



POLITIKA
KIBERNETIČKE SIGURNOSTI REGOS-a

Sadržaj

1. Uvod.....	3
2. Skraćenice	3
3. Svrha i opseg	4
4. Ciljevi.....	4
5. Uloge i odgovornosti	4
6. Opis procesa upravljanja kibernetičkom sigurnošću	5
7. Mjere upravljanja kibernetičkim sigurnosnim rizicima koje REGOS primjenjuje	6
7.1. Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima.....	7
7.2. Upravljanje programskom i sklopovskom imovinom	7
7.3. Upravljanje rizicima	8
7.4. Sigurnost ljudskih potencijala i digitalnih identiteta	9
7.5. Osnovne prakse kibernetičke higijene	9
7.6. Osiguravanje kibernetičke sigurnosti mreže.....	9
7.7. Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima ...	10
7.8. Sigurnost lanca opskrbe	10
7.9. Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava.....	11
7.10. Primjena kriptografije	11
7.11. Upravljanje sigurnosnim incidentima.....	12
7.12. Kontinuitet poslovanja i upravljanje kibernetičkim krizama.....	12
7.13. Fizička sigurnost	13
8. Provedba Politike	13
9. Pregled i ažuriranje Politike.....	14
10. Završna odredba.....	14
Prilog – Izjava o prihvatanju Politike kibernetičke sigurnosti REGOS-a	15

1. Uvod

U suvremenom digitalnom okruženju, u kojem se broj i složenost kibernetičkih prijetnji neprestano povećava, nužno je osigurati visoku razinu otpornosti informacijskih sustava i sposobnost brzog odgovora na kibernetičke incidente koji mogu ugroziti poslovanje, podatke i ključne usluge Središnjeg registra osiguranika (dalje: REGOS).

REGOS svakodnevno prikuplja, obrađuje i razmjenjuje podatke o osiguranicima koji su nužni za ostvarivanje njihovih prava u sustavu mirovinskog osiguranja. S obzirom na važnost i značaj podataka koji se obrađuju u Informacijskom sustavu REGOS-a, nužno je osigurati odgovarajuću razinu zaštite njihove povjerljivosti, cjelovitosti i dostupnosti kao temeljnih načela kibernetičke sigurnosti. U okviru postupka kategorizacije subjekata, utvrđeno je da REGOS predstavlja ključni subjekt koji ima obvezu provedbe napredne razine mjera kibernetičke sigurnosti.

Politika kibernetičke sigurnosti REGOS-a (dalje: Politika) predstavlja strateški dokument kojim se definiraju ciljevi REGOS-a u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima, organizacijski sustav, raspodjela uloga i odgovornosti. Ovom Politikom uspostavlja se okvir za upravljanje rizicima, jača svijest radnika te osigurava usklađenost s važećim zakonodavstvom i standardima iz područja kibernetičke sigurnosti.

2. Skraćenice

U smislu ove Politike, koriste se sljedeće skraćenice:

- **IS REGOS** – informacijski sustav REGOS-a,
- **IKT sustav** – informacijski i komunikacijski sustav,
- **BCP (eng. Business Continuity Plan)** – plan kontinuiteta poslovanja kojim se definiraju postupci i mjere za održavanje kritičnih poslovnih funkcija u slučaju prekida rada,
- **DRP (eng. Disaster Recovery Plan)** – plan oporavka nakon katastrofe koji definira postupke i resurse potrebne za vraćanje sustava u funkcionalno stanje nakon ozbiljnog kibernetičkog incidenta,
- **EDR (eng. Endpoint Detection and Response)** – sigurnosni sustav za praćenje, analizu i automatski odgovor na prijetnje koje pogađaju krajnje uređaje (računala, poslužitelje, mobilne uređaje),
- **MFA (eng. Multi-Factor Authentication)** - sigurnosni mehanizam kojim se identitet korisnika potvrđuje kombinacijom dvaju ili više različitih faktora (npr. lozinka, sigurnosni token, biometrija),
- **VPN (eng. Virtual Private Network)** – siguran komunikacijski kanal koji omogućuje šifriranu vezu između korisnika i informatičke infrastrukture REGOS-a putem javnih mreža,
- **IDS (eng. Intrusion Detection System)** – sustav za otkrivanje upada koji kontinuirano nadzire mrežni i informacijski promet, analizira događaje i prepoznaje sumnjive ili zlonamjerne aktivnosti koje mogu ukazivati na pokušaj kompromitacije

sustava. IDS sustav ne blokira promet, već upozorava administratore na potencijalne prijetnje,

- **IPS (eng. Intrusion Prevention System)** – sustav za sprječavanje upada koji nadograđuje funkcionalnost IDS-a s mogućnošću automatskog reagiranja na otkrivene prijetnje. IPS ne samo da detektira sumnjive aktivnosti, već može i aktivno blokirati promet ili izolirati ugrožene segmente mreže kako bi spriječio nastanak incidenata.
- **SIEM (eng. Security Information and Event Management)** – sustav za centralizirano prikupljanje, pohranu, korelaciju i analizu sigurnosnih zapisa (logova) iz različitih informacijskih i mrežnih sustava radi pravovremene detekcije, analize i odgovora na sigurnosne incidente.

