POLITIKA INFORMACIJSKE SIGURNOSTI

1 Uvod

Organizacija NTH Mobile d.o.o. (u nastavku: **NTH**) je centar za razvoj i održavanje tehnoloških rješenja i servisa međunarodne organizacije NTH Group (u nastavku: **Grupa**), koja svojim klijentima pruža niže navedene usluge:

- **više-kanalna razmjena poruka** (eng. multi-channel messaging),
- **mobilno plaćanje** (eng. mobile payment service).

NTH razumije svoju ulogu u obradi podataka, stoga teži najvišim standardima u informacijskoj sigurnosti i privatnosti podataka. Uprava NTH prepoznala je informacijsku sigurnost i privatnost kao jedno od ključnih upravljačkih načela, važnih za ispunjavanje svojih glavnih strateških ciljeva, osiguravanje konkurentske prednosti na tržištu kao i izgradnju i održavanje povjerenja sa svojim kupcima i poslovnim partnerima.

Kako bi osigurao jedinstveni, sveobuhvatan i odgovoran pristup informacijskoj sigurnosti, NTH je uspostavio sustav upravljanja informacijskom sigurnošću (u nastavku: **ISMS**) zasnovan na međunarodnoj normi ISO 27001:2013.

Glavni cilj uspostavljenog ISMS-a je spriječiti gubitak, krađu ili oštećenje podataka, osigurati kontinuitet poslovanja i poštivanje svih važećih zakona i propisa.

Politika informacijske sigurnosti navedena u ovom dokumentu je ključni dokument, koji je odobrila uprava NTH, a koji definira glavna načela i ciljeve ISMS-a organizacije i pokazuje predanost uprave informacijskoj sigurnosti i privatnosti. To je ključni dokument koji se koristi kao osnova za sve ostale aktivnosti informacijske sigurnosti unutar NTH.
Uprava NTH će osigurati sve potrebne resurse potrebne za učinkovitu provedbu ove politike.

2 Svrha

NTH donosi ovu Politiku informacijske sigurnosti (u nastavku: **Politika**) kao krovni dokument sustava upravljanja informacijskom sigurnošću u svrhu:

- utvrđivanja obveze odgovornog upravljanja informacijskom sigurnošću kao sastavnog dijela svojeg poslovanja
- uspostavljanja okvira za upravljanje sigurnošću informacijskog sustava
- smanjivanja mogućnosti gubitka podataka i prekida u poslovanju,
- smanjivanja mogućnosti gubitka povjerenja kod svojih partnera, kupaca, i krajnjih korisnika,
- smanjivanja mogućnosti financijskih gubitaka koji mogu nastati kao izravna ili neizravna posljedica incidenta,
- smanjivanja mogućnosti gubitka tržišne pozicije Društva.

3 Ciljevi informacijske sigurnosti

Osnovni ciljevi sustava upravljanja informacijskom sigurnošću NTH su:

- osiguravanje povjerljivosti, integriteta i raspoloživosti informacijskog sustava i podataka koji se u njemu obrađuju, u skladu s organizacijskim i sigurnosnim zahtjevima te procjenom rizika. Poseban naglasak stavlja se na zaštitu osobnih podataka te sredstava za elektronička plaćanja,
- uspostava, nadzor i kontinuirano unaprjeđenje ključnih procesa vezanih uz upravljanje informacijskom sigurnošću,
- uspostava pouzdanog sustava izvješćivanja kao temelja za pravovremeno i kvalitetno donošenje odluka vezanih uz informacijsku sigurnost,
- usklađivanje poslovanja sa zakonskom regulativom te regulatornim i ugovornim obvezama.

Postavljeni ciljevi ostvaruju se kroz:

- uspostavu odgovarajućih procesa, uloga i odgovornosti,
- uspostavu i redovito održavanje internih akata vezanih uz informacijsku sigurnost,
- implementaciju tehničkih i organizacijskih mjera usklađenih s rezultatima procjene rizika, ugovornim obvezama, primjenjivim regulatornim i zakonodavnim okvirima te dobrim praksama,
- redovitu edukaciju i sigurnosno osvješćivanje zaposlenika,
- osiguravanjem potrebnih ljudskih, financijskih i drugih materijalnih i nematerijalnih resursa.

Za ostvarivanje ciljeva informacijske sigurnosti definiranih ovom Politikom odgovorna je Uprava.

4 Opseg

Pravila definirana ovom Politikom i povezanim dokumentima, koji detaljiziraju pojedina pravila, uloge i postupke, odnose se na NTH procese

razvoja, upravljanja, i tehničke podrške za pružanje usluga više-kanalne razmjene poruka i mobilnog platnog sustava.

Unutar gore navedenih procesa, područje primjene ove Politike obuhvaća:

- sklopovsku imovinu u vlasništvu NTH ili koje NTH koristi u najmu,
- programsku imovinu koju korisnici (zaposlenici NTH ili treće strane) koriste u svom radu,
- ako korisnici koriste vlastite uređaje (npr. mobilni telefon, laptop, i sl.) za pristup podacima iz informacijskog sustava NTH, pravila se primjenjuju i na te uređaje,
- na sve mrežne servise i infrastrukturu koju NTH koristi (bilo u svom vlasništvu ili u najmu).

