A black background with red text

Description automatically generated

***IT381 Zaštita i bezbednost informacija***

***Domaći zadatak br. 14***

***Ime i prezime: Jovan Pavkovic***

***Broj indeksa: 4442***

**Rešenje domaćeg zadatka**

Bezbednosna Politika “SafeNet Dynamics” firme koja je fokusirana na pružanje dinamičnih i sigurnih rešenja u oblasti informacione bezbednosti. Ovo može uključivati inovativne tehnologije, usluge bezbednosti mreže, zaštitu podataka, upravljanje identitetom ili slične oblasti.

**Politika informacione bezbednosti**

I          Uvod

1. **Informacija** postoji u različitim formama. Ona može biti odštampana ili napisana na papiru, sačuvana u elektronskom obliku, prenesena putem pošte ili korišćenjem elektronskih sredstava, kao i izgovorena. Bez obzira na formu u kojoj se pojavljuje ili na sredstvo pomoću kojeg je prenesena ili sačuvana, ona treba uvek da je zaštićena na odgovarajući način.
2. **Informaciona bezbednost** se ostvaruje primenom odgovarajućeg skupa administrativnih, tehničkih i fizičkih kontrola, koje obuhvaćaju politike, procese, postupke, organizacione strukture, softverske i hardverske funkcije.
3. **Glavni ciljevi** informacione bezbednosti su:

* **Poverljivost** (eng. Confidentiality) – Osobina informacije da je dostupna isključivo ovlašćenim korisnicima ili procesima.
* **Integritet** (eng. Integrity) – Osobina informacije da mogu da je izmene isključivo ovlašćeni korisnici ili procesi.
* **Dostupnost** (eng. Availability) – osobina informacije da je dostupna ovlašćenim korisnicima ili procesima onda kada za to postoji poslovna potreba.

1. **Drugi ciljevi** informacione bezbednosti su:

* **Identifikacija** (eng. Identification) – Jednoznačna identifikacija korisnika ili procesa sistema ili aplikacije.
* **Provera identiteta** (eng. Authentication) – Potvrda da je korisnik sistema ili aplikacije identifikovana osoba ili proces.
* **Primena ovlašćenja** (eng. Authorization) – Dodela odgovarajućih ovlašćenja korisniku ili procesu u okviru sistema ili aplikacije nakon što se uspešno završi identifikacija i provera identiteta.
* **Odgovornost za urađeno** (eng. Accountability) – Izvršene aktivnosti u okviru sistema ili aplikacije koje su relevantne za sigurnost moraju da budu zabeležene i dokazive.

II         Kontekst organizacije

1. SafeNet Dynamics je bezbednosna firma koja deluje u oblasti informacione bezbednosti, fokusirana na pružanje sigurnih i dinamičnih rešenja. Razvijen je sveobuhvatan informacioni sistem za proizvodnju, održavanje i nadogradnju softvera za bezbedno upravljanje podacima i identitetima klijenata, sa posebnim osvrtom na priređivanje igara na sreću i online platforme.
2. U registru identifikovanih zainteresovanih strana, definisani su zahtevi koji su od suštinskog značaja za bezbednost informacija.
3. Aktivnosti SafeNet Dynamics obuhvaćene su ISMS-om, a kreirana Izjava o primenjivosti jasno definiše obim sistema u skladu sa ISO 27001:2013 standardom.
4. ISMS sistem u okviru SafeNet Dynamics-a je uspostavljen, implementiran i kontinuirano se održava i unapređuje kako bi se zadovoljili standardi bezbednosti informacija, obezbeđujući visok nivo zaštite za informacije o transakcijama igara na sreću i druge poverljive podatke.

III        Politika informacione bezbednosti

1. Rukovodstvo kompanije odobrava Politiku informacione bezbednosti. Politika je objavljena i saopštena svim zaposlenima i trećim stranama.
2. Specifične uloge i odgovornosti informacione bezbednosti utvrđuju se dokumentima nižeg nivoa, opisima rada i ugovorima zaposlenih.
3. SafeNet Dynamics redovno preispituje Politiku informacione bezbednosti i po potrebi je dopunjava kada se uoče nove pretnje ili promene u okruženju, prepoznaju nove najbolje prakse informacione bezbednosti, dese velike promene u infrastrukturi, uslugama, organizacionoj strukturi ili kao rezultat nezavisnih internih ili eksternih nalaza provere ISMS-a.

IV        Podrška rukovodstva

1. Rukovodstvo kompanije priznaje da program informacione bezbednosti postoji da bi se podržali poslovni zahtevi za uspešno i konkurentno poslovanje kompanije, kao i zbog usaglašavanja sa relevantnim standardima, zakonima i propisima tržišta na kojima kompanija posluje. Takođe, rukovodstvo kompanije potvrđuje činjenicu da je njegova podrška ključna za ostvarivanje kompanijskih ciljeva informacione bezbednosti i efikasno planiranje, implementiranje i održavanje kontrola informacione bezbednosti.
2. Rukovodstvo kompanije daje punu podršku u razvoju i sprovođenju aktivnosti informacione bezbednosti.