3. Svrha i opseg

Svrha ove politike je uspostavljanje temeljnih principa, obveza i odgovornosti za zaštitu IS REGOS-a i podataka od kibernetičkih prijetnji.

Ova Politika primjenjuje se na:

- sve radnike REGOS-a, ugovorne partnere koji imaju pristup informacijama, podacima ili IKT sustavima REGOS-a te vanjske suradnike,
- sve IKT sustave, podatkovne baze, aplikacije, poslužitelje, mrežnu infrastrukturu, korisničke uređaje i sigurnosne sustave,
- sve podatke koje REGOS prikuplja, obrađuje ili razmjenjuje s drugim tijelima/organizacijama,
- sve lokacije i procese u vlasništvu ili pod upravljanjem REGOS-a.

4. Ciljevi

Osnovni cilj ove Politike je uspostava okvira za učinkovito upravljanje kibernetičkom sigurnošću radi sprječavanja, otkrivanja i ublažavanja kibernetičkih prijetnji te usklađenost s zakonskim i regulatornim zahtjevima iz područja kibernetičke sigurnosti.

Posebni ciljevi ove Politike su uspostava sustava za učinkovito upravljanje rizicima kibernetičke sigurnosti, kontinuitet poslovanja u kibernetičkim krizama, upravljanje incidentima kibernetičke sigurnosti te jačanje svijesti radnika u području kibernetičke sigurnosti.

5. Uloge i odgovornosti

REGOS primjenjuje načelo razdvajanja uloga i odgovornosti u području kibernetičke sigurnosti s ciljem smanjenja rizika, sprječavanja sukoba interesa i povećanja učinkovitosti. Ovo načelo osigurava da nijedna osoba ne može samostalno inicirati, odobriti i provesti radnju koja bi mogla ugroziti sigurnost IKT sustava. Ako potpuno razdvajanje nije moguće, primjenjuju se dodatne mjere kontrole, poput neovisnih provjera, ograničenja pristupa, dodatnih odobrenja i praćenja aktivnosti.

Posebna pažnja se posvećuje sprječavanju sukoba interesa u obavljanju poslova povezanih s kibernetičkom sigurnošću. Sukob interesa u kibernetičkoj sigurnosti nastaje kada osobni,

financijski ili profesionalni interesi radnika mogu utjecati na objektivnost u procjeni rizika, odabiru tehnologija ili reagiranju na sigurnosne incidente. Postupak za identifikaciju i sprječavanje sukoba interesa u kibernetičkoj sigurnosti uključuje prepoznavanje potencijalnih sukoba interesa, njihovu procjenu, prijavu, primjenu mjera neutralizacije te kontinuiranu edukaciju radnika i dokumentiranje svih koraka.

Ovom Politikom utvrđuju se sljedeće uloge i odgovornosti vezane uz kibernetičku sigurnost:

Ravnatelj REGOS-a – osigurava organizacijske, kadrovske i financijske resurse za provedbu mjera kibernetičke sigurnosti, razmatra izvješća o stanju kibernetičke sigurnosti i donosi odluke o potrebnim poboljšanjima te promiče kulturu kibernetičke sigurnosti.

Voditelj informacijske sigurnosti – koordinira provedbu ove Politike, vodi procjene rizika kibernetičke sigurnosti te izrađuje planove ublažavanja rizika, upravlja incidentima kibernetičke sigurnosti te vodi evidencije o istima, izrađuje sveobuhvatno godišnje izvješće o stanju kibernetičke sigurnosti i provodi edukacije.

Služba kibernetičke sigurnosti – odgovorna je za uspostavu i provedbu politika i procedura kibernetičke sigurnosti za rano upozoravanje, razmjenu informacija o prijetnjama i ranjivostima, uspostavu mjera kibernetičke sigurnosti informacijskih i mrežnih sustava, koordinaciju postupanja u slučaju značajnih kibernetičkih incidenata te suradnju s nadležnim tijelima.

