IKOM Industrija komunalne opreme i mjerila, dioničko društvo, OIB: 86247075815, Kovinska ulica 7, Zagreb (dalje: Društvo), dana 15.01.2024.donosi

POLITIKU INFORMACIJSKE SIGURNOSTI

1. Svrha

1.1. Politika informacijske sigurnosti predstavlja opća pravila i postupke za upravljanje sustavom informacijske sigurnosti i za održavanje, zaštitu i upravljanje informacijama kako bi se osigurala njihova povjerljivost, integritet i dostupnost.

1.2. Sustav upravljanja informacijskom sigurnosti uspostavlja se u svrhu zaštite informacija od prijetnji kojima se narušava njihova povjerljivost, integritet i/ili dostupnost radi osiguranja kontinuiteta poslovanja, smanjenja poslovnog rizika i povećanja prihoda od poslovnih prilika.

1.3. Društvo u svrhu sprječavanja narušavanja povjerljivosti, integriteta i dostupnosti uređuje postupke zaštite informacije i podataka koji se stvaraju, preuzimaju, obrađuju, spremaju ili prosljeđuju resursima informacijskog sustava Društva, uzimajući u obzir relevatne zakonske, regulatorne i ugovorne obveze.

2. Područje primjene

2.1. Ova Politika se primjenjuje na sve informacije unutar Društva i na sve korisnike informacijskog sustava Društva, odnosno radnike, suradnike, vanjske partnere i druge strane koje na bilo koji način dolaze u doticaj s resursima informacijskog sustava Društva.

3. Resursi informacijskog sustava

3.1. Informacijski sustav je računalni, komunikacijski ili drugi sustav u kojem se podaci obrađuju, pohranjuju ili prenose tako da budu dostupni i uporabljivi za korisnike informacijskog sustava.

3.2. Resursi informacijskog sustava su harvderska, softverska i informacijska imovina te korisnici informacijskog sustava.

3.3. Hardverska imovina su računala i računalna oprema, komunikacijska oprema, sustavi za pohranu podataka te ostala tehnička oprema koja podržava rad informacijskog sustava.

3.4. Softverska imovina su operativni sustavi, program za nadzor informacijskih sustava, sigurnosni program, korisnički programi, programi za upravljanje bazama podataka, alati za razvoj programa, uslužni programi i ostali programi koji se nalaze na informacijskim sustavima.

3.5. Informacijska imovina su podaci u bazama podataka, datoteke s podacima, programski kod u tekstualnom obliku, dokumentacija o informacijskim sustavima i programima, priručnici, planovi i usluge informacijskog sustava te cjelokupni edukacijski material koji služi podršci poslovanju.

3.6. Korisnici informacijskog sustava su radnici, suradnici, vanjski partneri i druge strane koje na bilo koji način dolaze u doticaj s resursima informacijskog sustava Društva.

4. Upravljanje pristupom

4.1. **Pristup informacijama:** Pristup informacijama određuje se prema načelu "najmanje privilegije". Svaki korisnik dobiva pristup samo onim informacijama koje su mu nužne za obavljanje poslovnih zadataka.

4.2. **Identifikacija i autentikacija**: Koristi se sustav identifikatora i zaporki za potvrdu identiteta korisnika pri pristupu informacijama.

5. Sigurnosne tehnologije

5.1. **Enkripcija:** Sve osjetljive informacije pohranjuju se i prenose putem sigurnih enkripcijskih metoda kako bi se osigurala njihova povjerljivost.

5.2. **Sigurnosni sustavi:** Implementiraju se sigurnosni sustavi, uključujući antivirusne programe, vatrozide i sustave za detekciju nepravilnosti te se redovito ažuriraju kako bi se otkrile i spriječile prijetnje.

6. Fizička sigurnost

6.1. **Sigurnost prostora:** Pristup prostorijama s informacijskom opremom i podacima ograničen je, a koriste se mjere kao što su video nadzor i kontrola pristupa.

