Kao moderna organizacija orijentisana ka budućnosti, organizacija je prepoznala potrebu da se poslovanje odvija bezbedno i neometano, što je interes korisnika, menadžmenta i drugih zainteresovanih strana.
U cilju obezbeđivanja adekvatnog nivoa bezbednosti informacija, sajber bezbednosti i zaštite privatnosti organizacija je implementirala sistem menadžmenta bezbednošću informacija (ISMS) u skladu sa međunarodnim standardom ISO/IEC 27001, kodom dobre prakse iz ove oblasti.
Poslovanje u skladu sa Sistemom menadžmenta bezbednošću informacija ima brojne prednosti za poslovanje, uključujući:

- Zaštita toka prihoda i profitabilnosti organizacije
- Sigurna isporuka proizvoda i usluga korisnicima
- Održavanje i jačanje vrednosti organizacije
- Usklađenost sa zahtevima zakona i propisa
- Usaglašenost sa ugovornim zahtevima.

Važno je razumeti koje poslovne oblasti su obuhvaćene ISMS-om, a koje su isključene iz opravdanih razloga. Predmet i područje primene ISMS-a u organizaciji je definisano u dokumentu Kontekst bezbednosti informacija. Preporučuje se da se pomenuti dokument preispituje zajedno sa ovom politikom.
Svrha ovog dokumenta je da definiše opštu politiku koja se odnosi na bezbednost informacija, sajber bezbednost i zaštitu privatnosti koja zadovoljava potrebe organizacije, a obuhvata:

- Okvir za postavljanje ciljeva Sistema mendžmenta bezbednošću informacija
- Posvećenost ispunjavanju zahteva
- Posvećenost stalnom poboljšanju ISMS-a.

ISMS politika dostupna je u papirnoj i elektronskoj formi i biće dostupna zaposlenima u organizaciji, kao i svim relevantnim zainteresovanim stranama.

Ciljevi Sistema menadžmenta bezbednošću informacija

Glavni ciljevi ISMS-a unutar organizacije definisani su u Kontekstu bezbednosti informacija. Ovi ciljevi su od ključne važnosti za poslovanje i ne treba ih često menjati. Opšti ciljevi će poslužiti kao smernice za kreiranje operativnih ciljeva, nižeg nivoa, kratkoročnih ciljeva kreiranih tokom godišnjeg planiranja ISMS-a, čiji se vremenski okvir poklapa sa planiranjem budžeta organizacije. Na ovaj način će se obezbediti odgovarajuća sredstva za identifikovane aktivnosti unapređenja.
Ciljevi će biti kreirani na osnovu jasnog razumevanja opštih zahteva poslovanja i pratiće se u skladu sa izmenama konteksta organizacije tokom godine. Ciljevi ISMS-a postoje kao dokumentovana informacija za svaku poslovnu godinu, zajedno sa detaljima plana za njihovo postizanje. Nakon odobrenja, ovaj plan će se preispitati svake godine kao deo procesa

preispitivanja od strane rukovodstva, tokom kojeg će se ciljevi takođe revidirati kako bi se osigurala njihova valjanost. Ako su promene neophodne, njima će se upravljati kroz proces upravljanja promenama u organizaciji.

Osnovni principi informacione bezbednosti, sajber bezbednost i zaštitu privatnosti

Informaciona bezbednost, sajber bezbednost i zaštita privatnosti zasnivamo na nekoliko osnovnih principa. Prva tri su poznata kao tripartitni model Poverljivost, Integritet i Dostupnost (Confidentiality, Integrity, Availability Model (CIA model)), dok su jednako važni i Autentičnost i Neporecivost.

Poverljivost (Confidentiality): Poverljivost podataka podrazumeva da su informacije dostupne samo onima koji su ovlašćeni da im pristupe. Ovaj princip štiti osetljive podatke od neovlašćenog otkrivanja ili pristupa, što je posebno važno u slučajevima kada su u pitanju podaci o ličnosti ili poslovne tajne.

Integritet (Integrity): Integritet podataka osigurava da informacije ostanu tačne i potpune, bez neovlašćenih izmena. Ovaj princip zahteva da se podaci zaštite od namerne ili slučajne promene tokom prenosa ili skladištenja.

Dostupnost (Availability): Dostupnost podrazumeva da ovlašćeni korisnici u svakom trenutku mogu pristupiti potrebnim informacijama. Održavanje dostupnosti podataka i sistema ključni je faktor za neometano poslovanje.

Autentičnost predstavlja svojstvo IKT sistema kojim se osigurava mogućnost da se proveri i potvrdi da je informaciju stvorio ili poslao onaj za koga se tvrdi da je tu radnju izvršio.