Služba informatičko tehničke podrške – odgovorna je za operativnu provedbu tehničkih i organizacijskih mjera kibernetičke sigurnosti, održavanje sigurnosti IKT sustava te pružanje podrške u sprječavanju, otkrivanju i sanaciji kibernetičkih incidenata.

Voditelj ustrojstvene jedinice – odgovoran je za integraciju kibernetičke sigurnosti u poslovne procese iz svoje nadležnosti te za osiguravanje kontinuiteta pružanja ključnih usluga u skladu s ovom Politikom, propisima i internim aktima REGOS-a.

Radnici – odgovorni su za poštivanje ove Politike, odgovorno korištenje IKT sustava, dodijeljenih pristupnih prava i sredstava rada, čuvanje vjerodajnica i sprječavanje neovlaštenog pristupa te pravodobno prijavljivanje sumnjivih aktivnosti, sigurnosnih slabosti i kibernetičkih incidenata.

Dobavljači i treće strane – odgovorni su za osiguravanje kibernetičke sigurnosti u skladu s ugovorom kojim se definiraju njihove obveze u pogledu zaštite podataka, upravljanja pristupom IKT sustavima, pravodobne prijave sigurnosnih incidenata te poštivanja utvrđenih sigurnosnih politika.

6. Opis procesa upravljanja kibernetičkom sigurnošću

Proces upravljanja kibernetičkom sigurnošću u REGOS-u temelji se na sustavnom pristupu koji uključuje identifikaciju i procjenu rizika, planiranje i implementaciju zaštitnih mjera,

kontinuirano praćenje i nadzor sustava, pravovremeno izvješćivanje, reviziju i unaprjeđenje sigurnosnih procesa radi zaštite informacija i kontinuiteta poslovanja.

Proces upravljanja kibernetičkom sigurnošću obuhvaća:

- **Planiranje i organizaciju** – definiranje okvira i smjernica za kibernetičku sigurnost, jasna podjela odgovornosti te osiguranje potrebnih tehničkih, financijskih i ljudskih resursa za provedbu sigurnosnih mjera,
- **Identifikaciju resursa i prijetnji** – popis i kategorizacija IKT sustava, podataka i potencijalnih prijetnji,
- **Procjenu rizika** – analiza ranjivosti, vjerojatnosti i utjecaja rizika na poslovanje,
- **Planiranje i implementaciju kontrola** – odabir i primjena tehničkih, organizacijskih i proceduralnih mjera zaštite,
- **Praćenje i nadzor** – kontinuirano praćenje sustava, detekcija anomalija i sumnjivih događaja,
- **Upravljanje incidentima kibernetičke sigurnosti** – Pravovremeno otkrivanje i prijava incidenata, analiza uzroka i provođenje korektivnih mjera te testiranje i ažuriranje planova za oporavak od incidenata i katastrofa,
- **Izvješćivanje** – pravovremeno izvješćivanje ravnatelja, radnika i regulatornih tijela,
- **Reviziju i kontinuirano poboljšanje** – praćenje novih prijetnji, ranjivosti i tehnologija, revizija i ažuriranje politike i procedura, evaluacija učinkovitosti mjera kibernetičke sigurnosti te edukacija i podizanje svijesti radnika o kibernetičkoj sigurnosti.

7. Mjere upravljanja kibernetičkim sigurnosnim rizicima koje REGOS primjenjuje

Upravljanje kibernetičkim sigurnosnim rizicima u REGOS-u temelji se na sustavnoj primjeni napredne razine mjera kibernetičke sigurnosti koje uključuju:

1. Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima,
2. Upravljanje programskom i sklopovskom imovinom,
3. Upravljanje rizicima,
4. Sigurnost ljudskih potencijala i digitalnih identiteta,
5. Osnovne prakse kibernetičke higijene,
6. Osiguravanje kibernetičke sigurnosti mreže,
7. Kontrolu fizičkog i logičkog pristupa mrežnim i informacijskim sustavima,
8. Sigurnost lanca opskrbe,
9. Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava,
10. Kriptografiju,
11. Postupanje s incidentima,
12. Kontinuitet poslovanja i upravljanje kibernetičkim krizama,
13. Fizičku sigurnost.

7.1. Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima

Predanost i odgovornost u upravljanju kibernetičkim sigurnosnim rizicima temelji se na pravovremenom prepoznavanju, procjeni i ublažavanju prijetnji, kontinuiranom praćenju sustava, stalnom unaprjeđivanju sigurnosnih mjera kako bi se minimizirali rizici uzrokovani kibernetičkim prijetnjama, incidentima ili nepredviđenim događajima te osigurao kontinuitet poslovanja u kriznim situacijama.