7. Upravljanje rizicima informacijske sigurnosti

7.1. **Identifikacija rizika:** Društvo je kao rizike informacijske sigurnosti prepoznalo sljedeće događaje: prirodne katastrofe, tehnički kvarovi, požari i eksplozije, cyber (hakerski) napadi, hardverski kvarovi ili gubitak podataka, problemi s informatičkom infrastrukturom.

7.2. **Razvoj strategija upravljanja rizicima:** Društvo je razvilo strategije za upravljanje rizicima, uključujući izbjegavanje, prijenos, smanjenje ili prihvaćanje rizika, uključujući, ali ne ograničavajući se na: redovito ažuriranje sigurnosnih kopija podataka, redovito održavanje opreme, redovito održavanje protupožarnih sustava, uspostava protupožarnih procedura, implementacija sigurnosnih mjera poput firewalla, antivirusnih programa, redovito ažuriranje softvera, obuka

radnika o sigurnosti na internetu te redovito održavanje mreže i servera, implementacija sustava za nadzor i brzo otklanjanje problema vezanih uz informatičku infrastrukturu.

7.3. **Kontinuirano praćenje rizika:** Rizici će se redovito pratiti kako bi se identificirale promjene u okolini rizika i njihov utjecaj na informacijsku sigurnost.

8. Upravljanje kontinuitetom poslovanja

8.1. Upravljanje kontinuitetom poslovanja jedan je od strateških interesa Društva kako bi se zaštitili poslovni procesi od većih prekida ili katastrofa te izvršio oporavak uslijed neželjenog događaja u što kraćem vremenu.

8.2. Društvo će osigurati pouzdanu pričuvnu pohranu ključnih informacijskih resursa i poduzimati sve potrebne mjere kako bi bile spremne pravovremeno i kompetentno odgovoriti na sigurnosne incidente koji mogu pogoditi resurse informacijskog sustava, kao što su: identifikacija ključnih resursa i procesa; procjena rizika; razvoj plana kontinuiteta poslovanja.

9. Edukacija i usavršavanje radnika

9.1. Svi radnici prolaze sigurnosno informiranje prilikom zapošljavanja te radnici potpisuju izjave o povjerljivosti kako bi bili svjesni potencijalnih prijetnji i kako bi znali pravilno postupati s informacijama. U slučaju potrebe, odnosno promjena u tehnologiji, zakonodavstvu i poslovnim potrebama Društva, radnici će se dodatno educirati i usavršavati.

10. Postupci u slučaju incidenta

10.1. **Prijavljivanje incidenata:** Svi incidenti vezani uz informacijsku sigurnost odmah se prijavljuju nadležnim osobama, a provodi se istraga kako bi se utvrdio uzrok i poduzeli odgovarajući koraci za rješavanje problema.

10.2. **Koordinacija s drugima:** Društvo će surađivati s relevantnim sudionicima, uključujući zakonske tijela, dobavljače, i druge organizacije kako bi učinkovito upravljalo incidentima i dijelila relevantne informacije.

10.3. **Odgovor na informacijske sigurnosne incidente:** Društvo će osigurati brz i učinkovit odgovor na incidente, uključujući primjenu odgovarajućih mjera kako bi se ograničila šteta i spriječilo daljnje širenje incidenta.

10.4. **Praćenje i pregled odgovora na incidente**: Periodički će se provoditi vježbe odgovora na incidente kako bi se osigurala učinkovitost postupaka i identificirale moguće poboljšave.

10.5. **Istraživanje i izvještavanje o informacijskim sigurnosnim incidentima:** Društo će provesti detaljne istrage o incidentima, dokumentirati rezultate i izvijestiti odgovorne strane prema utvrđenim postupcima.

11. Praćenje i revizija

11.1. **Praćenje:** Sigurnosne mjere redovito se prate kako bi se osiguralo njihovo ispravno funkcioniranje.

11.2. **Revizija:** Politika informacijske sigurnosti redovito se pregledava i ažurira kako bi odražavala promjene u tehnologiji, zakonodavstvu i poslovnim potrebama Društva.

Industrija komunalne opreme i mjerila IKOM d. d. ZAGREB Kovinska 7

IKOM Industrija komunalne opreme i

mjerila, dioničko društvo