BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
FEDERALNO MINISTARSTVO KULTURE I SPORTA
FEDERALNO MINISTARSTVO KULTURE I ŠPORTA

PROCEDURE I PRAVILA UPORABE SIGURNOSTI ZAŠTITE PODATAKA INFORMACIJSKOG SUSTAVA

Sarajevo, kolovoz 2023.

Na temelju članka 56. stavak 2. Zakona o organizaciji organa uprave u Federaciji Bosne i Hercegovine („Službene novine Federacije BiH", broj 35/05), a u vezi s Odlukom o usvajanju politike upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 2017. - 2022. godine („Službene novine BiH" broj: 38/17), federalna ministrica kulture i športa, donosi

PROCEDURE I PRAVILA UPORABE SIGURNOSTI ZAŠTITE PODATAKA INFORMACIJSKOG SUSTAVA

I. UVOD

Ovim Procedurama i Pravilima regulira se način ponašanja i postupanja rukovodećih i ostalih službenika i namještenika (u daljnjem tekstu: djelatnici) u Federalnom ministarstvu kulture i športa (u daljnjem tekstu: Ministarstvo) tijekom pristupa podacima i za korištenje podataka. Odgovornost za siguran i pravilan pristup podacima je na rukovodećim djelatnicima/cama Ministarstva.
Kroz uspostavu sustava informacijske sigurnosti i upravljanje tim sustavom, Ministarstvo izvršava svoju ulogu u izgradnji informacijskog društva. Uspostavljaju se preventivne mjere i stvaraju organizacijsko-tehnički preduvjeti za razvitak zaštitnih i represivnih mjera unutar informacijskog društva.

II. DEFINICIJA INFORMACIJSKE SIGURNOSTI

Informacijska sigurnost se odnosi na zaštitu informacija bez obzira na medij na kome se čuva i prenosi. Sustavom informacijske sigurnosti obuhvaćaju se fizičke osobe, procesi, organizacija i tehnologija. Taj sustav se sastoji od uravnoteženog skupa sigurnosnih mjera, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava, koordiniranog uvođenja formalnih procedura, kao što su procjene rizika, certificiranje uređaja i akreditacije tehničkih sustava za primjenu u određenim segmentima poslovnih procesa u Institucijama. Uravnoteženost i koordiniranje mjera i postupaka postiže se organizacijom i upravljanjem sustavom informacijske sigurnosti.
Mehanizmi zaštite i sprječavanja dijele se na tri temeljne razine: fizička sigurnost, pod kojom se podrazumijeva sigurnost računalne opreme i podataka, **osobna sigurnost**, koja podrazumijeva zaštitu korisnika i povjerljivih informacija korisnika, **sigurnost institucije**, koja proizilazi iz prve dvije razine. Termin informacijska sigurnost podrazumijeva stanje u kojemu je osiguran integritet hardvera, njihova raspoloživost i povjerljivost podataka i informacija. Integritet u razmatranom kontekstu podrazumijeva točnost i

kompletnost podataka i informacija koji se nalaze na sustavu i samog sustava u njegovoj cijelosti, uključujući i procese koji se na njemu odvijaju. Da bi se smatrali raspoloživim, podaci, informacije i sustav moraju biti na svom mjestu, dostupni i upotrebljivi za obavljanje funkcija koje su im namijenjene. U tom kontekstu termin raspoloživost povezan je i s kontinuitetom usluga. Povjerljivost se koristi u kontekstu osjetljivosti na otkrivanje (objelodanjivanje) podataka i informacija.

III. ORGANIZACIJA INFORMACIJSKE SIGURNOSTI

Za provođenje mjera sigurnosti zaduženi su rukovoditelji sektora i šefovi unutarnjih organizacijskih jedinica.
U svrhu upravljanja informacijskom sigurnošću unutar Ministarstva potrebno je uraditi procjenu razine sigurnosti nekog dijela opreme (npr. laptopa), popisati vrijednosti koje Ministarstvo posjeduje na način da se svaka uporaba dokumentira s ciljem zaštite vrijednosti od kopiranja, uništavanja i zamjene od strane djelatnika.
Svi djelatnici u Ministarstvu obvezni su pridržavati se pravila sigurnosti, kao i poduzimati mjere za njihovo provođenje, posebno u djelokrugu svog rada.
Svi podaci kojima raspolaže Ministarstvo moraju biti klasificirani ovisno o stupnju povjerljivosti.
Klasifikacija je posebno važna za materijal koji se nalazi na računarima zbog rizika od neovlaštenog pristupa računarima.
Klasifikacija vrijedi za sav materijal bez obzira na vlasništvo. Materijal koji je vlasništvo druge institucije zaštićen je dok je unutar Ministarstva.
Postizanje i održavanje odgovarajuće zaštite Ministarstva se provodi kroz identificiranje (popisivanje) imovine Ministarstva u svrhu procjene vrijednosti i važnosti i sukladno tome određivanje primjerene razine zaštite.
Kako bi se sprječilo oštećenje, gubitak, krađa ili ugrožavanje imovine potrebno je opremu smjestiti sukladno uputama proizvođača opreme, voditi računa o ispravnosti instalacija u prostorijama institucije kako ne bi došlo do oštećenja. Održavanje opreme smiju raditi samo ovlaštene osobe.