Posebna pozornost posvećuje se sprječavanju sukoba interesa u obavljanju poslova povezanih s kibernetičkom sigurnošću.

Sukob interesa u kibernetičkoj sigurnosti nastaje kada osobni, financijski ili profesionalni interesi radnika mogu utjecati na objektivnost u procjeni rizika, implementaciji ili nadzoru sigurnosnih mjera, odabiru tehnologija i dobavljača te reagiranju na sigurnosne incidente.

U cilju osiguranja objektivnosti, transparentnosti i cjelovitosti u provedbi aktivnosti kibernetičke sigurnosti, REGOS primjenjuje načelo razdvajanja odgovornosti gdje god je to primjenjivo. To načelo osigurava da niti jedna osoba ne može samostalno inicirati, odobriti i provesti radnju koja bi mogla dovesti do ugroze sigurnosti informacijskih sustava.

REGOS nastoji identificirati funkcije i aktivnosti koje zahtijevaju razdvajanje dužnosti, osobito u područjima:

- iniciranja, odobravanja i provedbe promjena u informacijskim sustavima,
- dodjele, izmjene i ukidanja korisničkih prava,
- pristupa i upravljanja konfiguracijama, bazama podataka i sigurnosnim postavkama pojedinih sustava,
- provođenja i revizije sigurnosnih kontrola.

7.2. Upravljanje programskom i sklopovskom imovinom

Upravljanje programskom i sklopovskom opremom predstavlja sastavni dio procesa upravljanja informacijskom imovinom REGOS-a, a uključuje primjenu odgovarajućih pravila te tehničkih i organizacijskih mjera zaštite kako bi se spriječila zlouporaba, gubitak ili neovlašteni pristup imovini.

Pravila i odgovornosti za upravljanje programskom i sklopovskom imovinom utvrđuju se radi osiguravanja potpune evidencije, odgovarajuće razine zaštite, zakonite uporabe te kontinuirane dostupnosti i sigurnosti mrežnih i informacijskih sustava. U okviru tih pravila propisuje se obveza uspostave i održavanja ažurnog registra imovine, klasifikacija imovine prema razini kritičnosti, određivanje vlasništva i odgovornosti, primjena kontrola pristupa, redovito ažuriranje i održavanje programske i sklopovske imovine, kao i sigurnosno zbrinjavanje.

Za provedbu navedenih pravila odgovorni su vlasnici imovine i svi korisnici kojima je imovina dodijeljena na korištenje, svatko u okviru svojih ovlasti i odgovornosti utvrđenih internim aktima.

Identifikacija i klasifikacija imovine provodi se prema utvrđenim razinama kritičnosti kako bi se osiguralo da su najvažnije komponente podvrgnute odgovarajućim sigurnosnim mjerama i nadzoru u skladu s razinom utvrđene kritičnosti.

Kritična imovina predstavlja resurse REGOS-a bez kojih poslovni procesi ne mogu funkcionirati ili čiji gubitak/kompromitacija može uzrokovati velike financijske, pravne ili reputacijske štete.

Ostala (sekundarna) imovina obuhvaća resurse REGOS-a koji nemaju presudan utjecaj na kontinuirano odvijanje poslovnih procesa, pri čemu eventualna nedostupnost te imovine ne bi uzrokovala značajnije operativne ili sigurnosne posljedice.

Klasifikacija imovine se redovito preispituje, osobito u slučaju promjena u poslovnim procesima, tehnološkoj infrastrukturi ili nakon sigurnosnog incidenta radi pravodobnog ažuriranja i prilagodbe novonastalim okolnostima.

7.3. Upravljanje rizicima

REGOS provodi sustavni i dokumentirani pristup upravljanju rizicima koji proizlaze iz prijetnji kibernetičkoj sigurnosti te rizicima koji mogu utjecati na povjerljivost, cjelovitost, dostupnost i autentičnost informacijskih sustava i podataka.

Proces upravljanja rizicima obuhvaća identifikaciju, analizu, procjenu, obradu i praćenje rizika te se provodi u skladu s međunarodnim normama i nacionalnim propisima iz područja kibernetičke sigurnosti. Procjene rizika temelje se na pristupu koji uzima u obzir sve relevantne prijetnje (tehničke, organizacijske, fizičke i ljudske), kao i rizike povezane s korištenjem usluga trećih strana i implementacijom novih tehnologija.

