REPUBLIKA HRVATSKA
DRŽAVNI ZAVOD ZA STATISTIKU

POLITIKA SUSTAVA INFORMACIJSKE SIGURNOSTI

Dokumentacija informacijske sigurnosti

Verzija	Status	Datum	Pregledao/Izmijenio/Odobrio	Komentar
3.0	Konačna verzija	26.07.2019.	Lidija Brković	Odobreno Ravnateljica
3.0	Konačna verzija	22.07.2019.	Mira Talan	Pravno usklađivanje
2.0	Arhivska verzija	21.03.2019.	Marko Krištof	Odobreno Ravnatelj
2.0	Arhivska verzija	03.12.2018.	Mira Talan	Pravno usklađivanje
1.0	Arhivska verzija	14.12.2017.	Gordana Hočuršćak	Izrada verzije

Sadržaj

1. Svrha

Politikom sustava upravljanja informacijskom sigurnošću (u daljnjem tekstu: Politika) Državni zavod za statistiku (u daljnjem tekstu: Zavod) uspostavlja smjernice za Sustav upravljanja informacijskom sigurnošću (engl. *Information Security Management System*, u daljnjem tekstu: ISMS) u skladu s dobrim praksama i zahtjevima regulatora.

Ovaj dokument namijenjen je upotrebi zaposlenih u Zavodu i vanjskih suradnika Zavoda u opsegu ISMS-a, ali i drugih koji dokažu da imaju opravdan interes. Svaki pojedinac u opsegu ISMS-a ima svoje definirano mjesto i odgovornost, a osigurani su mu osvješćivanje, obrazovanje i obuka. Vlasnik ISMS-a omogućuje nadzor i odgovarajuće disciplinske mjere u slučaju kršenja definiranih pravila.

Zavod ISMS-om uspostavlja sustav upravljanja koji će kontinuiranim poboljšavanjem u sklopu ciklusa Planiranje – provedba – provjera – poboljšanje (engl. *Plan-Do-Check-Act*, PDCA) zajamčiti sigurnost informacija i tehničkih resursa kojima zaposleni ili vanjski suradnici provode obradu informacija u sklopu svojih dužnosti i/ili ovlaštenja.

ISMS je određen u smjernicama ove Politike te detaljnijim postupcima opisanima u drugim dokumentima vezanima za informacijsku sigurnost. ISMS-om se štiti:

- povjerljivost (informacije se štite od neovlaštenog pristupa)
- integritet/cjelovitost (štite se točnost i potpunost informacija)
- raspoloživost (osigurava se raspoloživost informacija ovlaštenim korisnicima kada su im one potrebne)
- autentičnost (osigurava se da je identitet subjekta zaista onaj za koji se tvrdi da jest)
- neporecivost (osigurava nemogućnost poricanja provedene aktivnosti ili primitka informacije/podatka)
- dokazivost (osigurava da se aktivnosti subjekta mogu pratiti jedinstveno do samog subjekta)
- pouzdanost (dosljedno, očekivano ponašanje i rezultati).

2. Ciljevi uspostave ISMS-a

Cilj uspostavljanja ISMS-a i zaštite informacija jest potpora postizanju poslovnih ciljeva Zavoda, odnosno ciljevi zaštite informacija trebaju biti usklađeni s poslovnim ciljevima Zavoda.

Provedbom ISMS-a želi se postići:

- zaštita podataka i informacijskog sustava Zavoda, odnosno umanjenje operativnog rizika
- usklađivanje s propisima u Republici Hrvatskoj.

Ciljeve ISMS-a utvrđuje ravnatelj Zavoda (u daljnjem tekstu: ravnatelj).

3. Uloge i odgovornosti

Odgovornosti su određene u sljedećoj tablici:

Rb	Stavka	Odgovornost
1.	Sponzorstvo informacijske sigurnosti	Ravnatelj
2.	Politika ISMS-a	Voditelj Odbora za upravljanje sustavom informacijske sigurnosti (u daljnjem tekstu: voditelj Odbora), odobrava ravnatelj
3.	ISMS	Voditelj Odbora
4.	Predlaganje ciljeva informacijske sigurnosti	Voditelj Odbora
5.	Pregledavanje ugovora iz aspekta sigurnosti	Voditelj Odbora
6.	Upravljanje dokumentima ISMS-a	Voditelj Odbora
7.	Upravljanje procesom procjene rizika	Voditelj Odbora
8.	Korektivne i preventivne mjere	Voditelj Odbora
9.	Upravljanje zapisima ISMS-a	Voditelj Odbora
10.	Revizija sigurnosti informacijskog sustava	Samostalna služba za unutarnju reviziju
11.	Osposobljavanje i osvješćivanje zaposlenih	Voditelj Odbora

Koordinacija u različitim organizacijskim dijelovima aktivnosti vezanih za upravljanje informacijskom sigurnošću obavlja se na sastancima Odbora za upravljanje sustavom informacijske sigurnosti (u daljnjem tekstu: Odbor).

