “Izjavu o prihvatanju PIB-a” i pridržavati se njenih odredbi, u cilju osiguranja pravilnog rada informacionog sistema, a u svrhu očuvanja neprekidnog poslovanja.

PIB se takođe primjenjuje na cjelokupnu informacionu strukturu DP, uključujući sve resurse informacionog sistema.

Ciljevi politike informacione bezbjednosti

- Uspostavljanje većeg kvaliteta upravljanja bezbjednošću IS;
- Obezbjeđenje usklađenosti sa zakonskom regulativom, relevantnim svjetskim standardima, kao i strategijom i planovima DP;
- Smanjenje štete od potencijalnih sigurnosnih incidenata;
- Povećanje nivoa svijesti korisnika o potrebi zaštite informacija i resursa u IS DP;
- Postizanje bolje reputacije DP i povećanje povjerenja klijenata.

Načela upravljanja informacionom bezbjednošću

1) Načelo usklađenosti – kontrole će se primjenjivati u skladu sa zakonskom regulativom i odabranim svjetskim standardima iz oblasti upravljanja IB.

2) Načelo sveobuhvatne zaštite – kontrole će se primjenjivati na svim organizacionim, fizičkim, tehničkim i logičkim nivoima, kao i tokom cjelokupnog životnog ciklusa IS.

3) Načelo svjesnosti i osposobljenosti – sve osobe koje svojim aktivnostima potencijalno ili efektivno utiču na bezbjednost IS treba da budu svjesne rizika i posjeduju odgovarajuća znanja i vještine za posao koji obavljaju.

Uloge i odgovornosti

Bezbjednost IS nije u nadležnosti isključivo SIB ili Direkcije za IT (DIT), već svih koji odlučuju, koriste ili učestvuju u radu informacionog sistema. U skladu sa tim, prepoznato je 5 glavnih uloga: direktor DP, Direkcija za IT, samostalni savjetnik za informacionu bezbjednost (SIB), rukovodioci organizacionih jedinica i korisnici IS.

Direktor DP je odgovoran da:

- pokaže posvećenost u odnosu na sistem upravljanja bezbjednošću IS;
- osigura da su dodijeljene i saopštene odgovornosti i ovlašćenja za relevantne uloge u sistemu upravljanja bezbjednošću IS;
- obezbijedi raspoloživost resursa potrebnih za upravljanje informacionom bezbjednošću;
- obezbijedi integrisanje zahtjeva sistema upravljanja bezbjednošću IS u ostale poslovne procese.

SIB je odgovoran da:

- periodično priprema izvještaje o informacionoj bezbjednosti i predlaže mjere za unapređenje;
- koordinira i dokumentuje aktivnosti vezano za politiku bezbjednosti, implementaciju i uvođenje poboljšanja;
- definiše sigurnosne kontrole unutar projektnih specifikacija i procjenu troškova za njihovo sprovođenje;
- ažurira dokumentaciju koja se odnosi na PIB.

DIT je odgovorna da kreira i održava registar resursa IS, kao i da sprovodi u djelo interne kontrole koje SIB definiše u procesu upravljanja bezbjednošću IS.

Rukovodioci organizacionih jedinica su odgovorni da nadziru sprovođenje PIB u svojim područjima rada i prenose politiku zaposlenima.

Korisnici informacionog sistema su sve osobe (zaposleni u DP, pružaoci usluga ili eksterni partneri) koji imaju pristup IS DP, shodno svojoj ulozi u poslovnim procesima. Dužnost je korisnika IS da:

- odgovorno koriste sve resurse IS koji su im dodijeljeni za potrebe izvršavanja radnog procesa;
- obavijeste svog neposrednog nadređenog i SIB-a o svim incidentima ili nepravilnostima koji mogu da ugroze bezbjednost IS.

Kontrole za sprovođenje PIB

Sigurnosni zahtjevi

Pravila bezbjednosti za kontrolu opreme i procesa moraju biti u skladu sa DP procedurama.

Primjena politike informacione bezbjednosti mora redovno biti predmet kontrole i nadzora. Ako se ustanovi da se sigurnosni proces može promijeniti ili poboljšati, te izmjene se i uvode.

U cilju smanjenja mogućnosti neovlašćene ili nenamjerne modifikacije ili zloupotrebe imovine treba primjenjivati princip “segregacije dužnosti” (tzv. “princip četiri oka”) kako bi se razdvojile konfliktne dužnosti i područja odgovornosti.

Svakom pojedincu treba omogućiti pristup informacijama na osnovu njegovih poslovnih potreba. Takođe, svaki pojedinac treba da dobije minimum privilegija neophodnih za obavljanje određenih aktivnosti.