REGOS redovito provodi procjene rizika nad kritičnom imovinom i uslugama od posebne važnosti te ih ažurira najmanje jednom godišnje, kao i nakon svake značajne promjene u sustavu, procesu ili tehnološkom okruženju. Identificirani rizici dokumentiraju se i unose u registar rizika uz praćenje njihove razine, statusa, odgovornih osoba i mjera ublažavanja. Rezultati procjene rizika dokumentiraju se i koriste kao osnova za definiranje i provedbu tehničkih i organizacijskih mjera kibernetičke sigurnost, kao i za kontinuirano unaprjeđenje sigurnosnog okvira.

REGOS kontinuirano razvija svijest o rizicima i potiče proaktivan pristup njihovom prepoznavanju i ublažavanju na svim razinama. Na taj način, REGOS osigurava dosljedno i učinkovito upravljanje rizicima, čime doprinosi stabilnosti, sigurnosti i pouzdanosti svojih informacijskih i mrežnih sustava.

7.4. Sigurnost ljudskih potencijala i digitalnih identiteta

Upravljanje ljudskim potencijalima i digitalnim identitetima u REGOS-u provodi se na način koji osigurava visoku razinu pouzdanosti, odgovornosti i sljedivosti u pristupu IKT sustavima. Uspostavljaju se i provode odgovarajuće mjere kontrole pristupa kojima se osigurava da se prava pristupa dodjeljuju isključivo ovlaštenim osobama te u opsegu koji je nužan za obavljanje njihovih radnih obveza, uz primjenu načela poslovne potrebe, najmanjih privilegija i razdvajanja dužnosti.

Svi korisnici IKT sustava imaju jedinstvene digitalne identitete povezane s konkretnim osobama, čime se osigurava odgovornost i transparentnost svakog pristupa. REGOS uspostavlja jasne procedure za dodjelu, izmjenu i ukidanje digitalnih identiteta te redovito provodi revizije prava pristupa, osobito prilikom organizacijskih promjena, promjena radnog statusa ili prekida poslovnog odnosa.

Edukacija i osposobljavanje radnika u području kibernetičke sigurnosti provodi se kontinuirano s ciljem podizanja razine svijesti, znanja i odgovornosti svih radnika u vezi s prepoznavanjem i sprječavanjem kibernetičkih prijetnji.

Svi radnici s administrativnim pristupom IKT sustavima prolaze dodatne programe edukacije kako bi se osigurala stručnost u provedbi sigurnosnih mjera.

7.5. Osnovne prakse kibernetičke higijene

REGOS uspostavlja i održava temeljna pravila kibernetičke higijene s ciljem smanjenja izloženosti kibernetičkim prijetnjama i osiguranja pouzdanog funkcioniranja IKT sustava.

Pravila osnovne prakse kibernetičke higijene uključuju redovito ažuriranje sustava i aplikacija, korištenje jakih i jedinstvenih lozinki uz višefaktorsku autentifikaciju (MFA) gdje je primjenjivo, redovitu izmjenu i nadzor pristupnih prava te edukacije o odgovornom ponašanju u digitalnom okruženju. Kao dio sustava prakse kibernetičke higijene, REGOS primjenjuje suvremene antivirusne alate, mehanizme za detekciju prijetnji i upravljanje sigurnosnim zakrpama te redovito provodi provjere ranjivosti i testiranja digitalne otpornosti. REGOS provodi kontinuirani nadzor i pohranu podataka relevantnih za sigurnost, osiguravajući forenzičku sljedivost aktivnosti na IKT sustavima te pravodobno otkrivanje i analizu incidenata.

Pridržavanje osnovnih mjera kibernetičke higijene obvezno je za sve radnike, suradnike i treće strane koje imaju pristup IKT sustavima REGOS-a.

7.6. Osiguravanje kibernetičke sigurnosti mreže

Osiguravanje kibernetičke sigurnosti mreže uključuje skup tehničkih, organizacijskih i proceduralnih mjera kojima se štite mrežna infrastruktura, podaci i korisnici od neovlaštenog pristupa, zlouporabe i prekida rada.

REGOS uspostavlja i održava sigurnu mrežnu arhitekturu temeljenu na načelima segmentacije i najmanjih privilegija, uz kontinuirani nadzor i detekciju prijetnji primjenom odgovarajućih mrežnih kontrola i sigurnih komunikacijskih protokola. Obvezne mjere zaštite mreže uključuju primjenu vatrozida nove generacije, IDS/IPS sustav za detekciju i prevenciju upada, sigurnih udaljenih pristupa (VPN kanali komunikacije) uz MFA autentifikaciju, EDR rješenja i SIEM. U svrhu pravovremenog otkrivanja i sprječavanja prijetnji, nadzora dolaznog i odlaznog mrežnog prometa, REGOS koristi sustav Sk@ut.