Izvješćivanje o incidentima obavlja se s namjerom ograničavanja štete prouzročene sigurnosnim incidentima, praćenjem incidenata i učenja na osnovi incidenata. Svi zaposleni i svi vanjski suradnici moraju biti informirani o procedurama prijave različitih incidenata, prekršaja, prijetnji i ranjivosti. U slučaju većih sigurnosnih incidenata koji mogu ugroziti glavne poslovne ciljeve ili opstanak Zavoda, odmah se izvješćuju voditelj Odbora i ravnatelj. Svaki pojedinac koji registrira sigurnosni incident, mora pokušati samostalno ograničiti štetu, ako raspolaže relevantnim znanjem i ima relevantne sposobnosti.

4. Odgovornosti ravnatelja

Funkcioniranje ISMS-a ravnatelj treba pregledati najmanje jedanput na godinu, ali i pri svim većim poslovnim i organizacijskim promjenama. Voditelj Odbora organizira ravnateljev pregled ISMS-a. Na pregledu koji provodi ravnatelj sudjeluju i voditelj Odbora, voditelj Službe za administrativne, tehničke i pomoćne poslove te drugi zaposlenici ovisno o području rada koje je tema dnevnog reda', u skladu s dnevnim redom. Ulazni podaci uključuju, među ostalim, izvještaje internih i eksternih revizija, rezultate procjene rizika, prijedloge ovladavanja rizikom, izjavu o prihvaćanju preostalih rizika i plan provedbe mjera zaštite.

5. Odbor za upravljanje sustavom informacijske sigurnosti

Odbor, u sklopu svojih redovitih zadaća, mora omogućiti jasno usmjerenje i posvećenost provedbi ISMS-a te razmatrati pitanja informacijske sigurnosti iz perspektive svake ustrojstvene jedinice i koordinirati razne inicijative. Članove Odbora imenuje ravnatelj odlukom iz različitih ustrojstvenih jedinica. Odborom predsjeda voditelj Odbora.

Odbor se sastaje minimalno dva puta na godinu i češće, ako se procijeni da je to potrebno.

Izvještaji sa sastanaka Odbora šalju se svim sudionicima sastanka te po potrebi i drugim zaposlenicima ovisno o temi sastanka i klasificiraju se oznakom povjerljivosti **Povjerljivo.**

6. Smjernice za upravljanje informacijskim rizicima

Procjenom rizika obuhvaćeni su svi resursi identificirani unutar opsega sustava, prijetnje koje mogu ugroziti sustav, vjerojatnost nastanka takva događaja te razina posljedica. Procjenu rizika provode vlasnici poslovnih procesa i voditelj Odbora. Procjena rizika provodi se najmanje jedanput na godinu ili češće, ako su nastale promjene u okružju koje bi mogle znatno utjecati na rezultate.

Za svaki identificirani rizik na osnovi postavljenih kriterija donosi se odluka o ovladavanju i smanjivanju rizika na poslovno prihvatljivu razinu. Rizicima se upravlja u skladu s poslovnim prioritetima i financijskim mogućnostima te ih se pokušava što prije sniziti na razinu prihvatljivu za poslovanje Zavoda.

Vlasnici poslovnih procesa odgovorni su u ustrojstvenim jedinicama za koje su zaduženi za sustavan nadzor nad upravljanjem informacijskim rizicima te za usklađenje potrebnih aktivnosti s propisanim postupcima. Pregledi aktivnosti obavljaju se jedanput na godinu na redovitim pregledima, ili češće prema potrebi.

Ravnatelj pri pregledu ISMS-a precizira razinu prihvatljivih rizika i odobrava sve mjere za čiju su realizaciju potrebni dodatni resursi.

7. Odgovornost

Svi sudionici poslovnog procesa Zavoda odnosno informacijskog sustava dužni su se pridržavati odredaba ove Politike u dijelu koji se na njih odnosi.

8. Valjanost

Ova Politika stupa na snagu i primjenjuje se od dana donošenja.

RAVNATELJICA

Lidija Brković

KLASA: 650-03/19-01/4

URBROJ: 555-13-02-01-19-2

Zagreb, 26. srpnja 2019.