Ovu Politiku su dužni su poštovati i provoditi svi korisnici informacijskog sustava NTH odnosno:

- odnosno zaposlenici NTH,
- treće strane koji koriste informacijski sustav NTH ili obavljaju ugovorene poslove za NTH.

5 Osnovna načela sustava upravljanja informacijskom sigurnošću

Osnovna načela sustava upravljanja informacijskom sigurnošću su opisana u nastavku:

- Informacijska sigurnost za NTH predstavlja važan dio u cjelokupnom upravljanju tvrtke kao i sastavni dio svih poslovnih aktivnosti.
- S ciljem efikasnog i odgovornog upravljanja informacijskom sigurnošću, NTH je uspostavila sustav upravljanja informacijskom sigurnošću usklađen sa sigurnosnim i poslovnim zahtjevima Društva, primjenjivim zakonskim i regulatornim okvirima te najboljim praksama na području informacijske sigurnosti.
- U okviru sustava upravljanja informacijskom sigurnošću, NTH je uspostavila ključne uloge i odgovornosti za informacijsku sigurnost, uključujući i ulogu Voditelja informacijske sigurnosti.
- Sustav upravljanja informacijskom sigurnošću temelji se na procesu upravljanja rizikom. Procjena rizika provodi se minimalno jednom godišnje ili nakon značajnijih promjena na dijelu informacijskog sustava NTH unutar ISMS opsega. Uprava je dužna usvojiti rezultate procjene rizika te osigurati provođenje mjera koje će identificirane rizike umanjiti na prihvatljivu razinu.
- S ciljem kvalitetnijeg upravljanja i kontinuiranog unaprjeđenja sustava upravljanja informacijskom sigurnošću, Direktor Društva je dužan uspostaviti proces neovisnog nadzora informacijskog sustava Društva koji će se provoditi minimalno jednom godišnje.
- Uprava NTH dužna je uspostaviti proces upravljanja incidentima s pripadajućim ulogama i odgovornostima koji će omogućiti pravovremenu detekciju i sprječavanje incidenata na informacijskom sustavu, umanjivanje njihovog štetnog utjecaja te pravovremeno i potpuno izvješćivanje svih zainteresiranih strana.
- Uprava NTH dužna je osigurati adekvatnu edukaciju zaposlenika kao i redovito provođenje programa podizanja svijesti o informacijskoj sigurnosti.
- Svi korisnici informacijskog sustava NTH aktivni su sudionici procesa upravljanja informacijskom sigurnošću.
- Od svih korisnika informacijskog sustava NTH očekuje se razumijevanje i prihvaćanje osobne odgovornosti za zaštitu informacijskih resursa Društva kroz aktivnu primjenu i poštivanje Politike informacijske sigurnosti i drugih povezanih internih akata.
- Korisnici informacijskog sustava dužni su aktivno sudjelovati u poboljšanju razine sigurnosti informacijskog sustava NTH, uočavanjem i prijavom potencijalnih sigurnosnih problema i incidenata.
- Kroz proces upravljanja informacijskom sigurnošću, NTH osigurava povjerljivost, integritet i raspoloživost ključnih poslovnih informacija i servisa.
- Uprava NTH dužna je osigurati adekvatno upravljanje eksternaliziranim procesima uključujući upravljanje rizicima eksternalizacije, upravljanje neželjenim događajima, te učinkovito upravljanje rizicima povezanim s ugovorenim eksternalizacijama.
- Sve eksternalizacije poslovnih procesa ili dijela poslovnih procesa moraju biti predmetom pisanog ugovora uključujući osiguranje kvalitete i obvezu pružatelja usluge da štiti povjerljivost svih informacija.

- Sve aktivnosti Društva koje na direktan odnosno indirektan način mogu utjecati na informacijsku sigurnost moraju biti organizirane, koordinirane, upravljanje i nadzirane od strane odgovornih osoba.
- NTH je dužno poseban naglasak staviti na eksternalizaciju poslovnih procesa ili dijela poslovnih procesa koji uključuju korištenje usluga u oblaku tj. cloud rješenja. Pri tome uzimajući u obzir kritičnost i inherentni rizik predmeta eksternalizacije, direktni utjecaj prekida eksternalizirane usluge, povezane pravne i reputacijske rizike, financijski utjecaj prekida eksternalizirane usluge, potencijalni utjecaj narušavanja povjerljivosti i cjelovitosti informacija na klijente Društva i na samo NTH.

6 Završne odredbe

Ovaj Politika stupa na snagu i primjenjuje se s danom donošenja.

Svi zaposlenici NTH dužni su se pridržavati ove Politike. Nepridržavanje bilo koje odredbe iz ovog Politike od strane zaposlenika smatrati će se povredom ugovora o radu koja može predstavljati razlog za otkaz ugovora o radu.

Nepridržavanje odredbi ovog Politike od trećih strana smatra se povredom ugovornih obveza koja može biti razlog za raskid ugovora.

Obvezu pridržavanja odredbi Politike sigurnosti informacijskog sustava te svih sigurnosnih pravilnika i procedura koje proizlaze iz ove Politike imaju svi korisnici informacijskog sustava NTH, zaposlenici, sve osobe koje privremeno obavljaju poslove prema ugovoru te svi vanjski suradnici ili partneri/kupci Društva koji dolaze u doticaj sa resursima informacijskog sustava.

U slučaju nastanka štete zbog nepoštivanje pravila iz ovog pravilnika, NTH zadržava pravo nadoknadu nastale štete.