Svi implementirani mehanizmi nadzora i filtriranja podliježu periodičnoj reviziji i ažuriranju kako bi se održala visoka razina mrežne sigurnosti i osigurala usklađenost s najboljim praksama i propisima.

7.7. Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima

Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima u REGOS-u uključuje primjenu mjera kojima se osigurava da samo ovlaštene osobe imaju pristup prostorima, uređajima i sustavima u skladu s poslovnim ulogama i načelima poslovne potrebe, najmanjih privilegija i razdvajanja nadležnosti.

REGOS provodi redovite revizije korisničkih prava, najmanje jednom godišnje, pri čemu se provjerava opravdanost dodijeljenih pristupa, usklađenost s poslovnim ulogama i sigurnosnim politikama.

Sve izmjene, uključujući dodavanje, uklanjanje ili promjenu privilegija, moraju biti dokumentirane, odobrene od strane ovlaštene osobe i dostupne za reviziju kako bi se osigurala cjelovitost i transparentnost upravljanja pravima pristupa.

Fizički pristup IKT prostoriji i opremi dopušten je samo ovlaštenim osobama uz primjenu fizičkih kontrola poput kartičnog pristupa ili elektroničke brave.

7.8. Sigurnost lanca opskrbe

Sigurnost lanca opskrbe uključuje primjenu mjera koje štite IKT sustav REGOS-a od rizika koji mogu nastati kroz odnose s IKT dobavljačima.

REGOS uspostavlja i provodi pravila sigurnosti lanca opskrbe koja se primjenjuju na sve izravne IKT dobavljače i pružatelje usluga. Pravila sigurnosti lanca opskrbe definiraju uloge, odgovornosti i ovlasti svih uključenih strana, uključujući sigurnosne aspekte koji uređuju odnose između REGOS-a i njegovih izravnih IKT dobavljača i pružatelja usluga.

Kako bi se zaštitila kritična infrastruktura i smanjili kibernetički rizici, REGOS provodi procjenu i upravljanje rizicima povezanim s dobavljačima, definira sigurnosne zahtjeve i ugovorne obveze, nadzire isporučene proizvode i usluge, štiti sustave od kompromitiranih komponenti te kontinuirano prati i poboljšava sigurnost kroz cijeli lanac opskrbe.

Na temelju procjene rizika, za svakog dobavljača ugovorom se definiraju sigurnosni zahtjevi koji uključuju zaštitu podataka i obvezu pravovremenog prijavljivanja incidenata s ciljem zaštite kritične infrastrukture i smanjenja kibernetičkih rizika.

Kriteriji za odabir IKT dobavljača uključuju njihovu sposobnost ispunjavanja sigurnosnih zahtjeva, razinu pouzdanosti, transparentnost u poslovanju te mogućnost pravodobnog reagiranja u slučaju sigurnosnih incidenata. U okviru plana odgovora na incidente, REGOS uključuje i ključne IKT dobavljače i pružatelje usluga, osobito one koji imaju značajnu ulogu u održavanju kontinuiteta poslovanja i informacijske sigurnosti.

Svi izravni IKT dobavljači i pružatelji usluga evidentiraju se u registru izravnih dobavljača.

7.9. Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava

REGOS osigurava da svi IKT sustavi, kao i korištene vanjske usluge i mreže, budu razvijeni, implementirani i održavani uz primjenu sigurnosnih principa i kontrola tijekom svih faza njihove primjene s ciljem zaštite podataka, sprječavanja ranjivosti i očuvanja kontinuiteta poslovanja.

Tijekom razvoja i održavanja primjenjuju se sigurnosni standardi, uključujući testiranje ranjivosti, implementaciju zakrpa i kontrolu pristupa. Pristup razvojnim i administrativnim okruženjima dopušten je isključivo ovlaštenim korisnicima, a sve aktivnosti se evidentiraju i povremeno revidiraju. Sve promjene koje se odnose na razvoj, održavanje i konfiguraciju IKT sustava, bilo planirane ili neplanirane, moraju biti dokumentirane, procijenjene s aspekta rizika i odobrene od strane nadležnih osoba prije implementacije. U slučaju hitnih promjena koje se provode izvan redovnog postupka, potrebno je naknadno provesti testiranje i evidentirati razloge odstupanja. Ovaj pristup osigurava kontrolu, transparentnost i smanjenje rizika povezanih s promjenama u sustavima.

