



Obvladovanje dogodkov in incidentov informacijske varnosti

Verzija dokumenta: 1.1

Datum veljavnosti: 23. 8. 2023 oziroma z dnem objave na SharePoint ARSO

Skrbnik dokumenta: Vodja informacijske varnosti

Oznaka dokumenta: ND-09/2023-1

Št. dokumenta (SPIS): 380-4/2023-3

Dokument pripravil:

mag. Bojan Pohar
podsekretar

Dokument odobril:

mag. Joško Knez
generalni direktor

Zgodovina sprememb:

Datum	Verzija	Avtorji	Spremembe
28. 5. 2020	Osnutek 0.1	Bojan Pohar	Priprava osnutka
12. 6..2020	Verzija 1.0	Bojan Pohar	Popravki glede na pripombe in komentarje
23. 8. 2023	Verzija 1.1.	Bojan Pohar	Dopolnitve vlog in priglasitev v primeru kršitev varstva osebnih podatkov Sklicevanje na referenčne dokumente Redakcijski popravki Sprememba podpisnika

Namen

Dokument Obvladovanje dogodkov in incidentov informacijske varnosti določa poenoteno reševanje incidentov, zbiranje vzrokov in rešitev na enem mestu z namenom reševanja incidentov v najkrajšem možnem času in na podlagi analize vzrokov predlagati izboljšave zagotavljanja informacijske varnosti Agencije Republike Slovenije za okolje (ARSO).

Ta dokument je interni dokument ARSO in je dostopen v aplikaciji Microsoft SharePoint na internem spletnem naslovu <http://dom.arso.sigov.si/>. Uporabnik je odgovoren, da preveri skladnost kopije z zadnjo veljavno različico.

VSEBINA

1 UVOD	5
1.1 Izrazi in definicije	6
1.2 Kratice	7
1.3 Referenčni dokumenti	7
2 NAMEN	8
3 VLOGE IN ODGOVORNOSTI	8
3.1 Uporabnik informacijskega sistema	8
3.2 IT podpora	8
3.3 Nosilec odziva	8
3.4 Skrbnik informacijskega sistema	9
3.5 Upravljavec informacijskega sistema	9
3.6 Vodja informacijske varnosti	9
3.7 Pooblaščen oseba za varstvo osebnih podatkov	9
3.8 Vodstvo	10
3.9 Nacionalni organ	10
4 PROCES OBVLADOVANJA DOGODKOV IN INCIDENTOV	10
5 SISTEM ZAZNAVE IN EVIDENTIRANJA DOGODKOV IN INCIDENTOV	10
6 ELEMENTI OBVLADOVANJA DOGODKOV IN INCIDENTOV	11
6.1 Zaznavanje	11
6.2 Priglasitev	11
6.3 Evidentiranje priglasitve	12
6.4 Zbiranje dodatnih informacij	12
6.5 Razvrščanje dogodka in incidenta glede na grožnjo in glede na vpliv	12
6.6 Potrditev incidenta	14
6.7 Obveščanje	14
6.8 Odziv	15
6.9 Priglasitev drugim organom	15
6.10 Poročanje	16
6.11 Analiza	16
6.12 Izboljševanje	16
7 UKREPI ZA PREPREČEVANJE DOGODKOV IN INCIDENTOV	17
8 TVEGANJA	17
9 NADZOR NAD IZVAJANJEM	17
10 VELJAVNOST	17
11 PRILOGE	17

1 UVOD

Dokument v skladu z Informacijsko varnostno politiko ARSO (IVP ARSO) obravnava obvladovanje dogodkov in incidentov informacijske varnosti, določa vloge in odgovornosti ter predpisuje postopke ukrepanja in obveščanja ob zaznavi dogodkov in incidentov.

Podlaga za pripravo in izvajanje postopkov obvladovanja dogodkov in incidentov informacijske varnosti je Zakon o informacijski varnosti (ZinfV) (Uradni list RS, št. 30/18)¹, Uredba o informacijski varnosti v državni upravi (UIVDU) (Uradni list RS, št. 29/18)² kot krovna politika informacijske varnosti organov državne uprave in Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. 68/19)³.

Pri izvajanju postopkov je potrebno glede na možnosti, ki jih posamezni informacijski sistemi (IS) omogočajo, ravnati v skladu z UIVDU, ki v Poglavju 6. Obvladovanje incidentov informacijske varnosti v členih 17. do 21. (Priloga1) predpisuje postopke organov državne uprave (ODU) v zvezi z dogodki in incidenti informacijske varnosti ter v skladu s Pravilnikom o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave, ki v 8. členu (Priloga2) opredeljuje odzivanje na incidente in protokol obveščanja odzivnega centra za incidente v informacijskih sistemih organov državne uprave (SIGOV-CERT) ter v skladu z Nacionalnim načrtom odzivanja na kibernetске incidente (NOKI)⁴.

V primeru vpliva dogodkov in incidentov informacijske varnosti na varstvo osebnih podatkov je pri izvajanju postopkov potrebno ravnati v skladu s Splošno uredbo o varstvu podatkov (GDPR)⁵ in Zakonom o varstvu osebnih podatkov (ZVOP-2) (Uradni list RS, št. 163/22)⁶.

Glede na številne in raznolike informacijskih rešitve, ki jih uporablja ARSO so možna tudi specifična odstopanja postopkov, ki v tem dokumentu niso zajeta. V teh primerih je potrebno odstopanja dokumentirati in seznaniti skrbnika dokumenta in izvajalce postopkov, ki so dolžni specifične dokumentirane postopke upoštevati.

Pri obravnavi dogodkov in incidentov informacijske varnosti je pomembno razumevanje definicij:

Dogodek informacijske varnosti (v nadaljevanju dogodek) je ugotovljeno stanje informacijskega sistema, storitev ali omrežja, ki kaže na možno kršitev politike informacijske varnosti ali izpad nadzorstev, ali predhodno neznane razmere, ki lahko pomembno vplivajo na varnost.

Incident informacijske varnosti (v nadaljevanju incident) je neželen dogodek informacijske varnosti ali zaporedje neželenih dogodkov informacijske varnosti, ki lahko z veliko verjetnostjo ogrozijo poslovanje in informacijsko varnost. Incident predstavlja tudi vse realizirane grožnje informacijske varnosti.

Kibernetска grožnja je možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja, sistema, storitev in podatkov.

