POLITIKA SIGURNOSTI INFORMACIJSKOG SUSTAVA HRVATSKOG GEOLOŠKOG INSTITUTA

U skladu s točkom 1. Odluke o prihvatljivom korištenju CARnet mreže: klasa: 500-200/12/95, ur.broj:110082-650-109-12-1 od 15. lipnja 2012. godine i čl. 21. Statuta Hrvatskog geološkog instituta: ur.broj: 2254/14 od 28. siječnja 2014. godine Upravno vijeće je na svojoj sjednici održanoj 13. rujna 2016. godine donijelo

POLITIKU SIGURNOSTI INFORMACIJSKOG SUSTAVA HRVATSKOG GEOLOŠKOG INSTITUTA

Članak 1.

Ovaj dokument ima za cilj definirati principe i strategiju programa sigurnosti informacijskog sustava (dalje u tekstu: politika sigurnosti) Hrvatskog geološkog instituta (u daljnjem tekstu: HGI).

Informacijski sustav mora omogućiti neometano odvijanje poslovnih procesa kroz upotrebu informacija. Obavljanje poslovnih procesa HGI-a ovisi o radu informacijskog sustava HGI-a

Sigurnosna politika treba biti planirana i provođena na način da omogućava sigurno obavljanje posla, a da pritom ne ometa poslovne procese.

HGI može usvojiti i druge dokumente kojima se specificiraju pojedine odredbe ovog programa sigurnosti.

Članak 2.

Informacijski sustav (u daljnjem tekstu: IS) podrazumijeva usklađeno djelovanje svojih sastavnica:

- Računalne i komunikacijske tehnologije
- Sistemskog i aplikativnog softvera
- Podataka/informacija
- Metoda i postupaka za obradu podataka
- Osoba koje održavaju IS, obrađuju podatke i koriste ih
- Poslovnih partnera i suradnika

Informacijsku imovinu sačinjava svaki resurs IS koji služi za prikupljanje, obradu, spremanje ili distribuciju podataka, na primjer:

- Opipljiva (materijalna) imovina (zgrade, računala i komunikacijska oprema, infrastruktura)
- Neopipljiva (nematerijalna) imovina (ugled, tehnologija, metodologija, zaštitni znak)
- Podaci (dokumenti, ugovori, osobni podaci itd.)
- Softver (sistemski i aplikativni programski paketi)
- Ljudi koji održavaju i koriste IS

Sigurnost informacijskog sustava definira se kao skup mjera i postupaka, na tehničkoj i organizacijskoj razini, čijom se primjenom postiže i održava prihvatljiva razina rizika IS.

Temeljna načela sigurnosti informacijskog sustava su

- **Povjerljivost** – informacije su dostupne samo ovlaštenim ljudima i organizacijama
- **Cjelovitost** – ažurnost i točnost podataka, sprečavanje neovlaštenog mijenjanja i uništavanja podataka
- **Dostupnost** – podaci moraju biti na raspolaganju ovlaštenim korisnicima u trenutku kada su potrebni

Procjena rizika je postupak kojim se identificiraju prijetnje i ranjivosti koje mogu ugroziti rad informacijskog sustava.

- Za svaku prijetnju određuje se vjerojatnost ostvarenja i potencijalna šteta, kako bi se odredili prioriteti i odabrale mjere koje smanjuju rizik na prihvatljivu razinu.
- Procjena rizika provodi se periodički kako bi se ustanovile promjene u prijetnjama, ranjivostima i poslovnim prioritetima.
- Troškovi primjene sigurnosnih mjera moraju biti razmjerni s osjetljivošću i vrijednošću informacija koje se takvim mjerama štite i prilagođeni materijalnim i ljudskim mogućnostima.

Sigurnosni događaj je svaki događaj koji ukazuje na probleme koji ne ugrožavaju rad samog informacijskog sustava niti povjerljivost podataka (na primjer kada korisnici zaborave zaporku).

