Organizacija je posvećena očuvanju povjerljivosti, integriteta i dostupnosti svih informacija kojima upravlja. Naša Politika informacione bezbjednosti ima za cilj zaštitu svih vrsta informacija (uključujući lične podatke i kritičnu infrastrukturu) u skladu sa važećim zakonodavstvom i međunarodnim standardima. Pored toga, politika pokreće smanjenje rizika i obezbjeđuje usklađenost sa pravilima zaštite privatnosti i korišćenja vještačke inteligencije (AI), uz kontinuirano poboljšanje sistema bezbjednosti.

Ciljevi Sistema menadžmenta bezbjednošću informacija

- Obezbjeđivanje bezbjednog pristupa, zaštite i upravljanja podacima svih klijenata i zaposlenih, kao i osiguranje privatnosti korisnika u skladu sa zakonodavstvom o zaštiti podataka.
- Uvođenje najsavremenijih tehnologija i procedura za upravljanje bezbjednošću, uključujući AI tehnologije, koje će omogućiti prepoznavanje i sprečavanje sigurnosnih prijetnji.
- Održavanje i kontinuirano poboljšanje sistema menadžmenta bezbjednošću informacija (ISMS), u cilju smanjenja rizika i unapređenja sigurnosnih sistema organizacije.
- Usklađivanje sa relevantnim standardima, kao što su ISO/IEC 27001, ISO/IEC 27701 i ISO/IEC 42001, i postizanje najviših standarda u industriji u vezi sa zaštitom podataka i primjenom AI.

Osnovni principi informacione bezbjednosti, sajber bezbjednost i zaštitu privatnosti

Politika informacione bezbjednosti zasniva se na sledećim osnovnim principima:

- **Povjerljivost**: Svi podaci moraju biti zaštićeni od neovlašćenog pristupa i razmjene. Ovaj princip se primjenjuje na sve vrste podataka, uključujući lične podatke, poslovne informacije i druge povjerljive informacije.
- **Integritet**: Podaci i sistemi moraju biti tačni i pouzdani. Organizacija implementira kontrole koje osiguravaju da podaci nisu izmijenjeni bez odobrenja i da su tačni tokom cijelog životnog ciklusa.
- **Dostupnost**: Podaci i sistemi moraju biti dostupni ovlašćenim korisnicima kada su im potrebni. To uključuje pravovremeno pružanje potrebnih informacija u skladu sa poslovnim potrebama i uslovima.
- **Transparentnost**: Organizacija se obavezuje da će obezbijediti transparentnost u svim postupcima koji se tiču zaštite informacija, privatnosti korisnika i upotrebe AI. Ovo uključuje jasno obavještavanje korisnika o tome kako se njihovi podaci prikupljaju, koriste i štite.
- **Odgovornost**: Svaka osoba u organizaciji, od menadžmenta do zaposlenih, snosi odgovornost za poštovanje politika i procedura u vezi sa informacijama i njihovom zaštitom. Menadžment je odgovoran za postavljanje strategije i nadgledanje implementacije istih.

- **Kompletna zaštita**: Organizacija implementira zaštitu koja pokriva sve aspekte informacija, uključujući fizičku, tehničku i organizacionu zaštitu, kako bi obezbijedila integralnu sigurnost svih podataka i resursa.
- **Kontinuirani razvoj i prilagođavanje**: Sa obzirom na brzo mijenjajući tehnološki pejzaž i nove prijetnje, organizacija je posvećena kontinuiranom razvoju svojih bezbjednosnih praksi, tehnologija i strategija kako bi se odgovorilo na nove izazove i prilike.
- **Usklađenost sa zakonodavstvom i regulativama**: Organizacija se obavezuje da će se pridržavati svih važećih zakona, regulativa i međunarodnih standarda u oblasti zaštite podataka, privatnosti i upravljanja AI, uključujući GDPR, ISO/IEC 27001, ISO/IEC 27701, i ISO/IEC 42001.

Posvećenost ispunjavanju primjenjivih zahtjeva

Organizacija se obavezuje da će:

- Ispunjavati sve zakonske, regulatorne i ugovorne zahtjeve koji se odnose na zaštitu informacija, privatnost i korišćenje vještačke inteligencije.
- Osigurati da sve operacije budu usklađene sa relevantnim industrijskim standardima, zakonodavstvom i politikama koje se odnose na bezbjednost informacija, zaštitu privatnosti i primjenu AI.