Kontrolne procedure promjene IKT sustava uključuju zahtjev za promjenu, procjenu rizika koje promjena unosi, kriterije za kategorizaciju, određivanje prioriteta promjena i plan reverznog postupka za povratak na prijašnje stanje, kao i podatke o odgovornim osobama za pojedine segmente IKT sustava. Kontrolne procedure promjene IKT sustava trebaju biti dokumentirane i sustavno primjenjivane kako bi se osigurala transparentnost, dosljednost i praćenje svih promjena.

7.10. Primjena kriptografije

REGOS osigurava primjenu kriptografskih mehanizama za zaštitu povjerljivosti, integriteta i dostupnosti podataka u skladu s procjenom rizika i poslovnim zahtjevima. To uključuje šifriranje podataka pri prijenosu, zaštitu pohranjenih podataka te sigurno upravljanje kriptografskim ključevima i certifikatima.

Kriptografske procedure se preispituju, ažuriraju i prilagođavaju novim sigurnosnim zahtjevima i tehnološkim dostignućima, čime se osigurava dugoročna učinkovitost i otpornost sustava na suvremene prijetnje.

7.11. Upravljanje sigurnosnim incidentima

Upravljanje sigurnosnim incidentima predstavlja sustavan proces otkrivanja, procjene, odgovora i oporavka od sigurnosnih prijetnji kako bi se minimizirao njihov utjecaj na poslovanje, zaštitili podaci i sustavi te spriječilo ponavljanje incidenata.

REGOS uspostavlja sustav za upravljanje sigurnosnim incidentima koji uključuje definiranje uloga, odgovornosti i procedura za praćenje, sprječavanje, otkrivanje, analizu, zaustavljanje, odgovor i oporavak od incidenata. Svi radnici i vanjski suradnici dužni su odmah prijaviti sumnjive aktivnosti ili incidente. REGOS evidentira sve sigurnosne incidente, provodi analizu njihovih uzroka i posljedica te po potrebi primjenjuje korektivne i preventivne mjere kako bi spriječio njihovo ponavljanje.

O značajnijim kibernetičkim incidentima REGOS izvješćuje Nacionalni centar za kibernetičku sigurnost putem nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima u propisanim rokovima.

Svi radnici REGOS-a moraju proći obuku za prepoznavanje i prijavu incidenata koja se provodi najmanje jednom godišnje. Provedba i rezultati obuke dokumentiraju se, a sadržaj se prilagođava poslovnim i tehnološkim promjenama.

REGOS sudjeluje u vježbama simulacije incidenata radi provjere učinkovitosti procedura i spremnosti radnika.

7.12. Kontinuitet poslovanja i upravljanje kibernetičkim krizama

REGOS osigurava kontinuitet poslovanja (BCP) i učinkovit odgovor na kibernetičke krizne situacije kroz planiranje i održavanje procedura za upravljanje incidentima, identifikaciju kritičnih sustava, procjenu rizika te izradu planova oporavka. Planovi uključuju jasnu podjelu uloga i odgovornosti, koordinaciju s ključnim dobavljačima i pružateljima usluga te aktivnosti za minimiziranje prekida poslovanja i zaštitu kritične infrastrukture i podataka.

Pravila kontinuiteta poslovanja i upravljanja kibernetičkim krizama definiraju ključne poslovne aktivnosti i resurse potrebne za njihovo nesmetano funkcioniranje u slučaju poremećaja ili sigurnosnog incidenta, kao i organizacijske i tehničke preduvjete za održavanje minimalnog prihvatljivog opsega poslovanja te postupni povratak u redovno poslovanje unutar unaprijed određenog vremenskog okvira.

U cilju zaštite kritične infrastrukture i podataka, smanjenja prekida u poslovanju te osiguravanja pravovremenog i koordiniranog odgovora na kibernetičke incidente, redovito se provode vježbe, simulacije i revizije kako bi se postigla učinkovitost u reagiranju na incidente koji mogu ugroziti poslovanje ili informacijske sustave.

Planovi kontinuiteta poslovanja i oporavka od katastrofa testiraju se najmanje jednom godišnje, a nakon svake značajne promjene u sustavima ili procesa poslovanja. Testiranja uključuju provjeru sposobnosti postizanja vremena oporavka sustava, ciljanog gubitka podataka i ciljane razine usluge, kako bi se osigurala učinkovitost planova u održavanju kontinuiteta kritičnih funkcija i minimiziranju prekida poslovanja.

