Naša opredijeljenost

Brodogradilište Viktor Lenac d.d. upravlja informacijskom i kibernetičkom sigurnošću kao sastavnim dijelom poslovanja, upravljanja rizicima i kontinuiteta poslovanja. Cilj je zaštititi informacije, poslovne procese, mrežne i informacijske sustave, digitalne usluge i povezanu imovinu te očuvati njihovu povjerljivost, cjelovitost, raspoloživost i autentičnost.

Uprava osigurava vodstvo, odgovornosti i potrebne resurse, odobrava ovu Politiku te se obvezuje ispunjavati primjenjive zakonske, regulatorne, ugovorne i normativne zahtjeve i kontinuirano poboljšavati sustav upravljanja informacijskom sigurnošću (ISMS).

Na koga se Politika primjenjuje

Politika se primjenjuje na sve zaposlenike, članove Uprave, rukovoditelje, vanjske suradnike, dobavljače, podizvođače, pružatelje IKT usluga i druge osobe koje pristupaju informacijama, sustavima, prostorima ili digitalnim uslugama Društva. Zahtjevi se primjenjuju razmjerno riziku, kritičnosti imovine, poslovnim potrebama i obvezama Društva.

Načela i ciljevi sigurnosti

- Upravljanje temeljeno na riziku: prijetnje, ranjivosti i utjecaji sustavno se identificiraju, procjenjuju, obrađuju i prate.
- Ugrađena i zadana sigurnost: sigurnosni zahtjevi uključuju se u planiranje, nabavu, razvoj, promjene, uporabu i održavanje sustava.
- Najmanja privilegija i razdvajanje dužnosti: pristup se dodjeljuje prema poslovnoj potrebi, u najmanjem potrebnom opsegu i uz odgovarajuća odobrenja.
- Zaštita tijekom cijelog životnog ciklusa: informacijama, podacima, uređajima, aplikacijama, mrežama i fizičkim prostorima upravlja se od nastanka ili nabave do sigurnog brisanja ili zbrinjavanja.
- Otpornost i kontinuitet: održavaju se i testiraju sigurnosne kopije, planovi odgovora, kontinuiteta poslovanja i oporavka.
- Pravodobno postupanje s incidentima: događaji i incidenti otkrivaju se, prijavljuju, evidentiraju, analiziraju, ograničavaju i rješavaju, uz obavještavanje nadležnih tijela i pogođenih dionika kada je primjenjivo.
- Sigurnost lanca opskrbe: sigurnosni zahtjevi ugovaraju se i nadziru kod relevantnih dobavljača i pružatelja usluga.
- Svijest i kompetencije: zaposlenici, Uprava i relevantni partneri osposobljavaju se prema svojim ulogama i izloženosti riziku.
- Mjerenje i poboljšavanje: djelotvornost mjera provjerava se metrikama, auditima, samoprocjenama, testiranjima, analizom incidenata i korektivnim mjerama.

Područja upravljanja

Društvo uspostavlja i održava tehničke, organizacijske i operativne mjere, razmjerne identificiranim rizicima, u sljedećim područjima:

upravljanje rizicima i informacijskom imovinom; klasifikacija i zaštita podataka; identiteti, autentikacija i prava pristupa; fizička sigurnost; mrežna sigurnost i sigurne konfiguracije; upravljanje ranjivostima, zakrpama i promjenama; zaštita od zlonamjernog sadržaja; kriptografija; sigurnosno praćenje i dnevnički zapisi; sigurnost nabave, razvoja i održavanja; sigurnosne kopije, kontinuitet i oporavak; upravljanje incidentima i krizna komunikacija; sigurnost dobavljača i lanca opskrbe; upravljanje ljudskim resursima; edukacija i kibernetička higijena.

Uloge i zajednička odgovornost

Uprava snosi konačnu odgovornost za upravljanje kibernetičkim sigurnosnim rizicima, odobrava mjere, nadzire njihovu provedbu i osigurava resurse. Predstavnik Uprave za informacijsku i kibernetičku sigurnost odgovoran je za ISMS, upravljanje rizicima, incidentima, usklađenošću, izvještavanjem i poboljšavanjem. Vlasnici procesa i imovine određuju poslovne i sigurnosne zahtjeve, a ICT i druge nadležne funkcije provode i nadziru odgovarajuće kontrole.

Svaki korisnik dužan je štititi dodijeljene informacije i imovinu, koristiti samo odobrene sustave i postupke, čuvati vjerodajnice, sudjelovati u obveznim edukacijama te bez odgode prijaviti sumnjiv događaj, ranjivost ili incident. Dobavljači i druge treće strane dužni su poštivati ugovorene sigurnosne zahtjeve i surađivati u upravljanju incidentima i rizicima.

Prijava sigurnosnih događaja

Sumnjivi događaji, incidenti i ranjivosti prijavljuju se bez odgode.

Usklađenost, praćenje i pregled

Politika podržava zahtjeve norme ISO/IEC 27001:2022, osobito vodstvo i opredijeljenost, politiku informacijske sigurnosti, uloge i odgovornosti, ciljeve, komunikaciju, upravljanje dokumentiranim informacijama, vrednovanje djelotvornosti i kontinuirano poboljšavanje. Istodobno daje javni strateški okvir za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima prema Zakonu o kibernetičkoj sigurnosti (NN 14/24) i Uredbi o kibernetičkoj sigurnosti (NN 135/24).

Djelotvornost Politike i povezanih mjera najmanje se jednom godišnje procjenjuje i izvještava Upravu. Politika se pregledava najmanje jednom godišnje te nakon značajnih incidenata, regulatornih, tehnoloških, organizacijskih ili drugih relevantnih promjena. Detaljna pravila, procedure, planovi, registri i tehničke konfiguracije uređuju se internom dokumentacijom i ne objavljuju se kada bi objava mogla ugroziti sigurnost.

Završna izjava Uprave

Zaštita informacija i kibernetička otpornost zajednička su odgovornost. Uprava očekuje dosljednu primjenu ove Politike i podupire otvorenu prijavu rizika, incidenata i prijedloga za poboljšanje. Nepridržavanje zahtjeva može rezultirati odgovarajućim disciplinskim, ugovornim, tehničkim ili drugim mjerama u skladu s primjenjivim propisima i internim aktima.

Ovaj dokument vrijedi od datuma donošenja.

Predsjednik Uprave

Luka Hrboka

BRODOGRADILIŠTE VIKTOR LENAC d.d. 1946 Kostrena, Martinscica 8