¹ <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707>

² <http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED7198>

³ <http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV13669>

⁴ <https://www.gov.si/assets/organi-v-sestavi/URSIV/Datoteke/Dokumenti/2022-03-NOKI.pdf>

⁵ <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679>

⁶ <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7959>

1.1 Izrazi in definicije

1. celovitost je lastnost informacij in informacijskih sistemov, da so točne in popolne;
2. dogodek informacijske varnosti je ugotovljeno stanje informacijskega sistema, storitev ali omrežja, ki kaže na možno kršitev politike informacijske varnosti ali izpad nadzorstev, ali predhodno neznane razmere, ki lahko pomembno vplivajo na varnost;
3. državno komunikacijsko omrežje je omrežje, namenjeno povezovanju lokalnih omrežij organov državne uprave ter dostopu do skupnih informacijskih sistemov in storitev;
4. incident informacijske varnosti je neželen dogodek informacijske varnosti ali zaporedje neželenih dogodkov informacijske varnosti, ki lahko z veliko verjetnostjo ogrozijo poslovanje in informacijsko varnost;
5. informacije so obdelani, organizirani, strukturirani ali v nekem sobesedilu predstavljeni podatki;
6. informacijska naprava je naprava, namenjena za zbiranje, prenos, hrambo in obdelavo podatkov;
7. informacijska varnost je zagotavljanje (ohranjanje) zaupnosti, celovitosti in razpoložljivosti informacij;
8. informacijski sistem so med seboj odvisni sestavni deli računalniške strojne, programske in komunikacijske opreme, ki je namenjena za obravnavo (zajemanje, procesiranje, predstavitev, hrambo, prenos ipd.) nekega informacijskega premoženja; so tudi med seboj odvisne storitve, ki zagotavljajo strežniške in omrežne vire, vire za hrambo podatkov, vire uporabniške programske opreme ipd.;
9. informacijsko premoženje so podatki in informacije, ki jih je glede na poslovna in varnostna merila smiselno obravnavati kot celoto;
10. IT podpora je enotna kontaktna točka ARSO namenjena enotni podpori vsem uporabnikom informacijskega sistema ARSO;
11. lastni informacijski sistem je informacijski sistem organa, za katerega pridobitev, razvoj, integracijo, spreminjanje, delovanje, vzdrževanje, varovanje in prenehanje uporabe ter varovanje informacijskih premoženj, ki jih ta informacijski sistem obravnava, je odgovoren ta organ;
12. kibernetična grožnja je možnost zlonamernega poskusa poškodovanja ali prekinitev računalniškega omrežja, sistema, storitev in podatkov.
13. nadzorstvo je ukrep, ki zmanjšuje tveganje; vključuje postopke, usmeritve, naprave, prakse ali druge aktivnosti, ki zmanjšujejo tveganje;
14. nosilec odziva na dogodek in incident je oseba (običajno izvajalec), ki prevzame dogodek in incident v reševanje;
15. ocenitev tveganja je celotni proces ugotavljanja tveganja, analize tveganja in ovrednotenja tveganja;
16. okrevanje je obnovitev podatkov in delovanja informacijskega sistema ter poslovanja po izpadu informacijskega sistema ali poslovanja;
17. ovrednotenje tveganja je proces primerjanja rezultatov analize tveganja z merili tveganja, da bi ugotovili, ali je tveganje oziroma njegova velikost sprejemljiva oziroma znosna;
18. podatki so formalizirana predstavitev dejstev, zamisli ali navodil, primernih za človeško ali strojno komunikacijo, interpretacijo ali obdelavo;
19. razpoložljivost je lastnost informacij in informacijskih sistemov, da so dostopni in uporabni na pooblaščen zahtevo;
20. revizijska sled je dnevnik z zapisi o operacijah nad poslovnimi podatki;
21. sistem upravljanja informacijske varnosti je sistem upravljanja, ki omogoča celovit in koordiniran pogled na informacijska varnostna tveganja organizacije ter zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti omrežij in informacijskih sistemov;
22. skrbnik informacijskega sistema je oseba, ki je odgovorna za pridobitev, razvoj, integracijo, spreminjanje, delovanje, vzdrževanje, varovanje in prenehanje uporabe tega informacijskega sistema in za varovanje informacijskih premoženj, ki jih ta informacijski sistem obravnava;
23. upravljavec informacijskega sistema je oseba ali skupina oseb ali organizacijska enota ali pogodbeni izvajalec, ki skrbi za učinkovito nameščanje, konfiguriranje, integracijo, vzdrževanje, delovanje ter izvaja druge naloge operativnega upravljanja in varovanje

- tega informacijskega sistema v skladu z navodili skrbnika tega informacijskega sistema, sprejetimi notranjimi akti organa, operativnimi navodili in sprejetimi standardi na področju informacijske varnosti;
24. zlonamerna programska oprema so vsi zlonamerni programi, na primer virusi, črvi, stranska vrata, trojanski konji, vohunsko programje;
 25. tveganje je učinek negotovosti na zastavljene cilje;
 26. ugotavljanje tveganja je proces odkrivanja, prepoznavanja in opisovanja tveganj;
 27. uporabnik je oseba, ki uporablja računalniške ali omrežne storitve;
 28. zaupnost je lastnost, da informacije niso razpoložljive ali razkrite nepooblaščenim subjektom ali procesom

1.2 Kratice

- ARSO – Agencija Republike Slovenije za okolje
- DIDI – Direktorat za informacijsko družbo in informatiko
- EU – Evropska unija
- EKC – enotni kontaktni center državne uprave
- ENISA - Evropska agencija za kibernetsko varnost
- HKOM – državno komunikacijsko omrežje
- IP – informacijsko premoženje
- IS – informacijski sistem
- ISO 9001:2015 – standard za sisteme vodenja kakovosti – zahteve
- ISO 27001:2017 – standard za sistem upravljanja informacijske varnosti - zahteve
- ISO 27002:2017 – standard za sistem upravljanja informacijske varnosti - kontrole
- ISO 22301:2014 – standard za sistem vodenja neprekinjenega poslovanja - zahteve
- IV – informacijska varnost
- IVP – Informacijska varnostna politika
- IVP ARSO – Informacijska varnostna politika ARSO
- MDP – Ministrstvo za digitalno preobrazbo
- NOE – notranja organizacijska enota
- ODU – organ državne uprave
- SI-CERT – Nacionalni odzivni center za kibernetsko varnost
- SIGOV-CERT – Odzivni center za incidente v informacijskih sistemih ODU
- SIEM – Sistem za upravljanje incidentov in dogodkov (angleško Security Information and Event Management)
- SUIV – Sistem upravljanja informacijske varnosti
- SOC – Varnostno operativni center (angleško Security Operations Center)
- UIVDU – Uredba o informacijski varnosti v državni upravi
- URSIV – Uprava Republike Slovenije za informacijsko varnost
- ZCR – zaupnost, celovitost, razpoložljivost
- ZinfV – Zakon o informacijski varnosti

1.3 Referenčni dokumenti

- ARSO - Poslovnik vodenja sistema kakovosti (010-8/2018-9)
- ARSO - Opisi procesov – Dodatek k poslovniku vodenja kakovosti (010-8/2018-2)
- ARSO - Informacijska varnostna politika (380-1/2019-12)
- Zakon o informacijski varnosti (Uradni list RS, št. [30/18](#))
- Uredba o informacijski varnosti v državni upravi (Uradni list RS, št. [29/18](#))
- Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. [68/19](#))
- Splošna uredba (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP-2) (ULRS št. [163/22](#))

2 NAMEN

Dokument Obvladovanje dogodkov in incidentov informacijske varnosti določa poenoteno obravnavanje dogodkov in incidentov, zbiranje in evidentiranje vzrokov in rešitev na enem mestu z namenom reševanja incidentov v najkrajšem možnem času in na podlagi analize vzrokov predlagati preventivne ukrepe za izboljšanje zagotavljanja informacijske varnosti ARSO. Opredeljuje način obveščanja in ukrepanja v zvezi z dogodki in incidenti z namenom omejitve grožnje informacijske varnosti in povzročitve nadaljnje škode.

Dokument velja tako za zaposlene kot tudi za vse zunanje uporabnike, ki dostopajo do IS ARSO.

