**RFC2350**

1. **Informacije o dokumentu**

Ovaj dokument sadrži informacije o OITeG CERT-u.

* 1. **Datum poslednje izmene**

17.06.2023.

* 1. **Distribucijska lista za obaveštenja**

Ne postoji distribucijska lista za obaveštavanje o izmenama u ovom dokumentu.

* 1. **Mesta na kojima je ovaj dokument dostupan**

Poslednja verzija ovog dokumenta se nalazi na : <https://www.ite.gov.rs/tekst/sr/88/cert.php>

1. **Kontaktne informacije**
	1. **Ime CSIRT tima**

OITeG CERT (Office for IT and eGovernment Computer Emergency Response Team)

* 1. **Adresa**

Nemanjina 11, Beograd, 11000, Srbija

* 1. **Vremenska zona**

CET; UTC+01:00

* 1. **Broj telefona**

+ 381 11 7358 400

* 1. **Broj faksimila**

/

* 1. **Druge metode kontakta**

Ne postoje

* 1. **Adresa Elektronske pošte**

cert@gov.rs

* 1. **Javni ključevi i informacije za enkripciju**

Key Fingerprint= 27669C7FFC5B64396F84E47418244C141B54747D

* 1. **Članovi tima**

Članovi OITeG CERT-a će se identifikovati po stupanju u komunikacju.

* 1. **Druge informacije**

Sve informacije o OITeG CERT-u su dostupne na: <https://www.ite.gov.rs/tekst/sr/88/cert.php>

* 1. **Preferirane metode komunikacije**

Primarni metod komunikacije je korišćenjem email-a preko cert@gov.rs, a sekundarni metod je putem telefona +381 11 7358 400

1. **Povelja**
	1. **Misija**

Glavni zadatak CERT-a republičkih organa je da obezbeđuje informacionu bezbednost IKT infrastrukture, usluga Kancelarije i jedinstvene informaciono-komunikacione mreže elektronske uprave. Ovo uključuje efikasno reagovanje i rešavanje incidenata kada do njih dođe, preventivne aktivnosti kako bi se broj mogućih incidenata minimizovao i podizanje svesti IKT bezbednosti kod državnih organa.

* 1. **Konstituenti**

CERT republičkih organa obavlja poslove koji se odnose na zaštitu od incidenata u sistemima republičkih organa u jedinstvenoj informaciono-komunikacionoj mreži elektronske uprave.

* 1. **Sponzorstvo ili pripadnost**

OITeG CERT se nalazi u okviru Kancelarije za informacione tehnologije i elektronsku upravu nadležne za projektovanje, razvoj, izgradnju, održavanje i unapređenje jedinstvene informaciono-komunikacione mreže elektronske uprave.

* 1. **Nadležnost**

Centar za bezbednost informaciono-komunikacionih sistema organa (CERT republičkih organa) osnovan je ([Zakon o informacionoj bezbednosti](https://test.ite.gov.rs/extfile/sr/2062/Zakon%20o%20informacionoj%20bezbednosti.pdf), ''Službeni glasnik Republike Srbije'', broj 6/2016 i 94/2017) u okviru Kancelarije za informacione tehnologije i elektronsku upravu nadležne za projektovanje, razvoj, izgradnju, održavanje i unapređenje jedinstvene informaciono-komunikacione mreže elektronske uprave ([Zakon o elektronskoj upravi](https://test.ite.gov.rs/extfile/sr/1882/Zakon_o_elektronskoj_upravi_cyr.pdf), ''Službeni glasnik Republike Srbije'', broj 27/2018).

1. **Politike**
	1. **Vrste incidenata i nivo podrške**

Pri odgovoru na incidente OITeG CERT odgovara na sve vrste incidenata te ima koordinatorsku ulogu kako bi izvršio one aktivnosti koje su potrebne da bi se donele ispravne odluke od detekcije pa do razrešenja incidenta. Sve ostale usluge kao što su otkrivanje ranjivosti, monitoring i detekcija od strane SOC tima, koordinacija sa drugim organizacijama i obaveštavanje i edukacija OITeG CERT izvršava u potpunosti u svrhu zaštite i unapređenja bezbednosti sistema državnih institucija i organizacija.

* 1. **Saradnja, interakcija i deljenje informacija**

OITeG CERT pridaje veliku pažnju privatnosti tako da će svi deljeni podaci biti deljeni bez ličnih ili osetljivih podataka. Podaci koji mogu biti deljeni od strane OITeG CERT-a su statistički.

Za svaku razmenu informacija OITeG CERT koristi TLPv2. Više informacija o načinu na koji se TLPv2 koristi na <https://www.ite.gov.rs/extfile/sr/6981/TLP.docx>

* 1. **Komunikacija i autentikacija**

OITeG CERT svu komunikaciju smatra poverljivom. Gde god se dele osetljivi podaci putem email-a trebalo bi koristiti PGP/GPG, dok informacije koje nisu osetljive mogu da se dele bez enkripcije.

Telefonska komunikacija se smatra bezbednom za deljenje svih informacija.

1. **Usluge**
	1. **Reaktivne usluge**
* reagovanje na sigurnosne incidente;
* reagovanje na sigurnosne ranjivosti i propuste;
* upozorenja o uočenim incidentima i ranjivostima.
	1. **Proaktivne usluge**
* praćenje korišćenih tehnologija;
* sprovođenje bezbednosne revizije i procene sistema i usluga Kancelarije;
* konfigurisanje i održavanje sigurnosnih alata;
* detektovanje upada u sistem;
* objavljivanje novih informacija i vesti od značaja za informacionu bezbednost;
* diseminaciju znanja državnim organima u vezi sa informacionom bezbednošću;
* sprovođenje bezbednosne revizije i procene.
	1. **Usluge u domenu upravljanja kvalitetom bezbednosti**
* analiza rizika;
* obezbeđivanje kontinuiranog poslovanja u situacijama kada dođe do incidenata;
* podizanje nivoa svesti o informacionoj bezbednosti;
* edukaciju zaposlenih.
1. **Forma za prijavu incidenta**

Forma za prijavu incidenta se nalazi na https://www.ite.gov.rs/tekst/sr/88/cert.php

1. **Izjava odricanja od odgovornosti**

OITeG CERT preduzima sve korake kako bi osigurao ispravnost informacija koje deli, ali ne preuzima odgovornost za bilo kakvu štetu nastalu korišćenjem istih.