Priloga 8: Kibernetska varnost

1. Upravljavec ali investitor sevalnega ali jedrskega objekta mora v skladu z zahtevami iz te priloge zagotoviti, da so digitalni računalniški in komunikacijski sistemi ter mreže ustrezno zaščitene pred kibernetskimi napadi, v skladu z oceno ogroženosti.
2. Upravljavec ali investitor mora zaščititi digitalne računalniške in komunikacijske sisteme in omrežja, povezane z:
   a) varnostnimi funkcijami in funkcijami, pomembnimi za jedrsko in sevalno varnost,
   b) funkcijami v povezavi z jedrskim varovanjem,
   c) nalogami v zvezi s pripravljenostjo na izredni dogodek, vključno z oddaljenimi komunikacijami, in
   d) podpornimi sistemi in opremo, ki bi lahko, če so ogroženi, negativno vplivali na jedrsko in sevalno varnost, jedrsko varovanje, nadzor nad jedrskimi snovmi ali pripravljenost na izredni dogodek.
3. Upravljavec ali investitor mora zavarovati sisteme in omrežja, opredeljene v točki 2 te priloge, pred kibernetskimi napadi, ki bi:
   a) negativno vplivali na celovitost ali zaupnost podatkov in/ali programske opreme,
   b) preprečili dostop do sistemov, storitev in/ali podatkov ter
   c) negativno vplivali na delovanje sistemov, omrežij in pripadajoče opreme.
4. Da bi izpolnili zahteve iz zgornjih točk te priloge, mora upravljavec ali investitor:
   a) analizirati digitalne računalniške in komunikacijske sisteme in omrežja ter opredeliti sredstva, ki morajo biti zaščitena pred kibernetskimi napadi, da zadosti zahtevam iz zgornjih točk tega poglavja in
   b) vzpostaviti, izvajati in vzdrževati program kibernetske varnosti za zaščito sredstev, opredeljenih v točki 4.a te priloge.
5. Program kibernetske varnosti mora biti zasnovan tako, da se:
   a) varnostne kontrole izvajajo tako, da se sredstva, opisana v točki 4.a te priloge, zavarujejo pred kibernetskimi napadi,
   b) uporablja in vzdržuje strategije obrambe v globino za zagotavljanje odkrivanja, odzivanja in odgovarjanja na kibernetske napade,
   c) ublaži škodljiv vpliv kibernetskih napadov in da se
   d) zagotovi, da zaradi kibernetskih napadov ni negativnih vplivov na funkcije pomembnih sredstev, opredeljenih v točki 4.a te priloge.
6. Kot del programa kibernetske varnosti upravljavec ali investitor:
   a) zagotovi seznanjenost osebja in zunanjih izvajalcev z računalniškimi varnostnimi zahtevami ter ustrezno usposabljanje, ki je potrebno za opravljanje dodeljenih nalog in odgovornosti;
   b) ovrednoti in upravlja kibernetska tveganja;
   c) zagotovi, da so kakršnekoli spremembe sredstev, opisane v točki 4.a te priloge, predhodno ovrednotene tako, da se cilji uspešnosti za kibernetsko varnost, opisani v 2. točki te priloge, lahko dosežejo.
7. Program kibernetske varnosti mora opisovati, kako se bodo zahteve iz te priloge izvajale, hkrati pa mora upoštevati posebnosti določenega objekta, ki vplivajo na izvajanje.
8. Program kibernetske varnosti mora vsebovati ukrepe v primeru izrednega kibernetskega dogodka in povrnitev v normalno stanje po kibernetskem napadu. Program kibernetske varnosti mora opisati, kako upravljavec ali investitor:
   a) ohrani sposobnost za pravočasno odkrivanje in odzivanje na kibernetske napade,

b) ovrednoti kibernetske napade,
c) ublaži posledice kibernetskega napada,
d) odpravi izkoriščene ranljivosti in
e) obnovi prizadete sisteme, omrežja oziroma opremo, ki jih je prizadel kibernetski napad.

9. Upravljavec ali investitor mora obvestiti pristojen organ za jedrsko varnost o kibernetskem napadu, ki se nanaša na digitalne računalniške in komunikacijske sisteme in omrežja opredeljene v točki 2. te priloge najkasneje v 24 urah od zaznave dogodka.

10. Upravljavec ali investitor mora vzpostaviti in vzdrževati pisne postopke za izvajanje programa kibernetske varnosti.