3 VLOGE IN ODGOVORNOSTI

3.1 Uporabnik informacijskega sistema

Uporabnik informacijskega sistema (v nadaljevanju Uporabnik) je dolžan:

- dosledno upoštevati in izvajati ukrepe za preprečevanje dogodkov in incidentov informacijske varnosti,
- priglasiti dogodke in incidente informacijske varnosti enotni kontaktni točki ARSO,
- priglasiti enotni kontaktni točki ARSO vsak sum ogrožanja informacijske varnosti,
- ravnati v skladu z navodili za preprečitev nadaljnje škode in zavarovanje dokazov.

3.2 IT podpora

IT podpora je enotna kontaktna točka ARSO, ki predstavlja 1. nivo podpore in je zadolžena za:

- sprejemanje prijavitev kršitev informacijske varnosti,
- sprejemanje prijavitev dogodkov in incidentov informacijske varnosti,
- evidentiranje prijavitev,
- razvrščanje prijavitev glede na stopnjo ogroženosti informacijske varnosti,
- posredovanje navodil prijavitelju glede ustreznega ravnanja ob prepoznanem dogodku ali incidentu informacijske varnosti,
- izvedbo ukrepov za preprečitev nadaljnje škode in zavarovanje dokazov,
- samostojno ali s pomočjo strokovno usposobljenih upravljavcev odpravo posledic oziroma grožnje informacijske varnosti,
- obveščanje skrbnika, upravljavca in vodje informacijske varnosti,
- pomoč uporabnikom pri preprečevanju in zaznavanju dogodkov in incidentov informacijske varnosti.

3.3 Nosilec odziva

Nosilec odziva na dogodek in incident (v nadaljevanju nosilec) je običajno izvajalec, ki prevzame dogodek in incident v reševanje. Zadolžen je za:

- izvajanje aktivnosti odziva,
- evidentiranje odziva
- obveščanje o poteku odziva,
- po potrebi vključevanje skrbnikov, upravljavcev, strokovnih sodelavcev, vodje informacijske varnosti in vodstva v izvajanje potrebnih aktivnosti,
- pripravo poročila o dogodku in incidentu z opisom izvedenih aktivnosti v postopku odziva,
- predlaganje ukrepov za preprečevanje dogodkov in incidentov.

3.4 Skrbnik informacijskega sistema

Skrbnik informacijskega sistema (v nadaljevanju skrbnik) je zadolžen za:

- spremljanje dogodkov in incidentov informacijske varnosti informacijskega sistema katerega je skrbnik,
- pomoč pri odkrivanju, preprečevanju in obravnavi dogodkov in incidentov informacijske varnosti,
- prigrasitev ugotovljenih dogodkov in incidentov informacijske varnosti enotni kontaktni točki ARSO.
- pomoč pri pripravi analize dogodkov in incidentov,
- predlaganje ukrepov za preprečevanje dogodkov in incidentov.

3.5 Upravljevec informacijskega sistema

Upravljevec informacijskega sistema (v nadaljevanju upravljevec) je zadolžen za:

- preprečevanje in odkrivanje dogodkov in incidentov informacijske varnosti,
- odzivanje na dogodke in incidente informacijske varnosti,
- odpravo posledic oziroma grožnje informacijske varnosti,
- poročanje o dogodkih in incidentih informacijske varnosti,
- prigrasitev ugotovljenih dogodkov in incidentov informacijske varnosti enotni kontaktni točki ARSO.
- pridobitev, delovanje in vzdrževanje informacijskih orodij za sistem upravljanja dogodkov in incidentov, orodij za odkrivanje in preprečevanje vdorov, orodij za preprečevanje delovanja škodljive programske opreme in drugih orodij za pomoč pri zagotavljanju informacijske varnosti
- pomoč pri pripravi analize dogodkov in incidentov informacijske varnosti,
- predlaganje ukrepov za preprečevanje dogodkov in incidentov.

3.6 Vodja informacijske varnosti

Vodja informacijske varnosti je zadolžen za:

- obravnavo in nadzor dogodkov in incidentov informacijske varnosti,
- nadzor nad izvajanjem postopkov obvladovanja dogodkov in incidentov,
- obveščanje SIGOV-CERT o dogodkih in incidentih informacijske varnosti,
- sodelovanje s pooblaščenimi osebo za varstvo osebnih podatkov,
- pripravo analize incidentov informacijske varnosti,
- predlaganje ukrepov za preprečevanje incidentov
- pripravo analize ocene tveganja in identificiranih groženj,
- redno poročanje predstojniku.

3.7 Pooblaščen osebni za varstvo osebnih podatkov

Pooblaščen osebni za varstvo osebnih podatkov je zadolžen za:

- pomoč in sodelovanje pri obravnavi in nadzoru dogodkov in incidentov informacijske varnosti, ki imajo vpliv na varstvo osebnih podatkov,
- obveščanje nadzornega organa o kršitvi varstva osebnih podatkov najkasneje v 72 urah po seznanitvi s kršitvijo,
- izvedbo obveščanja posameznikov, na katere se nanašajo osebni podatki, v primeru kršitve varstva osebnih podatkov

3.8 Vodstvo

Vodstvo je odgovorno za učinkovito upravljanje informacijske varnosti. V zvezi z obvladovanjem dogodkov in incidentov informacijske varnosti vodstvo pregleduje in potrjuje:

- analize incidentov informacijske varnosti,
- analize ocene tveganja in identificiranih groženj,
- ukrepe in predloge za preprečevanje incidentov,
- ukrepe za odpravo posledic incidentov večjih razsežnosti in preprečitve nadaljnje škode.

3.9 Nacionalni organ

Za prigrasitev incidentov organov državne uprave, ki upravljajo informacijske sisteme in dele omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti je pristojen Odzivni center za incidente v informacijskih sistemih organov državne uprave (SIGOV-CERT)⁷, ki deluje v okviru Ministrstva za digitalno preobrazbo.

Za prigrasitev incidentov v zvezi z varstvom osebnih podatkov je pristojen samostojen in neodvisen državni organ Informacijski pooblaščenec⁸

4 PROCES OBVLADOVANJA DOGODKOV IN INCIDENTOV

Obvladovanje dogodkov in incidentov informacijske varnosti poteka v skladu z upoštevanjem specifičnih potreb in zakonskih zahtev.

5 SISTEM ZAZNAVE IN EVIDENTIRANJA DOGODKOV IN INCIDENTOV

Sistem zaznave in evidentiranja dogodkov in incidentov informacijske varnosti ARSO sestavljajo različne informacijske in organizacijske rešitve. Skupna točka in povezava je IT podpora, ki omogoča prigrasitev s strani uporabnikov, skrbnikov ali upravljavcev in evidentiranje zaznanih dogodkov in incidentov na enem mestu ter komunikacijo in obveščanje. Postopek prikazuje diagram poteka obvladovanja dogodkov in incidentov (Priloga4).

Zaščita pred grožnjami virusov je s programsko opremo za zaščito, odkrivanje in obveščanje pred grožnjami zlonamerne programske opreme (virusov) sistemsko urejena v okviru standardne programske opreme za strežnike in osebne računalnike.