Sigurnosni incident je događaj koji ugrožava povjerljivost, integritet i dostupnost podataka. Integritet sistemskog softvera i poslovnih aplikacija, ili ukazuje na neovlašten pristup informacijskim resursima. Incidentom se smatraju i događaji koji onemogućavaju neprekidnost poslovanja, poput nestanka električne energije, poplave, požara itd.

Članak 3.

Politika sigurnosti primjenjuje se na sve komponente informacijskog sustava.

Pravila sigurnosne politike dužni su poštivati i provoditi ih svi zaposleni, poslovni partneri i vanjski suradnici koji imaju pristup podacima i informacijskoj infrastrukturi u skladu s poslovnim potrebama.

Članak 4.

HGI usvaja slijedeću strukturu dokumentacije koja se bavi informacijskom sigurnošću:

Politika sigurnosti IS kao najviša razina dokumentacije definira temeljne odrednice za uspostavu sigurnog i učinkovitog informacijskog sustava.

Pravilnici HGI-a: Pravilnik o korištenju elektroničke pošte, Pravilnik o prihvatljivom korištenju računalne opreme i Pravilnik o korištenju lozinki detaljno opisuju mjere i pravila čijom primjenom se osigurava uspostava prihvatljive razine informacijske sigurnosti.

Upute sadrže konkretne procedure i mjere koje treba slijediti u okviru pojedinih poslovnih procesa.

Članak 5.

Pod informacijskom imovinom se smatra svaki materijalni ili nematerijalni resurs informacijskog sustava ili organizacijske strukture HGI koji služi za prikupljanje, obradu, spremanje ili distribuciju informacija značajnih u poslovnom procesu.

Podaci se smatraju naročito vrijednim oblikom informacijske imovine.

Članak 6.

Korisnik je svaki zaposlenik, vanjski partner ili suradnik HGI koji u skladu s poslovnim potrebama pristupa informacijskom sustavu HGI.

Pristup korisnika informacijskim resursima bit će odobren tek nakon potpisivanja izjave o prihvaćanju odredbi sigurnosne politike.
Prilog 1. Izjava o prihvaćanju odredbi sigurnosne politike.

Izvanrednu suglasnost za pristup informacijskom sustavu i korištenje podataka unutarnjim i vanjskim korisnicima daju voditelji organizacijskih jedinica uz suglasnost ravnatelja.

Ovlasti dodijeljene pojedinom korisniku ne smiju prelaziti ovlasti koje ta osoba obavlja u redovitom poslovnom procesu. Korisnik smije imati uvid samo u one podatke koji su neophodni za obavljanje njegovih poslovnih funkcija.

Dužnosti korisnika su:

- Pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu sa poslovnim procesima, etičkim normama i pravilima aktualne sigurnosne politike.
- Izbor kvalitetne zaporke i njezina povremena promjena
- Prijava sigurnosnih događaja i incidenata
- Korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. To znači da su dužni povesti računa o izradi sigurnosnih kopija, tj. ako nisu u mogućnosti moraju od voditelja organiazcijskih jedinica zatražiti da uspostave automatsku pohranu (backup) isključivo poslovnih podataka po unaprijed definiranim pravilima i strukturi
- Autori geoloških podataka dužni su upisivati podatke u GEOLIS prema trenutnoj strukturi baze podataka.

Članak 7.

Ovaj dokument se bavi sigurnošću informacijskog sustava te u razmatranje uzimamo samo prostore od važnosti za funkcioniranje informacijskog sustava (u daljnjem tekstu nazvati ćemo ih sigurnim zonama). Na dan donošenja dokumenta, u području informatičke, tj. informacijske sigurnosti, sigurne zone su:

1. Server soba (soba broj 51)

2. Soba s mrežnom komunikacijskom opremom (soba broj 9)

Izbor i osiguranje navedenih prostora, smještaj opreme i radni uvjeti u sigurnim zonama moraju uzeti u obzir sigurnosne rizike i značaj resursa koji su u njima smješteni.

Osjetljivi informacijski resursi moraju biti smješteni u posebno osiguranim dijelovima radne okoline, kako bi im se omogućili optimalni radni uvjeti (temperatura, vlažnost, zaštita od požara i sl).