REGOS osigurava redundantne resurse za ključnu imovinu i opremu, radnike s kritičnim ulogama i ovlastima, komunikacijske kanale te napajanje električnom energijom, gdje god je to moguće. Po potrebi, redundancija se može ostvariti kroz ugovorne odnose s vanjskim pružateljima usluga, uz prethodnu dokumentiranu procjenu rizika i troškova.

7.13. Fizička sigurnost

Na temelju procjene rizika REGOS uspostavlja i provodi pravila fizičke sigurnosti koja definiraju razine zaštite, opseg primjene, odgovorne osobe, metode provedbe te učestalost provjera učinkovitosti. Cilj ovih mjera je spriječiti neovlašteni pristup, oštećenje ili krađu IKT opreme te povjerljivih podataka.

Pristup prostorijama u kojima se nalaze IKT sustavi i kritična infrastruktura dozvoljen je isključivo ovlaštenim osobama, uz primjenu sustava kontrole pristupa i vođenje evidencije ulazaka i izlazaka. Oprema je zaštićena fizičkim bravama i zaključanim ormarićima, dok se prostorije nadziru pomoću videonadzora i alarmnih sustava radi osiguranja sigurnosti i sprječavanja neovlaštenog pristupa.

Osim toga, poduzimaju se aktivnosti zaštite od okolišnih rizika kroz detekcijske sustave, uređaje za gašenje požara i sustave neprekidnog napajanja. Sve mjere redovito se provjeravaju, održavaju i nadziru kako bi se osigurala njihova učinkovitost i kontinuitet sigurnosti.

REGOS osigurava upravljanje dnevničkim zapisima pojedinačnih sustava fizičke sigurnosti radi analize pristupa u slučaju incidenta ili revizije.

8. Provedba Politike

Provedba ove Politike osigurava se sustavnim procesom koji obuhvaća komunikaciju pravila radnicima, implementaciju tehničkih i organizacijskih mjera, nadzor i praćenje usklađenosti te osposobljavanje za pravilnu primjenu sigurnosnih procedura.

Svi radnici, vanjski suradnici i druge osobe koje imaju pristup informacijskim sustavima organizacije obvezni su se upoznati s odredbama ove Politike prije dobivanja pristupnih prava te potpisati Izjavu o prihvaćanju Politike kibernetičke sigurnosti REGOS-a koja je prilog ove Politike.

Potpisivanjem Izjave o prihvaćanju Politike kibernetičke sigurnosti REGOS-a, korisnici potvrđuju da su pročitali, razumjeli i da će se pridržavati svih odredbi ove Politike.

Nepridržavanje propisanih sigurnosnih procedura i tehničkih mjera od strane radnika predstavlja povredu ove Politike. Ovisno o težini, posljedicama i okolnostima počinjenja, za utvrđene povrede poduzimaju se odgovarajuće aktivnosti i izriču mjere sukladno odredbama Zakona o radu, Pravilnika o radu te drugih važećih internih akata.

9. Pregled i ažuriranje Politike

Pregled i ažuriranje ove Politike provodi se najmanje jednom godišnje, kao i pri promjenama u tehnologiji, zakonodavstvu, procjeni rizika ili drugim okolnostima koje mogu utjecati na njenu učinkovitost i relevantnost kako bi Politika ostala aktualna, usklađena s regulatornim zahtjevima i učinkovita u zaštiti sustava, podataka i poslovnih procesa.

10. Završna odredba

Politika stupa na snagu osam dana od dana objave na e-oglasnoj ploči REGOS-a.

KLASA: 650-05/26-01/10

URBROJ: 353-02/3-26-1

Zagreb, 27. ožujka 2026. godine

PREDSJEDNIK UPRAVNOG VIJEĆA

Dražen Opalić



Ova Politika objavljena je na e-oglasnoj ploči REGOS-a dana 27. 03. 2026. godine.

Prilog – Izjava o prihvaćanju Politike kibernetičke sigurnosti REGOS-a

Izjava o prihvaćanju Politike kibernetičke sigurnosti REGOS-a

Potvrđujem da sam upoznat/a s Politikom kibernetičke sigurnosti REGOS-a i da su mi njezine odredbe jasne.

Obvezujem se pridržavati svih pravila, smjernica i sigurnosnih mjera propisanih Politikom kibernetičke sigurnosti REGOS-a.

Potpisom ove Izjave potvrđujem da razumijem i prihvaćam pravila kibernetičke sigurnosti te da sam svjestan/na mogućih posljedica njenog nepridržavanja.

Ime i prezime davatelja Izjave: _____

Gospodarski subjekt: _____
(popunjavaju samo vanjski korisnici)

Potpis davatelja Izjave: _____

Datum i mjesto: _____