Delovanje kritične infrastrukture ARSO (strežniki in omrežje) je nadzorovano s programskim orodjem za sistem upravljanja incidentov in dogodkov (SIEM)⁹, ki upravljavcu avtomatizirano zagotavlja zaznavanje in evidentiranje dogodkov in incidentov kritične infrastrukture ter omogoča preventivno ukrepanje in odzivanje na prepoznane dogodke in incidente.

Nadzor fizičnega dostopa je urejen z sistemom elektronske dostopne kontrole, video nadzornim sistemom, fizičnim varovanjem in alarmnim sistemom nepooblaščenega dostopa v sistemski prostor.

Varovanje pred požarom je urejeno s protipožarnim sistemom.

⁷ <https://www.gov.si teme/informacijska-varnost/>

⁸ <https://www.ip-rs.si/>

⁹ <https://icinga.com/>

Komunikacijsko varnost oddaljenih ARSO lokacij do centralne ARSO lokacije zagotavlja državno komunikacijsko omrežje HKOM. Omrežje HKOM upravlja Ministrstvo za digitalno preobrazbo (MDP). MDP Operativni varnostni center (SOC) izvaja stalni proaktivni nadzor omrežja in se odziva na potencialne grožnje ter ustrezno obvešča potencialno ogrožene uporabnike.

Evidenca priglasitev dogodkov in incidentov se glede izvor priglasitev nahaja v obliki zapisov v skupni mapi evidence dogodkov in incidentov¹⁰ ter mapi evidence infrastrukturnih incidentov ¹¹, oziroma v sistemu SIEM.

V primeru potrebe po evidentiranju in upravljanju povečanega števila priglasitev je priporočljiva vsaj uporaba preglednice (primer Priloga3) oziroma informacijski sistem za celovito podporo aktivnostim IT podpore vključno z upravljanjem informacijskega premoženja, upravljanja zahtevkov, dogodkov, incidentov in sprememb ter baze znanja.

6 ELEMENTI OBVLADOVANJA DOGODKOV IN INCIDENTOV

6.1 Zaznavanje

Zaznavanje dogodkov in incidentov sestavlja:

- avtomatizirano zaznavanje in obveščanje upravljavca oziroma uporabnika v okviru sistemskih rešitev protivirusne programske opreme, sistema SIEM, pristopne kontrole, alarmnega in protipožarnega sistema,
- zaznavanje upravljavcev informacijskih sistemov in storitev,
- zaznavanje skrbnikov informacijskih sistemov in storitev,
- zaznavanje uporabnikov informacijskih sistemov in storitev,
- zaznavanje osebja IT podpore,
- zaznavanje vodje informacijske varnosti
- zaznavanje vzdrževalcev informacijske opreme,
- zaznavanje izvajalcev fizičnega varovanja
- obveščanje upravljavca omrežja HKOM,
- obveščanje pogodbenih izvajalcev storitev,
- ugotovitve notranjih presoj in revizij.

6.2 Priglasitev

Za priglasitev vseh dogodkov in incidentov na enem mestu je namenjena IT podpora.

Kdorkoli in neglede na način zaznave dogodkov in incidentov mora nemudoma priglasiti zaznani dogodek ali incident IT podpori vsaj na en način:

- preko elektronske pošte ITpodpora.arso@gov.si,
- po telefonu 01 478 4085, ob dela prostih dnevih od 8.00 do 14.00 na GSM 041 674 191,
- osebno na lokaciji IT podpore.

Informacijske naprave in sistemi ter nadzorni sistemi pošiljajo upravljavcem avtomatska obvestila preko:

- elektronske pošte,
- SMS sporočil

¹⁰ [\\venera\InformacijskaVarnost\Incidenti_IV](#)

¹¹ [\\venera\INFOdoc\incidenti](#)

6.3 Evidentiranje priglasitve

IT podpora priglasitev dogodka in incidenta informacijske varnosti evidentira v evidenci dogodkov in incidentov.

Evidentiranje obsega najmanj naslednje podatke:

- referenčna številka,
- datum in ura priglasitve,
- vrsta dogodka
- vrsta incidenta glede na grožnjo
- vrsta incidenta glede na težo
- Priimek in Ime priglasitelja,
- kratek opis,
- lokacija,
- oceno obsega prizadetega oziroma ogroženega informacijskega premoženja,
- ocena škode
- pomembne informacije o dogodku, incidentu

6.4 Zbiranje dodatnih informacij

V primeru, da IT podpora presodi, da so potrebne dodatne informacije poskrbi za njihovo pridobitev pri priglasitelju, skrbniku, upravljavcu ali s pridobivanjem informacij na terenu.

Zaželeno je zbrati maksimalen obseg informacij za čim bolj natančno prepoznavo in razvrščanje glede na vrsto in obseg dogodka in incidenta, kar omogoča ustreznost odziva v najkrajšem možnem času in kasnejšo analizo.

IT podpora z dodatno zbranimi informacijami dopolni evidenco dogodkov in incidentov.

Pri zbiranju dodatnih informacij incidenta in tudi med samim odzivom so v pomoč vprašanja, katerih odgovori so lahko pomembni za potek odziva in reševanje dogodka in incidenta:

1. Ali so sumi upravičeni ali je prišlo do napake kje drugje (programska ali človeška napaka).
2. Ali je pri incidentu prišlo do kakršnekoli škode?
3. Kakšna je verjetnost, da je prišlo do spremembe sistemskih programov (stranska vrata in trojanski konji)?
4. Ali boste nadaljevanje incidenta spremljali z namenom zbiranja dodatnih podatkov, ali želite sisteme čimprej "očistiti"?
5. Kako je najbolje zavarovati podatke; ali je možno, da bo prišlo do kazenskega pregona?
6. Ali je potrebno prizadete sisteme ali dele omrežja čimprej spet spraviti v stanje normalnega delovanja na omrežju?
7. Ali želite je potrebno oziroma želite o incidentu koga obvestiti (znotraj ali zunaj vaše organizacije), ali pa nasprotno želite informacijo zadržati v čim ožjem krogu?
8. Ali se lahko incident ponovi?
9. Ali gre za posledice načrtovane ali nenačrtovane spremembe?
10. Ali gre za problem, ki zahteva spremembo?

6.5 Razvrščanje dogodka in incidenta glede na grožnjo in glede na vpliv

IT podpora glede na zbrane informacije določi vrsto dogodka in incidenta in dopolni evidenco dogodkov in incidentov.

Pri razvrščanju po potrebi sodelujejo tudi skrbniki, upravljavci vodja informacijske varnosti ali drugo strokovno osebje

Razvrščanje dogodka in incidenta se glede na dodatno zbrane informacije ali ugotovitve tekom odziva lahko spreminja oziroma dopolni.

Dogodek informacijske varnosti je ugotovljeno stanje informacijskega sistema, storitev ali omrežja, ki kaže na možno kršitev politike informacijske varnosti ali izpad nadzorov, ali predhodno neznane razmere, ki lahko pomembno vplivajo na varnost.

vrsta dogodka:

1. neučinkovit nadzor nad varnostjo v informacijskih sistemih,
2. odstopanja od pričakovane celovitosti, zaupnosti ali dostopnosti informacij,
3. človeške napake,
4. neskladnost s politikami ali navodili,
5. kršitev ureditve fizične varnosti, ki bi lahko vplivala na informacijsko varnost,
6. nenadzorovane sistemske spremembe,
7. motnje v delovanju programske ali strojne opreme,
8. kršitve dostopa,
9. druge sumljive okoliščine.

