Na temelju članka 18. stavak 1. Zakona o informacijskoj sigurnosti („Narodne novine“ broj 79/07) donosim

PRAVILNIK O STANDARDIMA SIGURNOSTI NEKLASIFICIRANIH INFORMACIJSKIH SUSTAVA

I. UVOD

Članak 1.

Ovim se Pravilnikom utvrđuju organizacijske i tehničke mjere koje je potrebno uspostaviti na informacijskim sustavima na kojima se obrađuju, prenose ili pohranjuju neklasificirani podaci za službenu uporabu označeni oznakom „NEKLASIFICIRANO“ ili bez oznake (u daljnjem tekstu: neklasificirani informacijski sustavi).

Članak 2.

(1) Tijela državne uprave, pravosudna tijela, stručne službe Hrvatskog sabora i Ureda predsjednika Republike Hrvatske, stručne službe i uredi Vlade Republike Hrvatske i ostala državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te pravne osobe s javnim ovlastima koja su vlasnici neklasificiranih informacijskih sustava dužna su provesti mjere sigurnosti informacijskih sustava u skladu s ovim Pravilnikom, radi osiguravanja minimalne razine njihove zaštite u Republici Hrvatskoj.

(2) Pored mjera propisanih ovim Pravilnikom tijela iz stavka 1. ovog članka mogu primijeniti i druge dodatne mjere.

Pojmovi

Članak 3.

U smislu ovog Pravilnika pojedini pojmovi imaju sljedeće značenje:

- „Vlasnik neklasificiranog informacijskog sustava“ – tijelo državne uprave, pravosudno tijelo, stručna služba Hrvatskog sabora i Ureda predsjednika Republike Hrvatske, stručna služba i ured Vlade Republike Hrvatske i drugo državno tijelo, tijelo jedinice lokalne i područne (regionalne) samouprave te pravna osoba s javnim ovlastima koja u svom radu upravlja i koristi neklasificirani informacijski sustav.
- „Odgovorna osoba“ – čelnik tijela odnosno druga osoba zadužena za sigurnost informacijskoga sustava određena sukladno odredbama ovog Pravilnika.
- „Voditelj informacijske sigurnosti“ - savjetnik za informacijsku sigurnost prema članku 25. Zakona o informacijskoj sigurnosti ili druga osoba zadužena za sigurnost informacijskoga sustava.

II. KRITERIJI ZA PROVOĐENJE MJERA

Procjena rizika

Članak 4.

(1) Vlasnici neklasificiranih informacijskih sustava primjenjuju mjere iz ovog Pravilnika razmjerno procjeni rizika kojemu je izložen njihov neklasificirani informacijski sustav.

(2) Vlasnici neklasificiranih informacijskih sustava dužni su redovito, a najmanje jednom u dvije godine, provesti procjenu rizika temeljem koje će donijeti odluke o razini provođenja mjera iz ovog Pravilnika.

(3) Sve odluke o razini provođenja mjera iz ovog Pravilnika, temeljene na provedenoj procjeni rizika moraju se dokumentirati, te ih mora odobriti odgovorna osoba.

III. UPRAVLJANJE SIGURNOŠĆU NEKLASIFICIRANIH INFORMACIJSKIH SUSTAVA

Okvir upravljanja

Članak 5.

Vlasnici neklasificiranih informacijskih sustava dužni su uspostaviti sustav upravljanja sigurnošću neklasificiranih informacijskih sustava.

Načela sigurnosti

Članak 6.

Funkcionalnost i sigurnost neklasificiranih informacijskih sustava temelji se na sljedećim načelima:

- cjelovitosti: svojstvu da usluge ili podaci nisu neovlašteno ili nepredviđeno mijenjani
- povjerljivosti: svojstvu da usluge ili podaci ne budu dostupne ili otkrivene neovlaštenim osobama
- raspoloživosti: svojstvu koje omogućuje pristup ili upotrebljivost usluge ili podataka na zahtjev ovlaštenog korisnika
- autentičnosti: svojstvu koje osigurava da je identitet korisnika zaista onaj za koji se tvrdi da jest i
- neporecivosti: svojstvu koje osigurava utvrđivanje neposredne odgovornosti za pojedine radnje.

