

PRILOGA: Razvrstitvena shema s poimenovanjem varnostnih razredov, merila za uvrščanje informacijskega premoženja in sistemov v posamezni varnostni razred ter postopki razvrščanja in označevanja

1. Namen

V tej prilogi je določena in opisana razvrstitvena shema s poimenovanjem varnostnih razredov, opisana so merila za uvrščanje informacijskega premoženja v posamezni varnostni razred ter postopki razvrščanja in označevanja. Varnostni razredi se uporabljajo skupaj z informacijami o ranljivostih in grožnjah pri ocenitvi tveganj za poslovanje organa in za uvedbo ustreznih nadzorstev.

2. Razvrščanje in označevanje informacijskega premoženja in informacijskih sistemov

Vsako informacijsko premoženje in informacijski sistem morata biti razvrščena v varnostni razred. Varnostni razredi se določijo glede na možni učinek, ki bi ga imel na organ dogodek, ki bi ogrozil informacijsko premoženje in informacijske sisteme, ki jih organ potrebuje za uresničevanje svojega poslanstva, varovanje svojega premoženja, izpolnjevanje zakonskih obveznosti, vzdrževanje rednega poslovanja in zaščito posameznikov.

3. Varnostni razredi in varnostni vidiki

Varnostni razredi se nanašajo na vse tri vidike informacijske varnosti: **zaupnost, celovitost in razpoložljivost**.

4. Določanje možnega učinka na organ in posameznike

Ta priloga določa tri ravni možnega učinka na organ ali posameznike v primeru ogrožanja ali izgube zaupnosti, celovitosti ali razpoložljivosti. Možni učinek je:

MAJHEN, če bi izguba zaupnosti, celovitosti ali razpoložljivosti lahko imela omejene negativne posledice za poslovanje organa, premoženje organa ali posameznike. **Omejene** negativne posledice pomenijo, da bi izguba zaupnosti, celovitosti in razpoložljivosti lahko:

- okrnila zmožnost opravljanja poslanstva v takem obsegu in trajanju, da bi organ sicer lahko izvajal svoje primarne funkcije, vendar bi bila učinkovitost teh funkcij zmanjšana;
- povzročila manjšo škodo premoženju organa (manj kot 100.000 eurov);
- povzročila manjšo finančno izgubo (manj kot 100.000 eurov);
- povzročila manjšo škodo posameznikom (ni potrebna zdravniška oskrba, manj kot dva dni izgube delovnega časa);
- povzročila manjšo škodo ugledu organa (posamične omembe v nekaterih tiskanih, elektronskih in spletnih medijih);

ZMEREN, če bi izguba zaupnosti, celovitosti ali razpoložljivosti lahko imela **resne** negativne posledice za poslovanje organa, premoženje organa ali posameznike. **Resne** negativne posledice pomenijo, da bi izguba zaupnosti, celovitosti in razpoložljivosti lahko:

- pomembno okrnila zmožnost opravljanja poslanstva v takem obsegu in trajanju, da bi organ sicer lahko izvajal svoje primarne funkcije, vendar bi bila učinkovitost teh funkcij znatno zmanjšana;
- povzročila znatno škodo premoženju organa (od 100.000 eurov do 500.000 eurov);
- povzročila znatno finančno izgubo (od 100.000 eurov do 500.000 eurov);
- povzročila znatno škodo posameznikom, ki pa ne vključuje izgube življenj ali resnih, smrtno nevarnih poškodb (potrebna zdravniška oskrba, do 30 dni izgube delovnega časa);
- povzročila znatno škodo ugledu organa (poročanje v medijih več dni zapored in/ali razprava v Državnem zboru);

VELIK, če bi izguba zaupnosti, celovitosti ali razpoložljivosti lahko imela **zelo resne ali katastrofalne** negativne posledice za poslovanje organa, premoženje organa ali posameznike. **Zelo resne ali katastrofalne** negativne posledice pomenijo, da bi izguba zaupnosti, celovitosti in razpoložljivosti lahko:

- močno okrnila zmožnost opravljanja poslanstva v takem obsegu in trajanju, da organ ne bi mogel izvajati ene ali več svojih primarnih funkcij;
- povzročila veliko škodo premoženju organa (nad 500.000 eurov);
- povzročila veliko finančno izgubo (nad 500.000 eurov);
- povzročila zelo resno ali katastrofalno škodo posameznikom, ki vključuje izgubo življenj ali resne, smrtno nevarne poškodbe (množične poškodbe in smrtne žrtve);
- povzročila veliko škodo ugledu organa (večtedensko poročanje v medijih in/ali razprava o ukrepih v Državnem zboru).

5. Varnostno razvrščanje informacijskega premoženja

Varnostni razred posameznega informacijskega premoženja je lahko povezan tako z uporabniškimi kot sistemskimi informacijami in se lahko nanaša na informacije v elektronski ali neelektronski obliki. Določitev ustreznega varnostnega razreda posameznega informacijskega premoženja zahteva določitev možnega učinka (na podlagi treh varnostnih vidikov), ki je povezan s tem informacijskim premoženjem.

Posplošeni zapis, s katerim izrazimo varnostni razred (VR) informacijskega premoženja (IP), je:

$$VR_{IP} = \{(zaupnost, u\check{c}inek_{IP}), (celovitost, u\check{c}inek_{IP}), (razpolo\check{z}ljivost, u\check{c}inek_{IP})\}$$

kjer so vrednosti za možni učinek lahko: MAJHEN, ZMEREN, VELIK ali SNU¹ (se ne uporablja).