Incident informacijske varnosti je neželen dogodek informacijske varnosti ali zaporedje neželenih dogodkov informacijske varnosti, ki lahko z veliko verjetnostjo ogrozijo poslovanje in informacijsko varnost. Incident predstavlja tudi vse realizirane grožnje informacijske varnosti.

vrsta incidenta glede na grožnjo:

1. naravna ali druga nesreča,
2. javni nemiri,
3. fizična poškodba,
4. odpoved infrastrukture,
5. učinki sevanja,
6. tehnična okvara,
7. škodljivo programje,
8. tehnični napad,
9. kršitev pravil,
10. ogrožanje funkcij,
11. ogrožanje informacij,
12. škodljiva vsebina,
13. drugo.

glede na težo incidenta:

1. lažji incident je enkratni incident, ki ima majhen negativen vpliv na ZCR, nima večjega vpliva na izvajanje storitev in ne povzroči večje škode
2. težji incident je enkratni incident oziroma zaporedje večjega števila različnih incidentov v kratkem obdobju, ki ima velik negativen vpliv na ZCR s pomembnim vplivom na izvajanje storitev in povzroči večjo škodo. Lahko ima tudi medpodročni vpliv na druge organe.
3. kritični incident je tisti incident ki ima zelo velik negativen vpliv na ZCR in povzroči oteženo delovanje države.

Kibernetska grožnja je možnost zlonamernega poskusa poškodovanja ali prekinitev računalniškega omrežja, sistema, storitev in podatkov. Realizirana kibernetska grožnja pomeni incident informacijske varnosti.

Najpogostejše prepoznane kibernetske grožnje¹² glede na klasifikacijo Evropske agencije za kibernetsko varnost (ENISA):

¹² https://www.gov.si/assets/ministrstva/MJU/DI/Ocena_kibernetskih_tveganj_v1_0_Fina_P.pdf

1. škodljiva koda (Malware),
2. spletni napadi (Web Based Attacks),
3. napadi na spletne aplikacije (Web Application Attacks),
4. zvaabljanje (Phishing),
5. nezaželena elektronska pošta (Spam),
6. onemogočanje storitve (Denial of Service),
7. izsiljevalsko programje (Ransomware),
8. omrežni roboti (Botnets),
9. grožnje od znotraj (Insider Threat),
10. fizična manipulacija/poškodba/kraja/izguba (Physical manipulation/damage/ theft/loss),
11. kršitve podatkov (Data Breaches),
12. kraja identitete (Identity Theft),
13. odtekanje informacij (Information leakage),
14. kompleti za izkoriščanje (Exploit Kits),
15. kibernetško vohunjenje (Cyber-Espionage).

6.6 Potrditev incidenta

Ob prepoznavi dogodka, da gre za incident informacijske varnosti je potrebno ugotovitve posredovati v seznanim in potrditev vodji informacijske varnosti.

Postopek potrjevanja incidenta s stani vodje informacijske varnosti, ne zadrži takojšnjega izvajanja odziva.

6.7 Obveščanje

Obveščanja poteka glede na prepoznano vrsto in obseg dogodka ali incidenta. Pri tem je pomembno je, da informacije o ranljivosti storitev ostanejo zaupne, dokler se varnost znova ne vzpostavi.

IT podpora posreduje povratne informacija priglasitelju z navodili za ukrepanje ter obvešča vodjo informacijske varnosti, upravljavca in skrbnika prizadetega informacijskega sistema in pooblaščen osebo za varstvo osebnih podatkov v primeru kršitve varstva osebnih podatkov. V primeru težjega ali kritičnega incidenta takoj obvesti celotno vodstvo ARSO.

Nosilec, ki je dogodek in incident prevzel v reševanje mora obveščati IT podporo v primernih časovnih intervalih o predvidenem času odprave posledic dogodka in incidenta ter obvestiti IT podporo o ponovni vzpostavitvi delovanja informacijskih storitev.

IT podpora (po dogovoru lahko tudi skrbnik, upravljavec ali vodja informacijske varnosti) obvesti uporabnike, katerim je zaradi dogodka in incidenta onemogočena uporaba informacijskih storitev, o nedelovanju storitev, jih obvešča v primernih časovnih intervalih o predvidenem času odprave posledic dogodka in incidenta ter jih obvestiti o ponovni vzpostavitvi delovanja informacijskih storitev.

Vodja informacijske varnosti obvešča oziroma prihlasi incident ustreznim organom, v kolikor je to potrebno (Policija, SI-CERT).

Pooblaščen oseba za varstvo osebnih podatkov prihlasi incident nadzornemu organu (Informacijski pooblaščenec) in poskrbi za obveščanje posameznikov, na katere se nanašajo osebni podatki, kadar je verjetno, da kršitev varnosti osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov (Splošna uredba člen 33 in člen 34 – Priloga5).

6.8 Odziv

Odziv na dogodke in incidente informacijske varnosti se izvaja na več nivojih:

1. nivo predstavlja IT podpora, ki prva prejme priglasitev dogodka in incidenta izjemoma so to lahko tudi skrbniki,
2. nivo predstavljajo notranji strokovni sodelavci oziroma upravljavci,
3. nivo predstavljajo zunanji izvajalci

Na 1. nivoju se izvaja reševanje dogodkov in incidentov primernih strokovni usposobljenosti osebja IT podpore. Običajno so to že od prej poznani dogodki in incidenti, za katere obstajajo poznane rešitve. Pri odzivu in reševanju je v pomoč iskanje rešitev v bazi znanja oziroma evidenci preteklih dogodkov in incidentov.

Osebe IT podpore takoj po prijavitvi, zbiranju dodatnih informacij in razvrščanju, če presodi, da je usposobljeno za reševanje, prevzame dogodek ali incident v reševanje oziroma ga dodeli v reševanje na 2. ali 3. nivo.

V primeru, da gre za incident informacijske varnosti IT podpora obvesti vodjo informacijske varnosti.

Odziv se prične s prevzemom dogodka in incidenta v reševanje na 1. nivoju ali prevzemom v reševanje na 2. ali 3. nivoju z določitvijo nosilca odziva (izvajalca). IT podpora vpiše v evidenco dogodkov in incidentov datum, uro ter ime in priimek izvajalca reševanja.

Odziv obsega:

- Omejitev škode,
- Zagotovitev zahtevane ravni informacijske varnosti,
- Ugotavljanje vzrokov in posledic,
- Zbiranje in zavarovanje dokazov čim prej po incidentu,
- Opravljanje forenzičnih aktivnosti, v kolikor je to potrebno,
- Odprava posledic in okrevanje delovanja informacijskega sistema in izvajanja storitev,
- Obveščanje priglasiatelja, odgovornih oseb in drugih organov ali organizacij,
- Obveščanje uporabnikov, katerim je onemogočena uporaba informacijskih storitev,
- Beleženje aktivnosti,
- Vpis v bazo znanja,
- Zaključevanje v evidenci dogodkov in incidentov.