Središnja računalna oprema mora biti smještena u sigurnoj zoni i mogu joj pristupati samo ovlašteni zaposlenici. Popis zaposlenika ovlaštenih za ulazak u sigurnu zonu mora biti na raspolaganju zaposlenicima porte, čija je obaveza ne puštati nikoga tko nije na popisu. Osobe koje nemaju ovlasti mogu pristupati sigurnoj zoni isključivo u pratnji osoba sa popisa. Popis izrađuje savjetnik za informacijsku sigurnost.

Članak 8.

Računalni sustavi i mrežna oprema mora biti konfigurirana tako da bilježi sistemsku i korisničku aktivnost, naročito događaje koji pružaju dokaze o pristupu povjerljivim ili osjetljivim podacima ili programima.

Podsustav za kontrolu pristupa korisnika mora imati mogućnost konfiguracije koja će omogućiti zadovoljavajuću provjeru identiteta korisnika i kontrolu dodjele prava za rad.

Administratori sustava su dužni slijediti sve stručne upute proizvođača komponenti koje čine informacijski sustav.

Popravke sistemskog programskog koda koje ispravljaju sigurnosne probleme moraju biti evaluirane i primijenjene u najkraćem mogućem roku.

Članak 9.

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. Da bi se HGI zaštitio od moralne i materijalne štete koja time može nastati, savjetnik za informacijsku sigurnost vodi brigu o instaliranju softvera i njihova licenciranja. Korisnik koji ima potrebu za instalacijom korisničkog programa, mora se obratiti voditelju organizacijske jedinice i zatražiti, uz obrazloženje, nabavu i instalaciju.

U slučaju povrede autorskih prava i intelektualnog vlasništva korisnici odgovaraju za nastalu materijalnu i nematerijalnu štetu, a za unutarnje korisnike pokreću se i ostali postupci sukladno propisima iz radnog odnosa.

Članak 10.

Prilikom dizajna novih ili unapređenja postojećih informacijskih sustava, savjetnik za informacijsku sigurnost će definirati sigurnosne zahtjeve i mjere neophodne za siguran rad sustava.

Isti zahtjevi vrijede i kod razmatranja gotovih programskih paketa.

Pristup do izvornog programskog koda mora biti ograničen i kontroliran. Izvršni kod se može primijeniti u produkcijskom okruženju samo nakon postupka testiranja, prihvaćanja i odobrenja.

Probni podaci koji se koriste u svrhu testiranja programa moraju biti zaštićeni, a pristup takvim podacima kontroliran. Korištenje zaštićenih, npr. osobnih podataka za probne svrhe nije dozvoljeno, osim ako su depersonalizirani.

Programski sustavi moraju imati mogućnost bilježenja početka i izvorišta pojedinih transakcija, te podatke o svakom pristupu i akciji nad osjetljivim podacima.

Svaka promjena na sustavu mora biti detaljno planirana, izvođenje promjene odobreno, a rezultati promjene dokumentirani.

Svaki novi resurs informacijskog sustava mora prije početka produkcijskog korištenja, u suradnji s djelatnikom zaduženim za upravljanje licencama proći kroz postupak provjere i odobravanja, kako bi se mogla jamčiti njegova ispravnost i mogućnost obavljanja očekivanih funkcija.

Članak 11.

Pravo pristupa informacijama, informacijskim resursima i procesima informacijskog sustava, može biti dodijeljeno samo temeljem odobrenja voditelja organizacijske jedinice uz suglasnost savjetnik za informacijsku sigurnost.

Svakom korisniku pojedine aplikacije ili informacijskog servisa mora biti dodijeljeno jedinstveno korisničko ime za takvu aplikaciju ili servis. Svako korisničko ime mora imati i svoju lozinku.

Davatelji usluga su nadležni za kontrolu, autorizaciju i nadzor pristupa korisnika.

Korisnik je dužan odabrati svoju lozinku na način kako je to opisano u Pravilniku o korištenju lozinki.