Neporecivost predstavlja sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći.

Posvećenost ispunjavanju primenjivih zahteva

Posvećenost ispunjenju zahteva ISMS-a je prisutno na najvišem nivou organizacije, a pokazuje se kroz Politiku bezbednosti informacija i obezbeđivanje adekvatnih resursa za uspostavljanje, primenu, održavanje i razvoj Sistema menadžmenta bezbednošću informacija (ISMS). Najviše rukovodstvo obezbeđuje da se vrednovanje i analiza sistema sprovodi na redovnoj osnovi, kako bi se osiguralo ispunjenje ciljeva ISMS-a i identifikovala moguća pobojšanja kroz program provere i procese upravljanja. Preispitivanje od strane rukovodstva mogu imati nekoliko oblika, uključujući

pojedinačne sastanke sa drugim rukovodiocima relevantnih sekora i druge sastanke rukovodstva. U okviru upravljanja postoji nekoliko glavnih uloga koje treba dodeliti kako bi se osigurao uspeh ISMS-a i zaštitilo poslovanje od pretnji i negativnih ishoda rizika. Menadžer ISMS-a je glavni odgovoran i ovlašćen za implementaciju i održavanje sistema menadžmenta bezbednošću informacija, posebno za:

- Identifikaciju, dokumentovanje i ispunjenje primenjivih zahteva
- Dodelu ovlašćenja i odgovornosti za implementaciju, upravljanje i poboljšanje ISMS procesa
- Integracija poslovnih procesa sa ISMS-om
- Usklađenost sa zakonskim, regulatornim i ugovornim zahtevima koji se odnose na bezbedno upravljanje imovinom koja se koristi za isporuku proizvoda i usluga
- Informisanje najvišeg rukovodstva o performansama i poboljšanjima ISMS-a.

Takođe je odgovornost ISMS menadžera da osigura da zaposleni razumeju uloge koje su im dodeljene i koje treba da ispune i da imaju odgovarajuće veštine i kompetencije za njihovo obavljanje.

Organizacija će osigurati da zaposleni odgovorni za upravljanje bezbednošću informacija budu kompetentni, na osnovu odgovarajućeg obrazovanja, obuke, veština i iskustva. Veštine neophodne za postizanje adekvatnog nivoa bezbednosti informacija biće određene i redovno preispitane zajedno sa procenom postojećih nivoa veština unutar organizacije. Identifikovaće se potrebe za obukom i održavati plan kako bi se obezbedile potrebne kompetencija. Sektor za ljudske resurse (HR) interno vodi evidenciju o obuci, obrazovanju i druge relevantne evidencije, tako da su sve individualne veštine, znanja i iskustva dokumentovana. Detalji o odgovornostima povezanim sa svakom od potrebnih uloga ISMS-a i kako su dodeljene unutar organizacije mogu se naći u posebnom dokumentu pod nazivom Uloge, odgovornosti i ovlašćenja. Organizacija koristi različite treće strane, interno i eksterno, za isporuku proizvoda i usluga svojim klijentima. Kada se pod tim podrazumeva izvođenje poslovnog procesa, odnosno dela poslovnog procesa, koji je deo definisane oblasti primene ISMS-a, onda se to evidentira kroz procese upravljanja bezbednošću informacija. U svakom slučaju, organizacija zadržava kontrolu nad relevantnim ISMS procesima, pokazujući:

- Odgovornost za proces
- Kontrola definicije procesa i interfejs procesa
- Praćenje učinka i usklađenosti
- Kontrola poboljšanja procesa.

Ovo će biti podržano dokumentovanim informacijama (dokumenti i zapisi) kao što su ugovori, zapisnici sa sastanaka i izveštaji o učinku, i druge relevantne dokumentovane informacije.

Kontinuirano poboljšanje ISMS-a

Politika koja se odnosi na kontinuirano poboljšanje ISMS-a odnosi se na:

