1. Uvod

Politika upravljana informacijskom sigurnošću proizlazi iz strategije razvoja i strategije upravljanja rizicima, usklađena je s poslovnom politikom i poslovnim ciljevima, te predstavlja najvišu razinu dokumentacije vezane za informacijsku sigurnost.

Svi zaposlenici dužni su, u okviru svojih ovlasti i nadležnosti, postupati u skladu s odredbama ove Politike.

2. Namjena i područje primjene

Svrha donošenja ove Politike je podizanje razine znanja i svijesti svih korisnika o značaju uspostave funkcionalnog i sigurnog informacijskog sustava organizacije.

Politikom sigurnosti IS definiraju se načela i osnovni principi, te odgovornosti koje se odnose na upravljanje resursima IS radi uspostavljanja adekvatne razine informacijske sigurnosti u cilju osiguranja:

- nesmetanog, odnosno kontinuiranog odvijanja poslovnih procesa
- povjerenja zaposlenika, poslovnih partnera i klijenata
- konkurentnosti i ugleda organizacije.

Siguran informacijski sustav zasniva se na sljedećim temeljnim načelima:

- Povjerljivost – svojstvo da informacije ne budu dostupne ili otkrivene neovlaštenim subjektima
- Integritet – svojstvo da informacije i procesi nisu neovlašteno ili nepredviđeno mijenjani
- Raspoloživost – svojstvo koje omogućuje pristup i upotrebljivost na zahtjev od strane ovlaštenog subjekta

Uprava organizacije usvaja strategiju razvoja informacijskog sustava i nadzire njeno provođenje, uspostavlja adekvatnu organizacijsku i funkcionalnu strukturu prema kojoj delegira ovlasti i odgovornosti, uspostavlja proces upravljanja rizikom informacijskog sustava, definira načine izvještavanja, te donosi interne akte kojima se regulira upravljanje i razvoj IS.

Sustav upravljanja informacijskom sigurnošću primjenjuje se na sve identificirane poslovne procese kao što je definirano u opsegu sustava upravljanja.

Sukladno usvojenoj organizacijskoj strukturi i posebnim odlukama, Uprava organizacije imenuje:
- voditelja informacijske sigurnosti (VIS), i
- grupu za sistemsku administraciju (GSA).

Interni audit provodi stalni nadzor efikasnosti sustava internih kontrola, utemeljen na procjeni rizika informacijskog sustava, pravodobno izvještava o izostanku internih kontrola, daje preporuke za poboljšanje, te prati učinak njihove implementacije. Unutarnja revizija uključena je u sve aktivnosti koje mogu imati utjecaj na funkcionalnost i sigurnost informacijskog sustava organizacije.

3. Politika

Organizacija je usvojila sljedeću dokumentacijsku strukturu:

- Politika informacijske sigurnosti (ovaj dokument)
- Priručnik integriranog sustava upravljanja (ISO 9001, ISO 14001 & ISO 27001)
- Opis pojedinih poslovnih procesa
- Politike koje tretiraju pojedine oblasti informacijske sigurnosti
- Procedure sustava upravljanja
- Evidencije i predlošci zapisa.

Politika informacijske sigurnosti kao najviša razina dokumentacije definira temeljne odrednice za uspostavu sigurnog i efikasnog informacijskog sustava.

Politike detaljno opisuju mjere i pravila čijom primjenom se osigurava uspostava zadovoljavajuće razine informacijske sigurnosti.

Procedure sustava upravljanja sadrže konkretne opise implementiranja i korištenja mjera i pravila u okviru pojedinih poslovnih procesa.

Svrha politike zaštite informacija je sigurnost informacijskih sredstava poduzeća od svih vrsta prijetnji, bilo unutarnjih ili vanjskih, namjernih ili nenamjernih. Sigurnost informacijskih sustava je ključna za preživljavanje i razvoj poduzeća zato ju podupire i odobrava Uprava.

Primjena Politike informacijske sigurnosti poduzeća mora osigurati:

- Klasifikaciju informacijskih sredstava obzirom na razinu upotrebe.
- Kontinuiranu procjenu i upravljanje rizicima informacijske sigurnosti na način da na rizike procijenjene kao visoke primijeni mjere koje će ih spustiti minimalno na srednju razinu rizika, u konačnici na nisku razinu rizika. Samo iznimno Uprava će prihvatiti preostale rizike.
- Zaštitu informacija od neovlaštenog pristupa.
- Povjerljivost informacija.
- Integritet (neokrnjenost) informacija.
- Poštivanje sigurnosnih zahtjeva u vezi s osobljem.
- Upravljanje fizičkom sigurnošću, te sigurnošću ukupnog okružja, uključujući i sigurnost komunikacija.
- Poštivanje zakonskih, regulatorskih i ugovornih zahtjeva.
- Primjenu metodologije životnog ciklusa sustava pri njegovom razvoju i održavanju.
- Razvoj, održavanje i ispitivanje planova za osiguranje neprekinutog poslovanja.
- Izvođenje osvještavanja iz područja sigurnosti informacija za sve zaposlenike poduzeća.
- Upravljanje incidentima (otkrivanje, istraživanje, izvještavanje) u zaštiti informacija.
- Sankcioniranje kršenja ove Politike informacijske sigurnosti.

Uprava, odnosno njeni imenovani predstavnici, preuzimaju odgovornost za:

- Izradu politika i procedura (postupaka) temeljem najbolje poznate prakse kao mjera za potporu izvođenja ove Politike informacijske sigurnosti. Politike i procedure će, između ostalog, obuhvaćati i zaštitu od računalnih virusa, upravljanje zaporkama, te backup podataka i restauriranje sustava nakon katastrofe.

- Raspoloživost informacija i informacijskih sustava koji će ispunjavati zahtjeve koji proizlaze iz zahtjeva poslovanja poduzeća.

U vezi sa zaštitom informacija određene su uloge i odgovornosti za:

- Rukovodstvo poduzeća
- Stručnjake za informacijsku sigurnost
- Vlasnike podataka
- Vlasnike procesa
- Dobavljače tehnologija
- Korisnike
- Revizore informacijskih sustava

Grupa za sistemsku administraciju (GSA) je neposredno odgovorna za održavanje ove Politike i pripremu smjernica i savjeta za njeno izvođenje i usavršavanje.

Svi rukovoditelji su neposredno odgovorni za provođenje ove Politike na područjima za koja su odgovorni, te za poštivanje njezinih odredbi od strane podređenih.

4. Poštivanje politike

Grupa za sistemsku administraciju (GSA) periodično revidira i ažurira ovu Politiku u skladu s promjenama u informacijskom sustavu organizacije i njegovoj okolini, u slučajevima narušavanja sigurnosti, te ovisno o rezultatima procjene rizika i/ili revizije informacijskog sustava.

Za kršenje ove politike primjenjuju se disciplinske mjere propisane Pravilnikom o radu, Ugovorom o radu i Izjavama o čuvanju tajnosti.

	Ime i prezime:	Funkcija:	Datum:	Potpis:
Odobrio:	Igor Begović	Direktor	2017-10-20	