Korisnik je obavezan čuvati svoju lozinku i ne odavati je drugim osobama

Članak 12.

Potrebno je redovito izrađivati zaštitne kopije produkcijskih podataka. Odgovornost i upute za izradu zaštitnih kopija moraju biti specificirani posebnim procedurama.

Odluka o načinu spremanja zaštitnih kopija, kao i njihovom broju formira se temeljem važnosti podataka, u skladu s mogućnostima. Ovu odluku donosi ravnatelj temeljem prijedloga savjetnika za informacijsku sigurnost. Prema potrebi, zaštitne kopije mogu biti spremljene izvan glavne lokacije HGI.

Davatelj informatičkih usluga dužan je osigurati odgovarajuće resurse za obnovu podataka sa zaštitnih kopija.

Postupak obnove podataka sa zaštitnih kopija mora se izvoditi sukladno zahtjevu određenom temeljem procjene rizika.

Članak 13.

Obrada, pohrana i korištenje podataka na osobnim računalima moraju biti provedeni tako da se spriječe sigurnosni rizici.

Korisnici osobnih računala moraju slijediti upute za zaštitu od računalnih virusa ili drugih destruktivnih programa. U slučaju pojave računalnog virusa ili drugih destruktivnih programa, korisnici moraju odmah obavijestiti voditelja organizacijske jedinice te postupiti prema uputama.

Članak 14.

Računalni resursi smiju se koristiti prvenstveno za svrhe poslovnog procesa HGI.

Korisnici su odgovorni za profesionalno, etičko i zakonito korištenje računalnih resursa koji su im dani na raspolaganje.

Korištenje programskih paketa mora biti u skladu sa zakonom i licencnim pravima.

S obzirom da kapaciteti mrežnih i računalnih resursa HGI imaju svoja ograničenja, od svih korisnika se očekuje korištenje računalnih resursa na način koji neće onemogućiti ili smanjiti efikasnost rada drugih korisnika.

Članak 15.

Elektroničkom poštom korisnici se služe isključivo radi obavljanja posla. Pri sastavljanju poruka dužni su čuvati ugled HGI.
Korisnici ne smiju slati elektroničkom poštom ili bilo kojom drugom formom elektroničke komunikacije informacije koje bi za druge osobe mogle biti uvredljive ili klevetničke. Elektroničkom poštom se ne smiju slati neistinite informacije u namjeri da nanesu štetu trećim osobama.

Pošiljatelji su odgovorni za istinitost i pouzdanost informacija koje se prenose elektroničkom poštom. Elektronička pošta se mora koristiti uvažavajući ista pravila ponašanja kao i u bilo kojem drugom obliku pisane komunikacije.

Podaci koji su klasificirani nekom od oznaka tajnosti mogu biti poslani elektroničkom poštom tek uz dopuštenje osobe odgovorne za te podatke, uz suglasnost ravnatelja i uz primjenu enkripcije.

Korisnici moraju biti svjesni da korištenje elektroničkih poruka ne podrazumijeva privatnost i sigurnost samih poruka.

Savjetnik za inforamcijsku sigurnost zadužen je za provedbu tehničkih mjera kojima se smanjuje rizik korištenja elektroničke pošte, što uključuje zaštitu od virusa i neželjenih poruka (spama).

Članak 16.

Internet se smatra značajnom komponentom informacijskog sustava HGI. Internet se može koristiti prije svega za poslovnu namjenu, informiranje i edukaciju.

Savjetnik za informacijsku sigurnost odgovoran je za provedbu odgovarajućih mjera kojima se onemogućuje neovlašten pristup unutarnjoj mreži ili podacima tvrtke putem Interneta.

Korisnici su dužni izbjegavati aktivnosti koje bi mogle ugroziti sigurnost njihovih računala i informacijskog sustava HGI.

Savjetnik za informacijsku sigurnost dužan je osigurati provedbu mjera na tehničkoj i organizacijskoj razini, uključujući edukaciju, kojima se smanjuju rizici korištenja Interneta.