6. Varnostno razvrščanje informacijskih sistemov

Za določitev varnostnega razreda informacijskega sistema je treba analizirati in upoštevati vse varnostne razrede informacijskih premoženj, ki se nahajajo v informacijskem sistemu. Vrednosti možnega učinka, dodeljene informacijskemu sistemu na podlagi vseh treh varnostnih vidikov (zaupnost, celovitost, razpoložljivost), morajo biti najvišje vrednosti varnostnih razredov, ki so bili določeni za vsako posamezno informacijsko premoženje, ki se nahaja v tem informacijskem sistemu.

¹ Za informacijsko premoženje, ki obsega javne informacije, se npr. možni učinek z vidika zaupnosti ne uporablja (SNU).

Posplošeni zapis, s katerim izrazimo varnostni razred (VR) informacijskega sistema (IS), je:

$$VR_{IS} = \{(zaupnost, u\check{c}inek_{max(IPI)}), (celovitost, u\check{c}inek_{max(IPI)}), (razpolo\check{z}ljivost, u\check{c}inek_{max(IPI)})\}$$

kjer so vrednosti za možni učinek lahko: MAJHEN, ZMEREN ali VELIK.

Pri določanju varnostnih razredov informacijskih sistemov vrednosti SNU ni mogoče dodeliti nobenemu varnostnemu vidiku, saj mora obstajati najmanj MAJHEN možni učinek ob izgubi zaupnosti, celovitosti in razpoložljivosti informacijskega sistema zaradi temeljne zahteve po varovanju sistemskih procesnih funkcij in ključnih informacij za delovanje informacijskega sistema.

7. Označevanje varnostnih razredov

Na podlagi določitve varnostnega razreda označimo posamezno informacijsko premoženje oziroma informacijski sistem, kot sledi:

Varnostni razred	Oznaka (kratka oznaka)	Varnostne zahteve
ZAUPNOST		
(zaupnost, MAJHEN)	Z: NOTRANJE (Z1)	Dostop omejen na uslužbenke organa
(zaupnost, ZMEREN)	Z: OMEJENO (Z2)	Dostop omejen na tiste uslužbenke organa, ki jih to zadeva
(zaupnost, VELIK)	Z: STROGO OMEJENO (Z3)	Dostop omejen na tiste prepoznane uslužbenke organa, ki to morajo vedeti
CELOVITOST		
(celovitost, MAJHEN)	C: UGOTOVLJIVA (C1)	Celovitost je lahko okrnjena, vendar je okrnjenost mogoče prepoznati
(celovitost, ZMEREN)	C: NADZOROVANA (C2)	Celovitost je lahko okrnjena, če je okrnjenost mogoče prepoznati in celovitost obnoviti
(celovitost, VELIK)	C: POPOLNA (C3)	Zahteva se popolna neokrnjenost
RAZPOLOŽLJIVOST		
(razpoložljivost, MAJHEN)	R: OBČASNA (R1)	Nerazpoložljivost več kot 24 ur
(razpoložljivost, ZMEREN)	R: PRETEŽNA (R2)	Nerazpoložljivost največ 24 ur
(razpoložljivost, VELIK)	R: STALNA (R3)	Razpoložljivost brez prekinitev

Oznaka odraža tudi varnostne zahteve za posamezni varnostni razred glede na posamezne vidike informacijske varnosti.

8. Pregled opredelitev možnih učinkov

V spodnji tabeli so povzete opredelitve možnih učinkov za vsak varnostni vidik: zaupnost, celovitost in razpoložljivost.

MOŽNI UČINEK			
Varnostni vidik	MAJHEN	ZMEREN	VELIK
Zaupnost – lastnost, da informacije niso razpoložljive ali razkrite nepooblaščenim posameznikom, entitetam ali procesom.	Nepooblaščen razkritje informacij ima lahko omejene negativne učinke na poslovanje organa, premoženje organa ali posameznike. Z: NOTRANJE (Z1)	Nepooblaščen razkritje informacij ima lahko resne negativne učinke na poslovanje organa, premoženje organa ali posameznike. Z: OMEJENO (Z2)	Nepooblaščen razkritje informacij ima lahko zelo resne ali katastrofalne negativne učinke na poslovanje organa, premoženje organa ali posameznike. Z: STROGO OMEJENO (Z3)

Celovitost – lastnost informacij in informacijskih sistemov, da so točni in popolni.	Nepooblaščen sprememba ali uničenje informacij in informacijskih sistemov ima lahko omejene negativne učinke na poslovanje organa, premoženje organa ali posameznike. C: UGOTOVLJIVA (C1)	Nepooblaščen sprememba ali uničenje informacij in informacijskih sistemov ima lahko resne negativne učinke na poslovanje organa, premoženje organa ali posameznike. C: NADZOROVANA (C2)	Nepooblaščen sprememba ali uničenje informacij in informacijskih sistemov ima lahko zelo resne ali katastrofalne negativne učinke na poslovanje organa, premoženje organa ali posameznike. C: POPOLNA (C3)
Razpoložljivost – lastnost informacij in informacijskih sistemov, da so dostopni in uporabni na zahtevo pooblaščen entitete.	Motnje ali prekinitve dostopa do informacij ali uporabe informacijskega sistema ima lahko omejene negativne učinke na poslovanje organa, premoženje organa ali posameznike. R: OBČASNA (R1)	Motnje ali prekinitve dostopa do informacij ali uporabe informacijskega sistema ima lahko resne negativne učinke na poslovanje organa, premoženje organa ali posameznike. R: PRETEŽNA (R2)	Motnje ali prekinitve dostopa do informacij ali uporabe informacijskega sistema ima lahko zelo resne ali katastrofalne negativne učinke na poslovanje organa, premoženje organa ali posameznike. R: STALNA (R3)