Politika upravljanja sigurnošću

Članak 7.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su donijeti opći akt za upravljanje informacijskom sigurnošću neklasificiranih informacijskih sustava koji će:

- definirati ciljeve i strateške smjernice očuvanja kontinuiteta poslovanja
- utvrditi sustav procjene i upravljanja rizicima i
- opisati sustav upravljanja informacijskom sigurnošću, uključujući interne nadzore provedbe mjera informacijske sigurnosti.

(2) Opći akt za upravljanje informacijskom sigurnošću neklasificiranih informacijskih sustava donosi se u pisanom obliku.

Organizacijska struktura

Članak 8.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su odrediti odgovornu osobu za uspostavu i upravljanje sigurnošću neklasificiranih informacijskih sustava.

(2) Ako nije određena osoba iz prethodnog stavka odgovorna osoba za uspostavu i upravljanje sigurnošću neklasificiranih informacijskih sustava je voditelj informacijske sigurnosti.

(3) Ako voditelj informacijske sigurnosti nije imenovan njegove poslove obavlja čelnik tijela.

(4) Vlasnici neklasificiranih informacijskih sustava dužni su uspostaviti organizacijsku strukturu, s formalnom raspodjelom zadaća, ovlasti i odgovornosti kojom će se osigurati primjereno upravljanje sigurnošću neklasificiranih informacijskih sustava.

Provedba sigurnosnih mjera

Članak 9.

(1) Vlasnik neklasificiranih informacijskih sustava dužan je osigurati provedbu sigurnosnih mjera u svrhu postizanja zadovoljavajuće razine sigurnosti za neklasificirani informacijski sustav u skladu s općim aktom za upravljanje informacijskom sigurnošću neklasificiranih informacijskih sustava iz članka 7. ovoga Pravilnika.

(2) Sigurnosne mjere iz stavka 1. ovog Pravilnika moraju zadovoljavati barem minimalne sigurnosne mjere provedene razmjerno procjeni rizika kojemu je izložen neklasificirani informacijski sustav, a koje su sadržane u Popisu minimalnih sigurnosnih mjera za neklasificirane informacijske sustave.

IV. PODRUČJA ZAŠTITE NEKLASIFICIRANIH INFORMACIJSKIH SUSTAVA

Fizička sigurnost i sigurnost okruženja

Članak 10.

Vlasnici neklasificiranih informacijskih sustava dužni su osigurati provedbu mjera koje se odnose na fizičku sigurnost i sigurnost okruženja neklasificiranih informacijskih sustava od štete uzrokovane kvarom sustava, ljudskim pogreškama, zlonamjernim djelovanjem ili djelovanjem prirodnih fenomena.

Upravljanje ugovornim odnosima

Članak 11.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su provesti postupak procjene rizika prije ostvarivanja ugovornog odnosa s pravnim i fizičkim osobama čije aktivnosti mogu utjecati na neklasificirane informacijske sustave.

(2) Vlasnici neklasificiranih informacijskih sustava dužni su kontinuirano nadzirati način i kvalitetu pružanja ugovorenih poslova i usluga koje mogu utjecati na neklasificirane informacijske sustave.

(3) Vlasnici neklasificiranih informacijskih sustava dužni su redovito procjenjivati i na prihvatljivu razinu svesti rizike koji proizlaze iz ugovornih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na neklasificirane informacijske sustave.

Kontrola pristupa prostorima

Članak 12.

Vlasnici neklasificiranih informacijskih sustava dužni su osigurati provedbu mjera kojima se osigurava kontroliran i ograničen fizički pristup prostorima u kojem je smještena ključna oprema neklasificiranog informacijskog sustava.

Dnevnički zapisi neklasificiranih informacijskih sustava

Članak 13.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su koristiti sustav za nadzor i bilježenje korisničkih aktivnosti (dnevničkih zapisa) na neklasificiranom informacijskom sustavu.