Članak 17.

Potrebno je definirati i provesti mjere zaštite od virusa i drugih destruktivnih programa na svim osobnim računalima i poslužiteljima.

Mjere zaštite od virusa podrazumijevaju korištenje programa za zaštitu od virusa, ali i uzdržavanje korisnika od radnji koje ugrožavaju sigurnost informacijskog sustava.

Korisnici moraju biti upoznati s procedurom zaštite od virusa u vidu praćenja redovitih informacija o sigurnosnim mjerama.

Programi koji služe za zaštitu od virusa moraju biti redovito ažurirani i dograđivani.

Korisnici ne smiju isključivati ili onemogućavati programe za zaštitu od virusa.

Članak 18.

Svaki događaj koji ukazuje na pojavu sigurnosnog incidenta mora biti prijavljen voditelju organizacijske jedinice u najkraćem mogućem roku.

Ukoliko je utjecaj sigurnosnog incidenta takav da je raspoloživost sustava znatno smanjena, primjenjuju se odredbe politike sigurnosti o osiguranju neprekidnosti radnog procesa.

Potrebno je definirati procedure odgovaranja na sigurnosne incidente i odgovornosti svih sudionika u njihovoj provedbi. Procedura odgovaranja na incidente mora brzo i efikasno odgovoriti na sve potencijalne tipove incidenata.

Procedura odgovaranja na incidente mora uključivati i postupak obnove sustava nakon incidenata.

Zaposlenici HGI su dužni obavijestiti voditelja organizacijske jedinice o svim slabim točkama ili ranjivostima produkcijskih sustava.

Bez prethodne dozvole ravnatelja, zaposlenici ne smiju javno objavljivati podatke o pojavi sigurnosnih incidenata, problema ili ranjivosti sustava i računalne mreže HGI.

Izuzetak predstavljaju slučajevi koji su regulirani zakonskim i podzakonskim propisima.

Članak 19.

Dijelovi informacijskog sustava koji obavljaju kritične funkcije moraju imati plan kontinuiranog djelovanja u slučaju izvanrednih okolnosti.

Pod izvanrednim okolnostima se smatraju događaji koji mogu uzrokovati gubitak povjerljivosti i integriteta podataka ili sustava, te prekid ili smanjenje raspoloživosti informacijskih sustava.

Prije donošenja plana neophodno je provesti postupak procjene rizika. Plan kontinuiranog djelovanja mora definirati mjere koje će biti sukladne predviđenim rizicima.

Plan djelovanja u slučaju izvanrednih okolnosti mora uključivati postupak odgovaranja na incidente, rezervni plan obavljanja funkcija i obnavljanje redovitih funkcija.

Provedba plana kontinuiranog djelovanja podrazumijeva i implementaciju preventivnih mjera kojima se smanjuje rizik pojave incidenata.

Članak 20.

HGI zadržava pravo nadzora i bilježenja svih aktivnosti na računalnim resursima, te provođenja redovitih provjera pridržavanja sigurnosne politike
Savjetnik za informacijsku sigurnost dužan je osigurati provjeru stanja sigurnosti pojedinih komponenti informacijskog sustava, sistemskih zapisa o radu informacijskog sustava, evidenciju o radu korisnika i druge sistemske podatke radi otkrivanja sigurnosnih incidenata i nepridržavanja politike sigurnosti.

Bilježenje aktivnosti na računalnim resursima može obuhvatiti i bilježenje aktivnosti i podataka koji nisu vezani za poslovne procese HGI.

HGI zadržava pravo provjere svake datoteke ili poruke elektroničke pošte koja je kreirana, spremljena ili proslijeđena računalnim resursima HGI, što uključuje i pravo provjere datoteka ili poruka s privatnim sadržajem koje se nalaze u osobnim mapama ili direktorijima korisnika.

Provjera se može obaviti radi istrage o sigurnosnim incidentima uz prisutnost savjetnika za inforamcijsku sigurnost zaposlenika i svjedoka.