6.9 Priglasitev drugim organom

Če vodja informacijske varnosti presodi, da gre za dogodek, ki vpliva ali bi lahko vplival tudi na druge organe ali druge povezane subjekte ali bi za njegovo obravnavo potreboval zunanjo pomoč, dogodek priglasi SIGOV-CERT prek sistema za pomoč in priglasitev napak enotnega kontaktnega centra (EKC). Po potrebi vodja informacijske varnosti v dogovoru z generalnim direktorjem ARSO o dogodku obvesti tudi druge organe (Policija, SI-CERT, URSIV).

Priglasitev dogodka informacijske varnosti na SIGOV-CERT vsebuje naslednje informacije:

- Identifikacijska oznaka dogodka: Številka interne evidence ali SPIS zadeve
- Podatki o osebi ki poroča: Ime Priimek, funkcija
- Opis dogodka: kaj, kdaj, kako in zakaj se je zgodil, kdaj je bil odkrit, katero premoženje je bilo prizadeto
- Podrobnosti o dogodku z oceno:
 - števila uporabnikov, ki jih je prizadela motnja pri zagotavljanju storitev,
 - trajanja incidenta,
 - geografske razširjenosti, kar zadeva območje, na katerega incident vpliva,
 - morebitnega medresorskega vpliva incidenta in

- pomembnosti vpliva incidenta na izvajanje storitev (lažji incident, težji incident, kritični incident).

V primeru kršitve varstva osebnih podatkov pooblaščenca oseba za varstvo osebnih podatkov pripravi nadzornemu organu (Informacijski pooblaščenec) zaznani kršitev varnosti osebnih podatkov, če je (vsaj) verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. Obvestilo je treba podati takoj po zaznani kršitvi, najkasneje pa v 72 urah. Podrobnejša navodila, smernice in obrazec so dostopni na spletni strani Informacijskega pooblaščenca »Prijava kršitev varnosti«¹³.

6.10 Poročanje

Po zaključku odziva na dogodek in incident nosilec pripravi poročilo, ki obsega:

- Osnovne informacije: dogodek ali incident kratka oznaka, vrsta dogodka in incidenta, vpliv, podatki o priglasiavi zaznavi, datum, ura, priglasiatelj, lokacija, podroben opis, resnost, trajanje, učinek na zaupnost celovitost in razpoložljivost (ZCR)
- Postopek odziva: sodelujoči v postopku, začetek in konec odziva, omejitev škode, zavarovanje dokazov, odstranitev grožnje, odprava posledic,
- Ugotovitev: obseg vpliva oziroma povzročene kode, povzročitelj, verjetnost ponovitve
- Ukrepi: Obveščanje: vodstva, uporabnikov, SIGOV-CERT, ustreznih organov
- Predlog nadaljnjih ukrepov za preprečitev ponovitve: proučitev pomanjkljivosti, organizacijski, tehnični ukrepi

Pri pripravi poročila po potrebi sodelujejo tudi: IT podpora, skrbniki, upravljavci, vodja informacijske varnosti in ostali povezani z nastankom oziroma odzivom na dogodek in incident.

6.11 Analiza

Najmanj enkrat letno običajno kot gradivo za vodstveni pregled vodja informacijske varnosti pripravi analizo dogodkov in incidentov.

Analiza predstavlja podlago za predlaganje ukrepov za preprečevanje dogodkov in incidentov izboljšave postopkov obvladovanja dogodkov in incidentov ter gradivo za oceno tveganja informacijske varnosti.

6.12 Izboljševanje

Podlaga za izboljšanje postopka ukrepanja ob dogodkih in incidentih so:

- rezultati analize dogodkov in incidentov
- spremenjene ocene tveganja informacijske varnosti,
- baza znanja poznanih dogodkov in incidentov,
- zakonodaja,
- standardi,
- dobre prakse,
- ideje, pobude, predlogi,
- nove grožnje iz okolja,
- nova tehnologija in storitve,
- ugotovljene neskladnosti presoj in revizij,
- ugotovitve vodstvenega pregleda,
- vse kar lahko pripomore k izboljšanju informacijske varnosti.

¹³ <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebni-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/prijava-kr%C5%A1itev>

7 UKREPI ZA PREPREČEVANJE DOGODKOV IN INCIDENTOV

Ukrepi za preprečevanje dogodkov in incidentov se stalno dopolnjujejo in prilagajajo glede na nove grožnje in dobre prakse. Pomembnejši ukrepi:

- Redno posodabljanje odobrene protivirusne programske opreme, ki mora biti nameščena na vseh osebnih računalnikih in strežnikih in tudi na vseh ostalih napravah za dostop do informacijskega sistema,
- Nemudoma prekiniti z uporabo informacijskega sistema ter obvestiti IT podporo v primeru zaznave nedelovanja protivirusne zaščite suma potencialnega nameščanja, uporabe, širjenja ali delovanja zlonamerne programske opreme.
- Redno posodabljanje systemske programske opreme po priporočilu proizvajalca,
- Vzdrževanje in posodabljanje informacijskih sistemov in nadzornih sistemov,
- Zagotavljanje ustreznih kapacitet informacijskih sistemov glede na predvidene potrebe in tekoče spremljanje dejanskega stanja,
- Uporaba informacijske opreme in sistemov v skladu z navodili,
- Upoštevanje Informacijske varnostne politike, pravil in navodil,
- Spremljanje obvestil SIGOV-CERT in SI-CERT,
- Ozaveščanje in usposabljanje uporabnikov in strokovnih sodelavcev,
- Prepovedano je:
 - zaganjanje, nameščanje in uporaba neodobrene programske opreme, ki ni del informacijskega sistema ARSO,
 - odpiranje sumljivih dokumentov neznanega izvora (internet, elektronska pošta, pomnilniški mediji) oziroma se ne ve čemu so namenjeni, ker lahko vsebujejo zlonamerno programsko opremo,
 - kakršno koli samovoljno poseganje v delovanje ali izključevanje protivirusne zaščite.

8 TVEGANJA

Pomanjkanje ustrezno usposobljenega kadra.

Opustitev preventivnih ukrepov.

Še nepoznane grožnje.

9 NADZOR NAD IZVAJANJEM

Za nadzor nad izvajanjem je odgovoren vodja informacijske varnosti.

10 VELJAVNOST

Dokument prične veljati z objavo na Microsoft Share Point Oglasni deski na internem spletnem naslovu <http://dom.arso.sigov.si/>.

11 PRILOGE

Priloga1: Uredba o informacijski varnosti v državni upravi, Poglavje 6. Obvladovanje incidentov informacijske varnosti

Priloga2: Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave, 8. člen

Priloga3: Evidenca dogodkov in incidentov

Priloga4: Diagram poteka obvladovanja dogodkov in incidentov

Priloga5: Splošna uredba o varstvu podatkov (GDPR) člen 33 in člen 34

PRILOGA1

UREDBA O INFORMACIJSKI VARNOSTI V DRŽAVNI UPRAVI

Poglavje 6. Obvladovanje incidentov informacijske varnosti

17. člen (postopki obvladovanja incidentov informacijske varnosti)

Organ in povezani subjekt vzpostavita postopke za:

- spremljanje, zaznavanje, analiziranje in poročanje o dogodkih in incidentih informacijske varnosti,
- beleženje aktivnosti obvladovanja incidentov in
- odziv na incidente, vključno s postopki za stopnjevanje ukrepov informacijske varnosti, postopki za nadzorovano obnovo po incidentu in komunikacijo z notranjimi ali zunanjimi osebami ali organizacijami.