(2) Dnevnički zapisi moraju minimalno obuhvaćati prijave i odjave korisnika sustava, otvaranje i zatvaranje korisničkih računa, promjene prava korisnika, promjene sigurnosnih prava na sustavu i podatke o funkcioniranju sustava koji pokrivaju odgovarajuće poslužitelje.

(3) Vlasnici neklasificiranih informacijskih sustava dužni su osigurati kontinuirano praćenje aktivnosti i provođenje postupka analize dnevničkih zapisa u slučaju incidenta.

(4) Dnevnički zapisi u sustavu za nadzor i bilježenje korisničkih aktivnosti čuvaju se najmanje godinu dana od trenutka njihovoga nastanka.

Zaštita podataka koji se obrađuju, pohranjuju i prenose u neklasificiranom informacijskom sustavu

Članak 14.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su osigurati provedbu mjera zaštite podataka koji se obrađuju, pohranjuju i prenose u neklasificiranom informacijskom sustavu u svrhu zaštite povjerljivosti, raspoloživosti i cjelovitosti podataka.

(2) Vlasnici neklasificiranih informacijskih sustava, ako temeljem provedene procjene rizika utvrde dodatnu potrebu zaštite skupova podataka, primijenit će kriptografske mehanizme zaštite tijekom njihove obrade, pohrane i prenošenja u neklasificiranom informacijskom sustavu, u svrhu zaštite povjerljivosti i cjelovitosti podataka.

(3) Vlasnici neklasificiranih informacijskih sustava dužni su mjere iz stavaka 1. i 2. ovog članka odgovarajuće primjenjivati i na prijenosne medije koji se koriste za obradu, pohranu ili pomoću kojih se prenose podaci u neklasificiranom informacijskom sustavu.

Zaštita od zlonamjernog programskog koda

Članak 15.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su zaštiti neklasificirani informacijski sustav od zlonamjernog programskog koda primjenom odgovarajućih sigurnosnih mjera.

(2) Sigurnosne mjere iz stavka 1. ovoga članka moraju osigurati prepoznavanje i onemogućavanje zlonamjernog programskog koda unutar neklasificiranog informacijskog sustava te zapisivanje i pohranu informacija nužnih za prepoznavanje narušavanja funkcionalnosti neklasificiranog informacijskog sustava i održavanje kontinuiteta.

Zaštita od ugroze raspoloživosti

Članak 16.

(1) Vlasnici neklasificiranih informacijskih sustava su dužni zaštititi neklasificirani informacijski sustav od računalnih napada koji mogu narušiti njegovu raspoloživost primjenom odgovarajućih sigurnosnih mjera.

(2) Sigurnosne mjere iz stavka 1. ovoga članka moraju osigurati prepoznavanje i onemogućavanje računalnih napada koji mogu ugroziti raspoloživost neklasificiranog informacijskog sustava te zapisivanje i pohranu informacija nužnih za prepoznavanje narušavanja funkcionalnosti neklasificiranog informacijskog sustava i održavanje kontinuiteta.

Edukacija i podizanje svijesti

Članak 17.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su uspostaviti i provoditi sustav edukacije korisnika svojih neklasificiranih informacijskih sustava iz područja informacijske sigurnosti.

(2) Vlasnici neklasificiranih informacijskih sustava dužni su provoditi kampanje podizanja svijesti o informacijskoj sigurnosti među korisnicima svojih neklasificiranih informacijskih sustava.

Razvoj i održavanje neklasificiranih informacijskih sustava

Članak 18.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su definirati načine, kriterije i postupke razvoja neklasificiranih informacijskih sustava, s posebnim naglaskom na važnost planiranja sigurnosnih aspekata od početne faze projekta.

(2) Vlasnici neklasificiranih informacijskih sustava dužni su, u sklopu procesa razvoja neklasificiranih informacijskih sustava, uspostaviti i dokumentirati proces razvoja i isporuke sustava koji obuhvaća postupke analize i projektiranja, razvoja programske podrške, testiranja i uvođenja u produkcijski plan.