Upravljanje resursima IS

Resursi IS moraju biti identifikovani i dokumentovani. Odgovornost je vlasnika imovine da se imovina za koju su zaduženi popiše, primjereno klasifikuje i zaštiti, te pravovremeno izbriše i adekvatno uništi.

DP zadržava pravo nadzora nad upotrebom resursa IS, kao i pravo bilježenja svih korisničkih aktivnosti na IS. U skladu sa tim, DP ne može garantovati zaštitu privatnosti korisnika u IS DP. Takođe, DP zadržava pravo ograničavanja pristupa pojedinim uslugama ili resursima IS.

Svi zaposleni su dužni da na primjeren, profesionalan i zakonit način koriste resurse IS. DP dozvoljava povremeno, ograničeno i odgovarajuće korišćenje interneta u privatne svrhe ukoliko se time ne krše poslovni principi DP.

Bez saglasnosti DIT-a nije dozvoljeno instaliranje bilo kakvih programskih paketa ili uređaja na računarima u DP.

Kako bi se osiguralo da će informacije i informaciona imovina biti zaštićeni na odgovarajući način, resursi IS moraju biti klasifikovani u skladu sa njihovim značajem za DP. Klasifikaciju vrši vlasnik resursa.

Preporučuje se izbjegavanje korišćenja prenosivih medijuma. Ukoliko postoji opravdana poslovna potreba, prenosivi medijumi se moraju čuvati sa posebnom pažnjom.

Fizička bezbjednost

Fizička bezbjednost mora biti sprovedena kako bi spriječili neovlašćeni pristup, oštećenje i prekide u radu informacionog sistema.

Preporučuje se korišćenje "politike praznog stola" u cilju zaštite papirnih dokumenata i prenosivih medijuma za skladištenje podataka, kao i "politike praznog ekrana" za elektronska sredstva za obradu informacija (npr. odjaviti se sa sistema ili zaključati ekran – eng. screensaver sa lozinkom).

Kontrola pristupa sistemu

Pristup informacionom sistemu DP mora biti strogo kontrolisan. Vlasnici resursa IS su odgovorni da odobre pravo pristupa resursima za koje su nadležni. Pristup se odobrava samo u onim slučajevima kada postoji jasna poslovna potreba i dok postoji potreba za pristup.

Svi zaposleni DP koji imaju pristup ličnim podacima treće strane, moraju raditi prema "Zakonu o zaštiti podataka o ličnosti" (Službeni list Crne Gore 79/08, 70/09, 44/12 i 22/17).

Prilikom dodjele pristupnih prava i privilegija treba uzeti u obzir i da dodijeljena prava pristupa obezbjeđuju adekvatnu segregaciju dužnosti, tj. da korisnicima nije dodijeljena kombinacija prava pristupa koja im omogućava zaobilaženje kontrola.

U slučaju prestanka radnog odnosa, pristupna prava se ukidaju bez odlaganja.

Aktivnosti korisnika, a naročito aktivnosti privilegovanih korisničkih naloga moraju se evidentirati u sistemskim i operativnim zapisima (logovima) računara, servera i mrežne opreme. Zapisi se moraju čuvati i štititi u skladu sa kritičnošću resursa IS koji ih je kreirao.

Treba implementirati kontrole da bi se osigurala bezbjednost informacija u mrežama i spriječio neovlašćeni pristup.

Zaštita od zlonamjernog softvera

U cilju smanjenja rizika IS, u informacionom sistemu DP moraju postojati kontrole koje će blagovremeno otkriti, spriječiti i oporaviti IS od zlonamjernog softvera.

Moraju se blagovremeno prikupiti informacije o tehničkim ranjivostima informacionih sistema koji se koriste i preduzeti odgovarajuće aktivnosti uzimajući u obzir pripadajući rizik.

Svi događaji koji upućuju na neočekivano ponašanje sistema moraju odmah biti prijavljeni, a zapoljeni i partneri upoznati sa procedurom za upravljanje incidentima.

Kontinuitet bezbjednosti informacija mora biti ugrađen u proces upravljanja kontinuitetom poslovanja. Moraju se identifikovati poslovni procesi koji zahtijevaju visok nivo dostupnosti.

Rezervne kopije podataka

Neophodno je redovno vršiti rezervne kopije korisničkih podataka i sistemskih konfiguracija. Rezervne kopije podataka moraju biti adekvatno ažurirane, zaštićene i smještene na jednoj ili više lokacija.