- Kontinuirano poboljšanjeefektivnosti i efikasnosti sistema menadžmenta bezbednošću informacija u svim oblastima obuhvaćenim delokrugom primene
- Poboljšanje postojećih procesa, kako bi se uskladili sa dobrom praksom definisanom u ISO/IEC 27001
- Sticanje ISO/IEC 27001 sertifikata i njegovo redovno obnavljanje (resertifikacija)
- Povećanje stepena proaktivnosti (i poslovne percepcije proaktivnosti) u odnosu na trenutni sistem menadžmenta bezbednošću informacija (razmotrite najnoviji pristup predviđanju događaja bezbednosti informacija, sajber bezbednosti i zaštite privatnosti!)
- Postizanje i povećanje razumevanja i boljeg odnosa između organizacionih jedinica u kojima se implementira ISMS
- Godišnji pregled metrike kako bi se procenilo da li je potrebno izvršiti izmene sistema, na osnovu prikupljenih istorijskih podataka i povratnih informacija iz relevantnih izvora
- Prikupljanje ideja za poboljšanje kroz redovne sastanke sa rukovodiocima na kojima se vrše preispitivanja i njihova dokumentovanost u politici posebne namene.
- Preispitivanje procedura kontinuiranog poboljšanja – korektivnih mera na redovnim sastancima rukovodstva, kako bi se odredili prioriteti i procenili rokovi i koristi.

Ideje za poboljšanje mogu doći iz različitih izvora, uključujući korisnike, dobavljače, zaposlene, procenu rizika i provere. Kada se identifikuju, preventivne i korektivne mere se dodaju u proces kontinuiranog poboljšanja i ocenjuje se njihova efektivnost od strane članova osoblja odgovornih za kontinuirano poboljšanje.
Tokom evaluacije predloženih poboljšanja koristit će se sledeći kriterijumi:

- Troškovi
- Poslovne pogodnosti i koristi
- Rizik
- Vremenski okvir implementacije
- Potrebni resursi.

Ako bude prihvaćen, predlog poboljšanja će imati prioritet kako bi se omogućilo efikasno planiranje.

Pristup upravljanju rizicima

Organizacija koristi strategiju i proces upravljanja rizikom koji su u skladu sa zahtevima ISO/IEC 27001 i preporukama ISO/IEC 27005, međunarodnog standarda za upravljanje rizikom

bezbednosti informacija. To podrazumeva identifikaciju imovine i uzimanje u obzir sledećih aspekata:

- Pretnje
- Ranjivosti
- Uticaj i verovatnoća pre tretmana rizika
- Tretman rizika (npr. Modifikacija nivo rizika, transfer, izbegavanje rizika)
- Uticaj i verovatnoća nakon tretmana rizika
- Vlasnik rizika/odgovorno lice
- Vremenski okvir i učestalost preispitivanja.

Upravljanje rizicima će se obavljati na nekoliko nivoa u okviru sistema menadžmenta bezbednošću informacija, uključujući:

- Planiranje upravljanja bezbednošću informacija, sajber bezbednošću i zaštitom privatnosti
- Procena rizika ugroženosti imovine po osnovu poverljivosti, integriteta i dostupnosti
- Procena rizika kontinuiteta poslovanja u kontekstu organizacije
- Procena rizika promena kao deo procesa upravljanja poslovnim promenama
- Na nivou projekta kao deo upravljanja značajnim poslovnim promenama.

Procena rizika će se vršiti jednom godišnje ili nakon značajnih promena u poslovnom okruženju.

Provera sistema menadžmenta bezbednošću informacija

Nakon što se uspostavi, ključno je sprovoditi redovna preispitivanja primene procedura i procesa sistema menadžmenta bezbednošću informacija. To se vrši na tri nivoa:

1. Struktuirana redovna provera usaglašenosti sa politikama i procedurama unutar organizacije od strane internih proveravača
2. Eksterni sertifikacioni audit treće strane, prema standardu, u cilju dobijanja i održavanja sertifikata ISO/IEC 27001
3. Nezavisne provere preko druge strane.

Sve politike i planovi upravljanja bezbednošću informacija, sajber bezbednošću i zaštitom privatnosti koje čine deo ISMS-a moraju biti dokumentovani. Vođenje zapisa je osnovni deo upravljanja kontinuitetom poslovanja. Zapis je ključni izvor informacija i dokaza da se procesi sprovode efektivno i efikasno.

Vlasnik dokumenta i odobrenje

Najviše rukovodstvo je vlasnik ovog dokumenta i odgovorno je da osigura da se ovaj dokument preispituje u skladu sa ISMS-om.

Trenutna verzija ovog dokumenta dostupna je svim članovima osoblja na korporativnom intranetu i Web stranici. Ne sadrži poverljive informacije i može se dati relevantnim eksternim stranama.

Politiku bezbednosti informacija je odobrio direktor 15.09.2025 i izdaje se na bazi kontrolisane verzije sa potpisom direktora.

Potpis:

Datum: 15.09.2025

Istorija izmena

Verzija	Opis izmene	Odobrenje	Datum izmene
2.0	Usaglasavanje sa ISO/IEC 27001:2022	Vojislav Beljanski	15.09.2025