Kontinuirano poboljšanje ISMS-a

Kontinuirano poboljšanje Sistema menadžmenta bezbjednošću informacija (ISMS) predstavlja ključni aspekt našeg pristupa u održavanju visokoefikasne zaštite informacija, privatnosti podataka i upotrebe vještačke inteligencije. Organizacija se obavezuje da će stalno evaluirati, unapređivati i prilagođavati svoje prakse, procese i tehnologije kako bi odgovarala novim izazovima, prijetnjama i potrebama korisnika.

Kontinuirano poboljšanje ISMS-a obuhvata nekoliko ključnih aktivnosti koje omogućavaju da organizacija ostane agilna, usklađena sa zakonodavstvom i međunarodnim standardima, a istovremeno minimizuje rizike i maksimizira efikasnost bezbjednosnih kontrola. Neki od ključnih elemenata ovog procesa uključuju:

1. **Redovno praćenje i procjena performansi ISMS-a**:
    - Organizacija će kontinuirano pratiti efikasnost implementiranih bezbjednosnih politika, procedura i kontrola kako bi obezbijedila da odgovaraju definisanim ciljevima i da se postiže očekivana zaštita podataka.
    - Sprovodićemo interne i eksterne revizije kako bismo procenili usklađenost sa standardima kao što su ISO/IEC 27001, ISO/IEC 27701 i ISO/IEC 42001, te identifikovali potencijalne nedostatke u sistemu.
2. **Praćenje i upravljanje promjenama**:

- S obzirom na brz razvoj tehnologije i stalne promjene u zakonodavstvu, organizacija je posvećena stalnom praćenju novih rizika i mogućnosti. To uključuje promjene u tehnologijama vezanim za informacionu bezbjednost, kao što su napredne metode zaštite podataka, vještačka inteligencija, ili zakonski zahtjevi koji utiču na poslovanje organizacije.
    - Kada se identifikuju nove tehnologije ili promjene u poslovnim procesima, organizacija će preduzeti odgovarajuće korake za implementaciju tih promjena u sistemu menadžmenta bezbjednošću informacija.

3. **Analiza incidenata i reakcija na bezbjednosne prijetnje**:
    - Organizacija će redovno analizirati bezbjednosne incidente, učiti iz njih i implementirati preventivne mjere kako bi smanjila mogućnost ponovnog nastanka sličnih incidenata. Ovo uključuje i praćenje i upravljanje sajber prijetnjama, zaštitu privatnosti podataka i analizu prijetnji koje dolaze od naprednih AI sistema.
    - Analize post-mortem nakon bezbjednosnih incidenata pomažu organizaciji da izvuče pouke i unaprijedi svoje bezbjednosne procedure, tako što identifikuje slabe tačke i preporučuje potrebne korektivne akcije.
4. **Poboljšanje obuka i svijesti zaposlenih**:
    - Jedan od ključnih aspekata kontinuiranog poboljšanja je redovno obučavanje zaposlenih o novim prijetnjama, tehnikama zaštite i principima koji se odnose na zaštitu podataka i privatnost. Organizacija će razviti programe koji poboljšavaju svijest zaposlenih o rizicima koji se odnose na sigurnost informacija, privatnost korisnika i etičko korišćenje vještačke inteligencije.
    - Obuke će se prilagoditi specifičnim potrebama organizacije, uzimajući u obzir sve oblasti koje se tiču bezbjednosti, privatnosti podataka, upotrebe AI i integracije novih tehnologija.
5. **Korektivne i preventivne mjere**:
    - Svaka identifikovana neskladnost ili slabost u postojećim bezbjednosnim praksama biće analizirana, a odgovarajuće korektivne mjere će biti implementirane. Osim toga, organizacija će koristiti preventivne strategije da bi minimizirala rizik od budućih problema.
    - Prepoznavanje mogućih prijetnji ili slabosti u sistemu menadžmenta informatičke bezbjednosti omogućava implementaciju preventivnih koraka i postupaka za smanjenje rizika i sprečavanje negativnih efekata.
6. **Evaluacija i usklađenost sa standardima i zakonodavstvom**:
    - Kontinuirano poboljšanje obuhvata i praćenje promjena u zakonodavstvu, industrijskim standardima i najboljim praksama. Organizacija će se pobrinuti da njen ISMS uvijek bude usklađen sa relevantnim zakonima o zaštiti podataka, sigurnosti informacija i upotrebi vještačke inteligencije, kao i sa globalnim standardima kao što su GDPR, ISO/IEC 27001, ISO/IEC 27701, i ISO/IEC 42001.
    - Sprovedene revizije će identifikovati usklađenost sa važećim standardima i preporučiti potrebne prilagodbe i unapređenja.
7. **Uključivanje povratnih informacija i korisničkih povratnih podataka**:
    - Organizacija će redovno koristiti povratne informacije od klijenata, zaposlenih i drugih zainteresovanih strana kako bi se poboljšali procesi informatičke bezbjednosti i zaštite