Članak 21.

Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama Ustanove i priključena je u mrežu CARNet, na sav instalirani softver, te na sve mrežne servise.

Pravila su dužni poštivati i provoditi svi zaposleni, studenti i vanjski suradnici koji po ugovoru obavljaju određene poslove.

Članak 22.

Korisnici su dužni pomoći osobama zaduženim za nadzor informacijskih sustava, na taj način što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora.

Isto vrijedi i za aministratore računala i pojedinih servisa, koji su dužni specijalistima za sigurnost pomagati pri istrazi.

Pristup uključuje:

- Pristup na razini korisnika ili sustava svoj računalnoj opremi
- Pristup svakoj informaciji, u elektroničkom ili tiskanom obliku, koja je proizvedena ili spremljena na opremi HGI, ili oprema HGI služi za njezin prijenos.
- Pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.)
- Pravo na interaktivno nadgledanje i bilježenje prometa na mreži Ustanove

Članak 23.

Ova Politika stupa na snagu osam dana od dana objave na oglasnoj ploči Instituta.

Predsjednik Upravnog vijeća

HRVATSKI GEOLOŠKI INSTITUT
1 ZAGREB - Sachsova

dr. sc. Dragan Krasić, dipl. ing. rud.

Prilog 1.

Izjava o prihvaćanju odredbi sigurnosne politike

- HGI posvećuje značajnu pažnju pitanjima informacijske sigurnosti i dužnost je svakog korisnika pridržavati se svih pravilnika i uputa koje reguliraju pitanja zaštite informacijske imovine HGI-a.

- Korisnik, ovime prima na znanje i prihvaća slijedeće odredbe:

- Korisnik je odgovoran za sigurno, etično i zakonito korištenje informacijskog sustava i imovine HGI-a.
- Od korisnika se očekuje korištenje informacijskog sustava na način koji neće onemogućavati ili umanjivati učinkovitost poslovnih procesa.
- Korisniku je dozvoljeno korištenje isključivo programskih rješenja dobavljenih od strane HGI-a ili programskih rješenja otvorenog koda.
- Korisniku je zabranjeno korištenje plug-in-ova koja nisu preporučena od strane informatičke podrške.
- Korisniku kojemu je istekao radni odnos u HGI-a u roku od 10 dana briše se elektronski identitet iz sustava AA@EduHR te se ukida korisnički račun iz domene: @hgi-cgs.hr.
- Korisnici ne smiju namjerno sudjelovati u širenju zlonamjernih programa.
- Korisnici ne smiju na vidljivom i lako dostupnom mjestu držati lozinke u pisanom obliku.
- Prilikom napuštanja prostorije korisnik mora adekvatno zbrinuti službene dokumente za koje je odgovoran i zaključati računalo. Ako osoba posljednja odlazi, dužna je ugasiti svjetlo u prostoriji, zatvoriti prozore, zatvoriti i zaključati vrata, a ako je to moguće, ugasiti klime, grijalice, električna i druga kuhala.
- Mogućnost korisnika da pristupa, koristi ili utječe na rad resursa za koji je odgovorna druga osoba ne podrazumijeva i dozvolu za takvu akciju.

- Korisnik će se pridržavati svih sigurnosnih odredbi i mjera koje proizlaze iz sigurnosne politike.

- Korisnik je upoznat s Politikom sigurnosti i prihvaća njegove odredbe.

- Korisnik će svaku nejasnoću u Politici sigurnosti razjasniti sa savjetnikom za informacijsku sigurnost.

- Vlastoručnim potpisom korisnik izjavljuje da je suglasan sa svim gore navedenim.

Potpis korisnika Datum (Ime i prezime korisnika)

Ova Politika objavljena je na oglasnoj ploči Poslodavca 15.09. 2016. godine, a stupila je na snagu 23.09. 2016. godine.

HRVATSKI GEOLOŠKI INSTITUT
1 ZAGREB - Sachsova 2

R a v n a t e l j

Dr. sc. Josip Halamić, dipl. ing. geol.