Nabavka, razvoj i održavanje sistema

Prilikom nabavke hardvera ili softvera neophodno je slijediti zvanični proces nabavki u DP.

Prilikom razvoja softvera neophodno je uspostaviti i primjenjivati pravila za razvoj u skladu sa najboljom svjetskom praksom. Sigurnost mora biti uključena u svim fazama životnog ciklusa razvoja softvera. Razvojno, testno i produkciono okruženje je potrebno adekvatno razdvojiti.

Prilikom upravljanja projektima na nivou DP neophodno je implementirati sigurnosne aspekte u raznim fazama realizacije projekata.

Odnosi sa pružaocima usluga i eksternim partnerima

Prije započinjanja poslovne saradnje ili dozvole pristupa informacijama i internim sistemima, mora biti potpisan ugovor sa eksternim partnerima u vezi sa tim poslovnim odnosom a koji će sadržati odredbe o mjerama informacione sigurnosti.

Takođe, eksterni partner mora biti upoznat sa elementima Politike informacione bezbjednosti koji se odnose na oblast poslovne saradnje.

Nivo sigurnosnih mjera implementiran u odnosima sa partnerima mora biti ekvivalentan procijenjenoj kritičnosti i obimu poslova koje eksterni partner obavlja za DP.

Dokumentacija

Sva pravila sadržana u PIB-u mogu biti razrađena dodatnim dokumentima. Sva dodatna dokumenta su sastavni dio ove Politike informacione bezbjednosti. U slučaju konflikta u sadržaju politike i dodatnih dokumenata koja iz nje proizlaze, važeća su pravila i tumačenja navedena u PIB.

Svi zaposleni u DP-u moraju biti upoznati sa PIB.

Promjene

Sprovođenje PIB-a je process koji traje. Ažurira se ako postoje promjene u organizaciji, tehnologiji, korišćenju, procedurama, zakonima ili rizicima.

PIB i dodatnu dokumentaciju je neophodno periodično revidirati, a najmanje jednom godišnje.

Nadzor nad politikom informacione bezbjednosti i procedurama

Praćenje i poštovanje procedura

Usklađenost implementacije nivoa bezbjednosti sa PIB mora biti praćena. Svi nalazi se dokumentuju i periodično prijavljuju rukovodstvu DP-a.

Kršenje pravila bezbjednosti i prijava kršenja

Događaji koji nisu u skladu sa PIB, standardima i uputstvima se tretiraju kao njeno kršenje. Svi zaposleni koji uoče takve slučajeve moraju postupati u skladu sa procesom za upravljanje bezbjednosnim incidentima.

Sankcije u slučaju kršenja pravila Politike informacione bezbjednosti

Nepridržavanje PIB-a i dodatnih dokumenata od strane pružaoca usluga i eksternih partnera smatra se povredom ugovornih obaveza koja može biti osnova za raskid ugovora i potraživanje naknade štete pravnim putem.

Prelazne i završne odredbe

Politika informacione bezbjednosti stupa na snagu danom potpisivanja od strane Generalnog direktora DP-a i objavljivanja na web portalima MPŠV.

DIREKTOR
Marko Radonjić

IZJAVA O PRIHVATANJU
POLITIKE BEZBJEDNOSTI INFORMACIJA

Direktorat za plaćanja Ministarstva poljoprivrede, šumarstva i vodoprivrede Crne Gore je uspostavio politiku bezbjednosti informacija u cilju obezbjeđivanja mjera za upravljanje bezbjednošću informacija.

Direktorat za plaćanja mi je obezbijedio obuku i skrenulo pažnju da moram slijediti principe opisane u Politici bezbjednosti informacija i svim ostalim dokumentima koji podržavaju tu politiku. Jasno mi je da moram da je poštujem i da obavijestim Samostalnog savjetnika za informacionu bezbjednost za bilo kakvu sumnju ili problem u vezi sa njom.

Ovim potvrđujem da sam dobio, pročitao, prošao obuku i razumio Politiku bezbjednosti informacija.

Obavezujem se da ću poštovati ovu politiku i svoj rad u operativnim procesima usaglasiti u pogledu pravila, mjera i svih zahtjeva, politika i ostalih akata u okviru organizacije.

Informisan sam da se bilo koji oblik kršenja ovih pravila (namjerno ili nenamjerno) definisanim u politikama bezbjednosti informacija smatra kršenjem radnih i poslovnih obaveza, a ja sam spreman da prihvatim sve materijalne i krivične odgovornosti i posljedice predviđene sporazumima o radu i drugim pravnim aktima u vezi sa radom.

_____ _____

(mjesto i datum davanja izjave) (potpis)