privatnosti. Kroz kontinuirani dijalog sa svim korisnicima i partnerima, biće moguće uočiti prednosti i slabosti postojećih sistema i izvršiti potrebne prilagodbe.

Kontinuirano poboljšanje ISMS-a nije jednokratan zadatak, već proces koji je integrisan u svakodnevno poslovanje organizacije. Organizacija se obavezuje da će nastaviti da razvija i unapređuje svoj sistem bezbjednosti informacija kako bi osigurala zaštitu podataka, privatnost korisnika i etičko korišćenje AI tehnologija. Kroz ovaj proces, naša organizacija će biti u mogućnosti da efikasno odgovori na nove izazove, smanji rizike i obezbijedi visok nivo sigurnosti i povjerenja.

Pristup upravljanju rizicima

U organizaciji, pristup upravljanju rizicima predstavlja osnovu za identifikaciju, procjenu, kontrolisanje i smanjenje potencijalnih prijetnji koje bi mogle uticati na bezbjednost informacija, privatnost podataka, operacije i korišćenje vještačke inteligencije. Ovaj pristup temelji se na osnovnim principima sistematičnosti, proaktivnosti, transparentnosti i usklađenosti sa relevantnim standardima, zakonodavstvom i najboljim praksama. U okviru sistema menadžmenta bezbjednošću informacija (ISMS), pristup upravljanju rizicima obuhvata sledeće ključne korake:

1. Identifikacija rizika

- Prvi korak u upravljanju rizicima je identifikacija svih mogućih rizika koji mogu negativno uticati na organizaciju. To uključuje rizike u vezi sa sigurnošću informacija, zaštitom privatnosti podataka, upotrebom vještačke inteligencije i drugim operativnim procesima.
- Ovaj proces podrazumijeva analizu svih aspekata organizacije, uključujući infrastrukturu, sisteme, aplikacije, ljudske resurse i potencijalne prijetnje sa spoljnog okruženja (npr. sajber napadi, prirodne nepogode, unutrašnje greške).

2. Procjena rizika

- Nakon identifikacije rizika, organizacija procjenjuje vjerovatnoću pojave svakog rizika, kao i potencijalnu ozbiljnost njegovih posledica. Kroz ovu procjenu, organizacija utvrđuje koji su rizici najkritičniji i koji zahtijevaju hitnu pažnju.
- Procjena rizika obuhvata analizu uticaja na poslovanje, korisnike, reputaciju organizacije, zaštitu podataka, sigurnost informacija i usklađenost sa zakonodavstvom.

3. Upravljanje rizicima

- Na osnovu procjene, organizacija usvaja odgovarajuće mjere za upravljanje identifikovanim rizicima. To uključuje:
- **Prevencija**: Uzimanje proaktivnih koraka kako bi se smanjila vjerovatnoća da se rizici ostvaruju. Na primer, implementacija tehničkih zaštita, obuka zaposlenih i usklađenost sa zakonodavstvom.
- **Kontrola**: Uvođenje kontrola za smanjenje potencijalnih negativnih posledica, kao što su implementacija zaštite podataka, monitorisanje IT sistema i kontrola pristupa.

- **Odziv**: Razvijanje planova i procedura za brzo reagovanje na rizike i minimiziranje njihovog uticaja na poslovanje. To uključuje planove za krizne situacije i obavezne postupke za reagovanje u slučaju bezbjednosnih incidenata.

4. Praćenje i nadzor

- Pratimo efikasnost implementiranih mjera za upravljanje rizicima kroz kontinuirani nadzor i evaluaciju. Uključuje periodične revizije sistema i analiza bezbjednosnih incidenata, kao i testiranje resursa organizacije u situacijama rizika.
- Praćenje može obuhvatiti redovne interne i eksterne revizije usklađenosti sa standardima kao što su ISO/IEC 27001, ISO/IEC 27701 i ISO/IEC 42001, kao i testiranje otpornosti na sajber napade ili druge prijetnje.

