PRILOGA 1

PROGRAM USPOSABLJANJA

1 Uvod v informacijsko in kibernetsko varnost, zakonodaja, predpisi in mednarodni standardi

- Osnovni izrazi in opredelitve: Razumevanje temeljnih izrazov in konceptov informacijske in kibernetske varnosti.
- Pregled trenutnih groženj in trendov: Pregled in analiza aktualnih groženj in trendov v informacijski in kibernetski varnosti.
- Notranja zakonodaja: Pregled ustrezne zakonodaje, ZInfV-1 in predpisi, izdani na njegovi podlagi.
- Evropski predpisi: Pregled evropskih predpisov, ki veljajo za posamezne sektorje in zavezance: uredbe, izvedbene uredbe, drugi akti.
- Mednarodni standardi: Pregled mednarodnih standardov in dobrih praks, kot so NIST CSF, ISO/IEC 27001, COBIT, ISO/IEC 22301.

2 Upravljanje sredstev in tveganj

- Prepoznavanje in popis sredstev: Prepoznavanje in razvrstitev informacijskih sredstev oziroma virov ter njihov popis.
- Prepoznavanje tveganj: Metode za prepoznavanje varnostnih tveganj.
- Ocena tveganj: Tehnike za ocenjevanje tveganj in določanje njihovega vpliva.
- Obvladovanje tveganj: Razvoj in uveljavitev strategij za obvladovanje tveganj.

3 Ocena vplivov na poslovanje in neprekinjeno poslovanje

- Ocena vplivov na poslovanje (BIA): Metode za ocenjevanje vplivov varnostnih incidentov na poslovanje.
- Načrti za neprekinjeno poslovanje (BCP): Priprava politike in načrta za zagotavljanje neprekinjenega poslovanja v primeru incidentov.

4 Odzivanje na incidente informacijske varnosti

- Praktičen prikaz incidenta informacijske varnosti: Prikaz pojava incidenta v omrežju in informacijskih sistemih ter odziva nanj in njegovih posledic.
- Odzivanje in sanacija: Postopki za učinkovito odzivanje na incidente in njihovo sanacijo.

5 Varnost dobavnih verig

- Prepoznavanje tveganj in ukrepi za zaščito dobavne verige: Prepoznavanje in ocenjevanje tveganj, povezanih z dobavnimi verigami, uveljavitev varnostih ukrepov za zaščito pred tveganji informacijske in kibernetske varnosti ter izvajanje nadzorstva nad ključnimi dobavitelji.
- Najmanjše potrebne zahteve vsebine pogodb za pogodbene partnerje za področje informacijske varnosti: Varnostni ukrepi, ukrepi za neprekinjeno poslovanje, obveščanje o incidentih, ravnanje s podatki in možnost preverjanja izvajanja varnostne klavzule.

6 Izvajanje dolžnega nadzorstva in pogoste ugotovitve neskladja s predpisi iz inšpekcijskih nadzorov

- Seznanitev z izvajanjem dolžnega nadzorstva: Razvoj sposobnosti in postopkov za izvajanje dolžnega nadzorstva nad varnostnimi ukrepi in postopki.
- Seznanitev s pogostimi ugotovitvami neskladij s predpisi, ki so bili ugotovljeni v inšpekcijskih nadzorih in podanih priporočilih za izboljšanje varnosti ali učinkovitosti.