(3) Vlasnici neklasificiranih informacijskih sustava dužni su na odgovarajući način razdvojiti razvojnu, testnu i produkcijsku okolinu.

(4) Vlasnici neklasificiranih informacijskih sustava dužni su osigurati da sve razvijene programske komponente neklasificiranih informacijskih sustava, kao i nove sklopovske komponente neklasificiranog informacijskog sustava, prije uvođenja u operativni rad budu na odgovarajući način testirane i da ih odobre odgovorne osobe.

(5) Vlasnici neklasificiranih informacijskih sustava dužni su osigurati da se za sve programske komponente neklasificiranih informacijskih sustava, prije uvođenja u produkcijski rad, provede postupak provjere ranjivosti i penetracijskog testiranja.

Upravljanje sklopovskom i programskom imovinom

Članak 19.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su upravljati sklopovskom i programskom imovinom neklasificiranog informacijskog sustava tijekom cijelog njegovog životnog ciklusa.

(2) Postupak upravljanja sklopovskom i programskom imovinom mora obuhvatiti njenu identifikaciju, evidentiranje, korištenje, održavanje, rashodovanje i kontrolirano uništavanje.

Članak 20.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su upravljati promjenama programske imovine neklasificiranih informacijskih sustava.

(2) Postupak upravljanja promjenama programske imovine mora obuhvatiti minimalno:

- utvrđivanje postojećih programskih inačica neklasificiranih informacijskih sustava
- identifikaciju i praćenje svih promjena programskih inačica neklasificiranih informacijskih sustava koje utječu ili mogu utjecati na funkcionalnost i/ili sigurnost neklasificiranih informacijskih sustava i
- evidentiranje svih promjena programskih inačica neklasificiranih informacijskih sustava onim slijedom kako su nastale zajedno s vremenom nastanka promjene.

(3) Vlasnici neklasificiranih informacijskih sustava dužni su u slučaju svake značajnije programske promjene neklasificiranog informacijskog sustava, u skladu s procjenom rizika, provesti postupak provjere ranjivosti i penetracijskog testiranja.

Preventivne provjere ranjivosti neklasificiranih informacijskih sustava

Članak 21.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su, u skladu s procjenom rizika, osigurati provođenje provjera ranjivosti i/ili penetracijskih testiranja neklasificiranih informacijskih sustava, osobito onih dijelova sustava koji koriste resurse na javno dostupnim mrežnim i informacijskim sustavima.

(2) Vlasnici neklasificiranih informacijskih sustava dužni su osigurati da se nedostatci i ranjivosti utvrđeni tijekom postupaka provjere ranjivosti i penetracijskog testiranja obrade kroz postupak upravljanja rizicima.

Upravljanje kontinuitetom poslovanja

Članak 22.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su identificirati poslovne procese bitne za osiguranje kontinuiteta poslovanja.

(2) Vlasnici neklasificiranih informacijskih sustava dužni su donositi operativne planove postupanja u svrhu osiguranja kontinuiteta poslovanja, koji moraju minimalno uključivati:

- konkretne tehničke procedure postupanja u svrhu oporavka
- jasne korake i odgovornosti za aktivaciju planova oporavka i
- definirana vremena u kojima oporavak mora biti dovršen.

(3) Vlasnici neklasificiranih informacijskih sustava dužni su jednom godišnje, u skladu s procjenom rizika, provesti i dokumentirati testiranje planova iz stavka 2. ovoga članka.

Pričuvna pohrana

Članak 23.

(1) Vlasnici neklasificiranih informacijskih sustava dužni su uspostaviti postupak upravljanja pričuvnom pohranom podataka koji su potrebni za ponovnu uspostava kontinuiteta poslovanja neklasificiranih informacijskih sustava u zahtijevanom vremenu.