5. Kontinuirano poboljšanje

- Na osnovu praćenja i analiza, organizacija se obavezuje da će kontinuirano poboljšavati strategije za upravljanje rizicima. To uključuje ažuriranje politika i procedura, obuku zaposlenih i primjenu novih tehnologija koje poboljšavaju bezbjednost i smanjuju rizike.
- Kontinuirano poboljšanje omogućava organizaciji da ostane fleksibilna i brzo odgovori na nove izazove, tehnologije i zakonske promjene, a sve u cilju minimiziranja rizika za organizaciju i njene klijente.

6. Usklađenost sa zakonodavstvom i standardima

- Pristup upravljanju rizicima podrazumijeva usklađenost sa relevantnim zakonodavstvom, kao što su zakonodavstvo o zaštiti podataka (GDPR, Zakon o zaštiti podataka o ličnosti), kao i međunarodni standardi kao što su ISO/IEC 27001, ISO/IEC 27701 i ISO/IEC 42001.
- Organizacija se obavezuje da će redovno pratiti promjene u zakonodavstvu i standardima te prilagoditi svoje prakse i politike u skladu sa novim zahtjevima.

7. Uključivanje zaposlenih i zainteresovanih strana

- Zaposleni i relevantne zainteresovane strane (klijenti, dobavljači, regulatorna tijela) igraju ključnu ulogu u procesu upravljanja rizicima. Organizacija se obavezuje da će ih uključiti u procese identifikacije i analize rizika, kao i u sprovođenje potrebnih mjera.
- Ova participacija omogućava organizaciji da dobije široku perspektivu na potencijalne rizike i poboljša efikasnost svojih reakcija.

Pristup upravljanju rizicima omogućava organizaciji da sistematski i efikasno reaguje na rizike koji mogu ugroziti bezbjednost informacija, privatnost podataka, bezbjednost korisnika i uspješno korišćenje vještačke inteligencije. Kroz ovaj sveobuhvatan pristup, organizacija stvara bezbjedno i sigurno poslovno okruženje koje štiti sve zainteresovane strane i omogućava rast i razvoj poslovanja.

Provjera sistema menadžmenta bezbjednošću informacija

Organizacija se obavezuje da će:

- Redovno pratiti usklađenost sa standardima ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 42001 i drugim relevantnim normama i regulativama.

- Pružiti odgovarajuće obuke svim zaposlenima kako bi osigurala usklađenost sa politikama bezbjednosti informacija, zaštite privatnosti i primjene AI.
- Sprovoditi interne i eksterne revizije i evaluacije kako bi se osigurala usklađenost i identifikovali potencijalni problemi ili oblasti za poboljšanje.

Organizacija će sprovoditi redovne provjere sistema menadžmenta bezbjednošću informacija kako bi osigurala:

- Efikasnost implementiranih bezbjednosnih kontrola i procedura.
- Identifikaciju nedostataka i područja koja zahtijevaju poboljšanje.
- Pravovremeno usklađivanje sa novim prijetnjama i sigurnosnim izazovima, kako bi se organizacija zaštitila od novih i razvijajućih rizika.

Ova Politika informacione bezbjednosti postavlja temelj za zaštitu informacija, privatnosti, kao i etičko korišćenje vještačke inteligencije unutar organizacije. Organizacija je posvećena održavanju najviših standarda zaštite podataka, sigurnosti i odgovornog upravljanja AI sistemima, sa stalnim unapređenjem sistema i njegovih procedura kako bi se obezbijedila usklađenost sa svim relevantnim zakonima, normama i industrijskim praksama.

Vlasnik dokumenta i odobrenje

Najmanje jednom godišnje ili u slučaju značajnih promjena u poslovanju, tehnologiji ili zakonodavstvu najviše rukovodstvo će vršiti preispitivanje ovog dokumenta.

Trenutna verzija ovog dokumenta dostupna je svim članovima osoblja na oglasnoj tabli i zvaničnoj Telegram grupi koja se koristi za internu komunikaciju zaposlenih. Ne sadrži povjerljive informacije i može se dati relevantnim eksternim stranama.

Politiku Sistema menadžmenta bezbjednošću informacija je odobrio osnivač Ivan Šoć, 10. 03. 2025. i izdaje se na bazi kontrolisane verzije sa potpisom osnivača.

Potpis:

Datum: 10.03.2025.

FIVE GROUP DOO
FIVE G
PODGORICA