Zepter International

ISMS OKVIR

Verzija:	1
Kod:	S_2_1_2018
Datum verzije:	23.07.2018.
Kreirano od strane:	ISMS koordinator
Odobreno od strane:	Head of IT
Nivo poverljivosti:	Public

Istorija promena

Datum	Verzija	Kreirano od strane	Opis promene
2018-07-23	1	ISMS koordinator	Definisan dokument

Sadržaj

1. OPSEG, NAMENA I ODGOVORNOSTI

U današnje vreme informacija je jedan od najvažnijih i najskupljih resursa u poslovanju. Njeno pravovremeno posedovanje, njena ispravnost i tajnost I pravovremena dostupnost su od odlučujuće važnosti u poslovanju kompanije Zepter International, koja svoj rad zasniva na validnim informacijama.

Za kvalitetan rad potrebno je zaštiti informacije od:

- neovlašćenih izmena - osigurati **integritet,**
- objavljivanja tajnih informacija - osigurati **tajnost,**
- uskraćivanja dostupnosti informacija ovlašćenim korisnicima – osigurati **dostupnost.**

U cilju povecanja bezbednosti, kreirana je Politika informacione bezbednosti Zepter International IT koja ima za cilj zaštitu informacija tj. osiguranje bezbednosti informacija. Ona predstavlja skup pravila kojima se definiše na koji način IS kompanije učiniti sigurnim i kako zaštititi njegove tehničke i informacione resurse. Politika definiše obaveze i odgovornosti, redovno se preispituje i biće unapređivana u skladu sa razvojem tehnologija i potrebama kompanije.

Implementacija I kontinualno unapredjenje ISMS koji sprovodi Zepter International IT omogućava uspostavljanje bezbednosti na svim kritičnim tačkama IS, u bilo kojem segmentu bezbednosti.

ISMS okvir

ISMS okvir (ISMS- Sistem upravljanja bezbednošću informacija – Information security management system - u daljem tekstu se upotrebljava skraćenica ISMS) predstavlja javno dostupan dokument kao izvod iz važeće PL_1_1_2018 Politika informacione bezbednosti Zepter International IT i obavezujući u poslovanju sa Zepter Internacional IT.

Namena Okvira ISMS

Namena ***Okvira ISMS*** je da prema zainteresovanim stranama definiše i objavi glavne elemente sistema bezbednosti informacija koji primenjuje Zepter internacional IT kao i način na koji se rad usklađuje sa zahtevima standarda ISO 27001 .

Svrha politike informacione pezbednosti

Politika informacione bezbednosti definiše set bezbednosnih pravila koje se odnose na:

- sva informaciona dobra uključujući I ne ograničavajući se na HW, SW, komunikacije I informacije
- Sve zaposlene u IT,
- korisnike IS
- Spoljnje saradnike i dobavljače (npr. ovlašćene firme koje rade na održavanju sistema, partnere, podizvođače, konsultante i treću stranu)

Cilj Politike informacione bezbednosti Zepter International IT, se odnosi na zaštitu svih informacionih vrednosti u kompaniji.

Informaciona dobra su svako intelektualno I materijalno vlasništvo Odeljenja IT Zepter Internationala, u bilo kojem obliku i na bilo kojem mediju.

Politika informacione bezbednosti definiše I obuhvata sva relevantna dokumenta iz oblasti Sistema upravljanja informacionom bezbednošću. Naglasak je prvenstveno na bezbednosnim procedurama i radnim uputstvima kao i zapisima koji iz njih proističu, pristupu istima i čuvanju.

Odgovornosti

ISMS framework I politika informacione bezbednosti na kojoj je baziran se primenjuje u Odeljenju IT, Zepter International IT, u svim organizacionim jedinicama. Odgovornost za njihovo poštovanje I sprovodjenje imaju svi zaposleni, spoljni saradnici i dobavljači, saglasno definisanom opsegu implementacije ISO 27001.

2. REFERENCE

Referentni standard, dokumenta i regulativa

- ISO/IEC 27000:2018 Vocabulary
- ISO/IEC 27001:2013 Requirements and controls
- Politika informacione bezbednosti
- Interna dokumenta ISMS-a
- Važeća regulative u zemlji a posebno:
    - Zakon o informacionoj bezbednosti
    - Zakon o zaštiti podataka o ličnosti

3. DEO 1 - ISMS standard u Zepter International IT – 1. Deo, zahtevi standarda koji se poštuju

3.4 Kontekst organizacije

Kontekst

Zepter international IT je odredio eksterne i interne relevantne činjenice od značaja za poslovanje kompanije koje su date u misiji, viziji i strategiji kompanije. Ovimokvirom i Politikom informacione bezbednosti definišu se one koje utiču na postizanje očekivanih rezultata sistema bezbednosti informacija kompanije.