18. člen (zaznava dogodkov in incidentov informacijske varnosti)

(1) Organ in povezani subjekt vzpostavita postopke za zaznavo dogodkov in incidentov informacijske varnosti v informacijskem sistemu in delovnem okolju.

(2) Kjer je mogoče in smiselno, se uvedejo samodejni sistemi za zaznavo, beleženje in analizo dogodkov in incidentov informacijske varnosti.

19. člen (obveščanje in prigrasitev dogodkov informacijske varnosti)

(1) Uslužbenec organa oziroma povezanega subjekta nemudoma obvesti vodjo informacijske varnosti oziroma koordinatorja informacijske varnosti o dogodku informacijske varnosti, če zazna:

- neučinkovit nadzor nad varnostjo v informacijskih sistemih,
- odstopanja od pričakovane celovitosti, zaupnosti ali dostopnosti informacij,
- človeške napake,
- neskladnost s politikami ali navodili,
- kršitev ureditve fizične varnosti, ki bi lahko vplivala na informacijsko varnost,
- nenadzorovane sistemske spremembe,
- motnje v delovanju programske ali strojne opreme,
- kršitve dostopa ali
- druge sumljive okoliščine.

(2) Pogodbene izvajalce se zaveže k obveščanju iz prejšnjega odstavka s pogodbo.

(3) Vodja informacijske varnosti oziroma koordinator informacijske varnosti beleži informacije o dogodkih informacijske varnosti v organu oziroma povezanem subjektu.

(4) Če vodja informacijske varnosti oziroma koordinator informacijske varnosti presodi, da gre za tak dogodek informacijske varnosti, ki vpliva ali bi lahko vplival tudi na druge organe ali druge povezane subjekte ali bi za njegovo obravnavo potreboval zunanjo pomoč, dogodek priglasi ministrstvu prek sistema za pomoč in prigrasitev napak.

(5) Prigrasitev dogodka informacijske varnosti vsebuje naslednje informacije:

- identifikacijsko oznako dogodka,
- podatke o osebi, ki poroča,
- opis dogodka, ki vsebuje podatke o tem, kaj, kako in zakaj se je zgodil, katero premoženje je bilo prizadeto, kakšni so bili negativni poslovni učinki ter katere so zaznane ranljivosti, in
- podrobnosti o dogodku, ki vključujejo podatke o tem, kdaj se je zgodil, kdaj je bil odkrit, kdaj se je poročalo o njem, ali je zaključen in koliko časa je trajal.

(6) Ministrstvo o dogodku informacijske varnosti lahko zbere dodatne informacije in presodi, ali gre za incident informacijske varnosti.

20. člen (evidentiranje incidentov informacijske varnosti)

(1) Ministrstvo vodi evidenco incidentov informacijske varnosti.

(2) Ministrstvo vpiše informacije o incidentu informacijske varnosti v evidenco incidentov informacijske varnosti, ki poleg podatkov iz prejšnjega člena vsebuje še podatke o:

- vrsti incidenta informacijske varnosti, glede na grožnjo (naravna ali druga nesreča, javni nemiri, fizična poškodba, odpoved infrastrukture, učinki sevanja, tehnična okvara, škodljivo programje, tehnični napad, kršitev pravil, ogrožanje funkcij, ogrožanje informacij, škodljiva vsebina, drugo),
 - prizadetih sestavnih delih oziroma sredstvih,
 - negativnih poslovnih učinkih (nepooblaščen razkritje informacij, nepooblaščen sprememba, nerazpoložljivost, uničenje, drugo),
 - stroškov obnove po incidentu,
 - reševanju incidenta,
 - povzročiteljih incidenta in njihovih nagibih,
 - izvedenih aktivnostih za odpravo posledic incidenta,
 - nadaljnjih aktivnostih,
 - končni oceni incidenta in
 - subjektih, obveščenih o incidentu.
- (3) Evidenca incidentov informacijske varnosti se sproti posodablja.

21. člen (odziv na incidente in obvladovanje incidentov informacijske varnosti)

(1) Na incidente informacijske varnosti se odziva: najprej vodja informacijske varnosti organa oziroma koordinator informacijske varnosti, če ta odziv ni zadosten, ministrstvo, in če je potrebno, tudi drugi organi, pristojni za obravnavo incidentov.

(2) Odziv vključuje:

- omejitev škode in zagotovitev zahtevane ravni informacijske varnosti,
- zbiranje in zavarovanje dokazov čim prej po incidentu,
- odpravo posledic incidenta, ki lahko vključuje obnovo podatkov, informacijskih sistemov in poslovanja,
- zagotavljanje, da se vse odzivne aktivnosti ustrezno beležijo za poznejšo analizo,
- sporočanje obstoja incidenta informacijske varnosti ali kakršnih koli pomembnih podrobnosti o njem drugim notranjim ali zunanjim osebam ali organizacijam, ki morajo biti obveščene,
- proučitev pomanjkljivosti informacijske varnosti, ki so povzročile incident ali prispevale k njegovemu nastanku, in zmanjšanje ali odpravo tveganj, ki so bila povezana z incidentom, ter
- zaključevanje in arhiviranje incidenta, ko je bil uspešno razrešen.

PRILOGA2

PRAVILNIK O VARNOSTNI DOKUMENTACIJI IN VARNOSTNIH UKREPIH ORGANOV DRŽAVNE UPRAVE

8. člen (načrt odzivanja na incidente)

(1) Načrt odzivanja na incidente s protokolom obveščanja CSIRT organov državne uprave (v nadaljnjem besedilu: načrt odzivanja na incidente) obsega najmanj:

1. opis sistema za zaznavo incidentov informacijske varnosti,
2. opis sistema za zbiranje in zavarovanje dokazov o incidentu informacijske varnosti, vključno z dnevniškimi zapisi in revizijskimi sledmi, če te obstajajo,
3. opis postopkov za odziv, obravnavo in analizo incidentov informacijske varnosti, vključno z beleženjem vseh odzivnih aktivnosti,
4. opis odgovornosti oseb oziroma organizacijskih enot, ki jih je treba vključiti v aktivnosti iz prejšnje točke,
5. opis postopkov in odgovornosti za poročanje o incidentih znotraj ODU in izven ODU ter

6. opis protokola obveščanja o incidentu informacijske varnosti CSIRT organov državne uprave.

(2) Obvestilo iz 6. točke prejšnjega odstavka se pošlje CSIRT organov državne uprave na način, kot je objavljen na njegovi spletni strani in zajema najmanj:

1. oceno števila uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvenih storitev,
2. oceno trajanja incidenta,
3. oceno geografske razširjenosti, kar zadeva območje, na katerega incident vpliva,
4. oceno morebitnega medresorskega vpliva incidenta in
5. oceno pomembnosti vpliva incidenta na neprekinjeno izvajanje storitev ODU (lažji incident, težji incident, kritični incident).