(2) Postupak upravljanja pričuvnom pohranom mora obuhvaćati postupke izrade, pohrane i testiranja pričuvnih kopija podataka te oporavka podataka s pričuvnih kopija.

(3) Pričuvne kopije podataka moraju biti ažurne i pohranjene na jednoj ili više lokacija.

(4) Sukladno procjeni rizika, alternativna lokacija mora biti dovoljno udaljena od lokacije na kojoj se nalaze izvorni podaci, kako ispad primarne lokacije ne bi izazvao ispad alternativne lokacije.

V. UPRAVLJANJE RAČUNALNO SIGURNOSNIM INCIDENTIMA

Uspostava komunikacijskih kanala

Članak 24.

Vlasnici neklasificiranih informacijskih sustava dužni su uspostaviti i redovito testirati komunikacijske kanale (poput e-maila, telefona i slično) prema tijelima nadležnim za prevenciju i koordinaciju odgovora na računalno–sigurnosne incidente.

Prijava računalno sigurnosnih incidenata

Članak 25.

Vlasnici neklasificiranih informacijskih sustava dužni su računalno-sigurnosne incidente koji ne mogu biti upravljani i razriješeni internim resursima, bez odlaganja prijaviti nadležnim tijelima za prevenciju i koordinaciju odgovora na računalno–sigurnosne incidente, ovisno o svojoj djelatnosti.

VI. KORIŠTENJE USLUGA RAČUNALSTVA U OBLAKU, KOLOKACIJA MREŽNIH I INFORMACIJSKIH SUSTAVA

Odgovornost za upravljanje informacijskom sigurnošću

Članak 26.

U slučaju da vlasnici neklasificiranih informacijskih sustava koriste usluge računalstva u oblaku ili je neklasificirani informacijski sustav vlasnika smješten (kolociran) kod davatelja usluge na iznajmljenom poslužitelju, odgovornost za upravljanje informacijskom sigurnošću ostaje na vlasniku informacijskog sustava.

Provođenje mjera informacijske sigurnosti

Članak 27.

(1) Vlasnik neklasificiranih informacijskih sustava dužan je osigurati provođenje minimalnih mjera informacijske sigurnosti.

(2) Vlasnik neklasificiranih informacijskih sustava za tu svrhu sklapa s davateljem usluge ugovor o razini usluge (*Service Lewel Agreement* - SLA) ili drugi važeći pravni dokument kojim obavezuje davatelja usluge na provođenje propisanih mjera informacijske sigurnosti.

(3) Standardi informacijske sigurnosti u korištenju usluga računalstva u oblaku ili kolokacija propisuju se Standardima sigurnosti informacijskih sustava državnih tijela u korištenju tehnologije računalstva u oblaku.

VII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 28.

(1) Popis minimalnih sigurnosnih mjera za neklasificirane informacijske sustave iz članka 9. ovoga Pravilnika donijet će Zavod za sigurnost informacijskih sustava (u daljnjem tekstu: ZSIS) u roku od devedeset dana od stupanja na snagu ovog Pravilnika.

(2) Standarde sigurnosti informacijskih sustava državnih tijela u korištenju tehnologije računalstva u oblaku iz članka 27. ovoga Pravilnika donijet će ZSIS u roku od devedeset dana od stupanja na snagu ovog Pravilnika.

Članak 29.

Tijela iz članka 2. ovog Pravilnika obvezna su se uskladiti s njegovim odredbama u roku od godine dana od njegovog stupanja na snagu.

Članak 30.

Pored mjera propisanih ovim Pravilnikom vlasnik neklasificiranih informacijskih sustava može primijeniti i ostale mjere sukladno normama za upravljanje informacijskom sigurnošću HRN ISO/IEC27001.

Članak 31.

Ovaj Pravilnik stupa na snagu osmog dana od dana donošenja i objavit će se na mrežnim stranicama ZSIS-a.

RAVNATELJ

Predrag Božinović, v. r.

KLASA: 650-02/20-01/03
URBROJ: 509-10/21-20-15
Zagreb, 31. prosinca 2020.