IV. OČUVANJE INTEGRITETA I DOSTUPNOSTI PODATAKA

Potrebno je redovito izrađivati sigurnosne preslike podataka radi očuvanja integriteta i raspoloživosti istih, pri čemu treba uzeti u obzir sljedeće:

- sigurnosnim preslikama mora se osigurati odgovarajuća razina fizičke zaštite i zaštite okoliša sukladno standardima koji se primjenjuju na glavnoj lokaciji

- mediji sigurnosnih preslika, gdje je primjenjivo, moraju se redovito testirati kako bi se osiguralo da se na njih može računati u slučaju potrebe

- procedure za ponovnu uspostavu sustava moraju se redovito provjeravati i testirati kako bi se osigurala njihova učinkovitost i mogućnost izvršavanja u predviđenom vremenu

- vrijeme čuvanja sigurnosnih preslika mora biti vremenski točno određeno.

V. UPRAVLJANJE POSLOVNIM KONTINUITETOM

Ministarstvo se mora suočiti s rizicima poslovanja i biti spremno primjereno reagirati ukoliko se dogodi incident koji može prouzrokovati zastoj u poslovanju, te je potrebno provoditi sljedeće radnje:

- identificirati i analizirati događaje, tj. incidentne situacije, koji mogu prekinuti poslovni proces, te definirati plan za kontinuirano poslovanje institucije

- kontinuirano provoditi ispitivanja kako bi se pravovremeno otkrili propusti uslijed promjena u sustavu

- odrediti potencijalne prijetnje informacijskom sustavu institucije

- odrediti koje je mjere moguće primijeniti kako bi se smanjili rizici kojima je izložen informacijski sustav

- primjena provjera za minimiziranje štete nastale prirodnim katastrofama (zemljotresi, poplave, požari, itd.) i

- poduzeti sve mjere zaštite i opreza kako korisnici sustava ne bi mogli prouzročiti prestanak ispravnog rada informacijskog sustava.

VI. PRAVA I OBVEZE DJELATNIKA MINISTARSTVA

Svi djelatnici u Ministarstvu moraju biti upoznati s temeljnim pravilima vezanima za sigurnost i tajnost podataka. Pripravnici također moraju biti upoznati s ovim Pravilima.
Kroz seminare i tečajeve o novim sustavima i informacijskim tehnologijama potrebno je uključiti i informacije o funkcijama sigurnosti.
Istu sigurnosnu razinu koja vrijedi za unutrašnji rad potrebno je primijeniti u uporabi vanjskih usluga.
Osoblje koje izvršava usluge kao što su čišćenje ili koje izvodi radove na uredskoj opremi mora biti informirano o pravilima sigurnosti i pridržavati se tih pravila.
Ukoliko se ocijeni da neki osobni računar mora biti zaštićen šifrom na isti način pristup svim podacima mora biti zaštićen šifrom.
Šifre iz ovih procedura trebaju znati tajnik i korisnik računara. Šifre moraju biti u zapečaćenoj koverti i pohranjene u metalnoj kasi kod tajnice u uredu ministrice.
Korisnik osobnog računala koje mora biti zaštićeno šifrom mora poduzeti mjere da zaštiti podatke od neovlaštenog pristupa ili gubitka.

Svaki korisnik je obvezan osigurati back-up /preslik dokumenata.
Također je obveza svakog korisnika računara da se dokumenti čuvaju na USB fleš memoriji ili izvanjskom disku.
Po pravilu nitko nema ovlaštenje da posjeduje više podataka nego što mu je potrebno za rad.
Djelatnicima koji napuštaju Ministarstvo ili iz drugih razloga nisu više ovlašteni da pristupe podacima, oduzet će se ovlaštenje.
Svi uredi trebaju imati odgovarajuću zaštitu. Djelatnici su obvezni provjeravati te spriječiti ulazak neovlaštene osobe u ured.
Djelatnik koji primi stranke odgovoran je za njih dok se nalaze u radnim prostorijama.
S dokumentacijom koja se prima putem pošte, faksa, e-maila i putem owis sustava treba postupati na način koji jamči privatnost.
Povjerljivi podaci se ne smiju slati putem Internet platformi.
Osobni računari će se držati u zaključanim prostorijama tijekom vikenda i praznika.
Povjerljivi podaci će se čuvati u zaključanoj arhivi u metalnoj kasi.
USB-ovi, CD-ovi, izvanjski diskovi ne smiju biti izloženi temperaturi preko 55°C. Moraju biti zaštitićeni od izravnog izlaganja suncu.
Sigurnosno kopiranje se radi da bi se zaštitilo od nesretnih slučajeva raznih vrsta:

- nenamjerno uništenje
- automatsko brisanje
- krađa računara s podacima
- pogreška programa
- katastrofe, npr. veliki požar u radnim prostorijama i drugo.

S ciljem zaštite podataka kada materijali više nisu potrebni neophodno ih je uništiti. Uništenje se odnosi na sve vrste medija (papir, CD-ovi i drugo).
Materijal se uništava na način koji onemogućava prijevod sadržaja.
Katastrofa znači ozbiljan incident koji zaustavlja rad u Ministarstvu najmanje jedan tjedan.
Najveća katastrofa u planiranju posljedica katastrofe je uništenje nekog od ureda u Ministarstvu.
Planiranje aktivnosti od posljedica katastrofe će osigurati da prikupljeni podaci i programi ne izgube zauvijek ili postanu neupotrebljivi uslijed katastrofe.
Radi predostrožnosti sigurnosne preslici se moraju iznijeti i čuvati izvan stalnog ureda.

VII. ZAVRŠNE ODREDBE

Ove Procedure i Pravila stupaju na snagu danom donošenja.

Stupanjem na snagu ovih Procedura prestaju važiti Procedure i pravila korištenja sigurnosti i zaštite podataka informacijskog (IT) sustava broj: 01-02-2-4003 /05 od 30. 12. 2005. godine.

MINISTRICA

Sanja Vlaisavljević

Broj: 06-02-4-3758/23
Sarajevo, 11. 8. 2023. godine