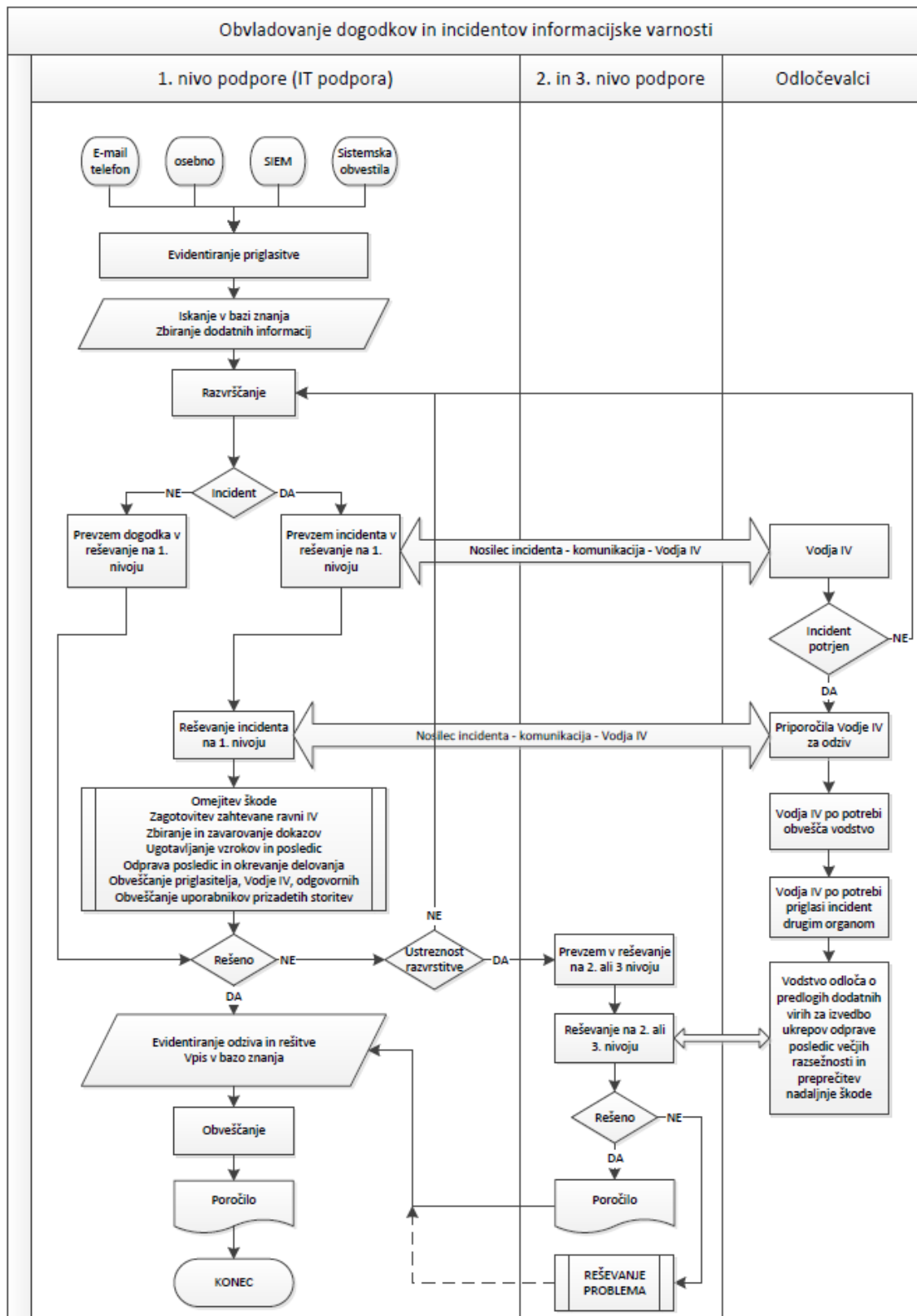
(3) Opis protokola obveščanja iz 6. točke prvega odstavka tega člena se lahko smiselno uporabi za obveščanje pristojnega nacionalnega organa za informacijsko varnost, če ima ODU lastne zmogljivosti vsaj na ravni varnostno operativnega centra.

PRILOGA3

Evidenca dogodkov in incidentov												
Referenčna številka	Datum priglavitve	Ura priglavitve	Vrsta dogodka	Vrsta incidenta grožnja	Vrsta incidenta teža	Priglasitelj Priimek Ime	Kratek Opis	Lokacija	Ocena obsega prizadetosti ogroženosti	Ocena škode	Pomembne informacije ob priglavitvi	

Obveščeni	Datum prevzema v reševanje	Ura prevzema v reševanje	Nosilec odziva	Opis aktivnosti odziva	Zavarovanje dokazov	Dejanski obseg	Dejanska škoda	Trajanje incidenta	Datum zaključitve odziva	Ura zaključitve odziva	Opomba

PRILOGA4



PRILOGA5

SPLOŠNA UREDBA O VARSTVU OSEBNIH PODATKOV (GDPR) **Oddelek 2 Varnost osebnih podatkov**

Člen 33

Uradno obvestilo nadzornemu organu o kršitvi varstva osebnih podatkov

1. V primeru kršitve varstva osebnih podatkov upravljavec brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvesti pristojni nadzorni organ v skladu s členom 55, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov. Kadar uradno obvestilo nadzornemu organu ni podano v 72 urah, se mu priloži navedbo razlogov za zamudo.
2. Obdelovalec po seznanitvi s kršitvijo varstva osebnih podatkov brez nepotrebnega odlašanja uradno obvesti upravljavca.
3. Uradno obvestilo iz odstavka 1 vsebuje vsaj:
 - (a) opis vrste kršitve varstva osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;
 - (b) sporočilo o imenu in kontaktnih podatkih pooblaščenih osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
 - (c) opis verjetnih posledic kršitve varstva osebnih podatkov;
 - (d) opis ukrepov, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.
4. Kadar in kolikor informacij ni mogoče zagotoviti istočasno, se informacije lahko zagotovijo postopoma brez nepotrebnega dodatnega odlašanja.
5. Upravljavec dokumentira vsako kršitev varstva osebnih podatkov, vključno z dejstvi v zvezi s kršitvijo varstva osebnih podatkov, njene učinke in sprejete popravne ukrepe. Ta dokumentacija nadzornemu organu omogoči, da preveri skladnost s tem členom.

Člen 34

Sporočilo posamezniku, na katerega se nanašajo osebni podatki, o kršitvi varstva osebnih podatkov

1. Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, upravljavec brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.
2. V sporočilo posamezniku, na katerega se nanašajo osebni podatki, iz odstavka 1 tega člena je v jasnem in preprostem jeziku opisana vrsta kršitve varstva osebnih podatkov ter so vsebovane vsaj informacije in ukrepe iz točk (b), (c) in (d) člena 33(3).

3. Sporočilo posamezniku, na katerega se nanašajo osebni podatki, iz odstavka 1 ni potrebno, če je izpolnjen kateri koli izmed naslednjih pogojev:

- (a) upravljavec je izvedel ustrezne tehnične in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za osebne podatke, v zvezi s katerimi je bila storjena kršitev varstva, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščen za dostop do njih, kot je šifriranje;
- (b) upravljavec je sprejel naknadne ukrepe za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz odstavka 1 verjetno ne bo več udejanjilo;
- (c) to bi zahtevalo nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

4. Če upravljavec posameznika, na katerega se nanašajo osebni podatki, še ni obvestil o kršitvi varstva osebnih podatkov, lahko nadzorni organ to od njega zahteva po preučitvi verjetnosti, da bi kršitev varstva osebnih podatkov povzročila veliko tveganje, ali pa lahko odloči, da je izpolnjen kateri koli od pogojev iz odstavka 3.