IV.1     Organizacione uloge

1. SafeNet Dynamics kontinuirano radi na prepoznavanju rizika informacione bezbednosti na svim tržištima u koordinaciji sa ISMS timovima, na kreiranju mera za tretiranje rizika informacione bezbednosti, kao i na koordinaciji aktivnosti za njihovo uspostavljanje i implementaciju.
2. ISMS timovi su formirani na svim tržištima s ciljem efikasnog sprovođenja aktivnosti informacione bezbednosti.
3. Svi zaposleni su odgovorni da se u svom radu pridržavaju pravila koja su propisana Politikom informacione bezbednosti i drugim politikama informacione bezbednosti.

V         Upravljanje rizicima informacione bezbednosti

1. SafeNet Dynamics kontinuirano radi na identifikaciji i evaluaciji rizika informacione bezbednosti, na definisanju mera za tretiranje rizika i na koordinisanju aktivnosti za njihovu implementaciju u skladu sa Politikom upravljanja rizicima.
2. Aktivnosti informacione bezbednosti, ciljevi, implementacija i unapređenje kontrola informacione bezbednosti se bazira na utvrđenim rizicima informacione bezbednosti i merama za njihovo tretiranje.
3. Ciljevi informacione bezbednosti se postavljaju i evaluiraju na godišnjem nivou.

VI        Svest o informacionoj bezbednosti

1. SafeNet Dynamics kontinuirano radi na podizanju svesti o informacionoj bezbednosti, organizuje i sprovodi različite oblike osvešćivanja zaposlenih o informacionoj bezbednosti koji uključuju, no nisu ograničeni na, sprovođenje phishing simulacija, organizovanje i/ili sprovođenje on-line ili on-site obuka i obaveštenja prema zaposlenima preko elektronske pošte i drugih kanala komunikacije.
2. Novi zaposleni prolaze inicijalnu obuku o informacionoj bezbednosti koja podrazumeva formalno upoznavanje sa politikama informacione bezbednosti i očekivanjima kompanije u periodu od mesec dana nakon zaposlenja, a ta se obuka dalje nastavlja u toku radnog odnosa i to najmanje jednom u periodu od godinu dana.

VII       Praćenje i merenje performansi ISMS sistema

1. SafeNet Dynamics definiše kriterijume za praćenje i merenje performansi ISMS sistema koje se analiziraju i vrednuju najmanje jednom godišnje pre preispitivanja ISMS sistema od strane rukovodstva kompanije.
2. **Svrsishodnost i Obim**

* Ova bezbednosna politika ima za cilj zaštitu informacionih resursa od potencijalnih pretnji i rizika.
* Obuhvata sve informacije, tehnologije i procese koji podržavaju poslovanje.
* Odgovornosti CIO/CTO/IT Direktora

1. **Rukovođenje Bezbednošću**

* Definisanje i implementacija strategija za bezbednost informacija.
* Praćenje i evaluacija rizika, a zatim i prilagođavanje politike prema promenama u pretnjama ili tehnologijama.
* Odnos sa Senior Izvršnim Osobama

1. **Saradnja sa CEO/CFO**

* Periodično izveštavanje o bezbednosnim inicijativama i rezultatima.
* Saradnja u pravljenju i održavanju budžeta za bezbednost informacija.
* Pravilnik o pristupu

1. **Identifikacija i Autentifikacija**

* Jasan pravilnik za pristup informacionim resursima na osnovu identiteta i uloga korisnika.
* Zaštita podataka

5. **Klasifikacija Informacija**

* Definisanje nivoa poverljivosti i pravila za rukovanje sa različitim vrstama informacija.
* Mrežna bezbednost

6. **Zaštita Mrežne Infrastrukture**

* Implementacija najnovijih sigurnosnih tehnologija i praksa zaštite mreže.
* Bezbednost aplikacija

7. **Sigurnosni Standardi Razvoja**

* Definisanje i primena standarda bezbednosti tokom razvoja i održavanja softverskih aplikacija.
* Monitoring i reakcija na incidente

8. **Praćenje Aktivnosti**

* Kontinuirani nadzor informacionih sistema radi rane detekcije nepravilnosti.
* Planiranje i sprovođenje postupaka odgovora na incidente.
* Obuka i svest zaposlenih

9. **Edukacija o Bezbednosti**

* Redovna obuka zaposlenih o bezbednosnim praksama i merama.

10. **Periodične Revizije**

* Planiranje i sprovođenje revizija politike radi prilagođavanja novim pretnjama i tehnološkim promenama.