Zainteresovane strane

Zeter international IT razume potrebe i očekivanja zaineresovanh strana i to:

- Vlasnika kao i top menadžmenta kompanije Zepter International,
- Države u kojoj posluje i zakonske regulative vezane za informacionu bezbednost a posebno Zakona o zaštiti podataka o ličnosti i GDPR kada se primeni, Zakona o informacionoj bezbednosti,
- Svojih zaposlenih,
- Svojih korisnika,
- Svojih saradnika (dobavljača, konsultanata i na drugi način angažovanih lica),
- Kompanije u okviru Zepter grupe kojima je zajednički ultimate beneficary,
- Zepter partnerske kompanije.

3.4 I 3.5 Uspostavljanje Ciljeva ISMSa I politike Informacione bezbednosti

Zepter International IT je uspostavio globalne I operativne ciljeve ISMS I uveo ISMS kroz implementaciju I primenu pravila I dokumenata ISMS kako je dalje objašnjeno.

Globalni ciljevi Informcione bezbednosti (Goals)i Politike informaciione bezbednosti

U skladu sa vizijom kompanije da obezbedi sigurne i pouzdane tehnologije za podršku poslovnim potrebama, globalni ciljevi za sistem upravljanja bezbednosti informacija su sledeći:

- obezbediti, održavati i zaštititi svu informacijsku imovinu,
- pružiti sigurne, pouzdane i dostupne informacije i okruženje koje podržava poslovne procese,
- kontinuirano praćenje i unapređenje sigurnosti informacija.

Na osnovu pomenutih globalnih ciljeva, Zepter International IT postavlja konkretne operativne ciljeve(objectives), čijim sprovođenjem se postižu pomenuti globalni ciljevi i konstantno unapređuje ISMS.

Top menadžment je utvrdio Politiku informacione bezbednosti koja:

a) odgovara svrsi organizacije;
b) obuhvata ciljeve sigurnosti informacija ili pruža okvir za postavljanje ciljeva informacione bezbednosti;
c) uključuje posvećenost zadovoljavanju primjenjivih zahteva u vezi sa sigurnošću informacija; i
d) uključuje posvećenost stalnom unapređenju sistema za upravljanje bezbednošću informacija.

Politikom informacione bezbednosti obuhvaćeno je široko područje bezbednosnih mera saglasno zahtevima I kontrolama standarda.

Uloga Politike informacione bezbednosti

Primarna uloga Politike informacione bezbednosti je određivanje prihvatljivog i neprihvatljivog načina ponašanja korisnika, zaposlenih i saradnika (dobavljača, konsultanata i na drugi način angažovanih lica) kako bi zaštitili informaciona dobra kompanije. Na osnovu pravila koja su definisane u dokumentu, Politika informacione bezbednosti osigurava tri ključna zahteva po pitanju bezbednosti:

- *Poverljivost (eng. Confidentiality)*

Poverljivost je zaštita podataka I dobara od neovlašćenog pristupa. Ključni faktor poverljivosti je identifikacija korisnika i provera njihove autentičnosti I autorizacije tj prava I nivoa pristupa

- *Integritet (eng. Integrity)*

Integritet predstavlja zaštitu informacija ili dobara asseta od namernog ili slučajnog neovlašćenog menjanja.

- *Dostupnost (eng. Availability)*

Dostupnost je garancija ovlašćenim korisnicima, da će im informacija biti maksimalno moguće raspoloživa u svakom trenutku kad za njom imaju potrebu.

Bezbednost informacionog sistema kompanije

Bezbednost IS može biti ugrožena na više načina pri čemu pretnje možemo podeliti prema izvoru:

- ljudi – namerne pretnje,
- ljudi – nenamerne pretnje,
- oprema - kvarovi i nefunkcionalnost
- neplanirane i prirodne nepogode

Zepter International IT se rukovodio izvorima pretnji kao I statističkim I stručnim podacima vezanim za najčešće uzroke pretnji kada je procenjivan rizik usled pretnji.

Saglasno ovim pretnjama nastaju I najveći rizici pa Zepter International IT, Politikom IB I uvedenim merama I saglasnim procedurama propisuje pravila I kontrole za mitigaciju navedenih rizika kojih su obavezni da se pridržavaju svi počev od korisnika, zaposlenih i saradnika (dobavljača, konsultanata i na drugi način angažovanih lica).

Kako bi se upravljalo rizicima Zepter International IT je uveo edukaciju zaposlenih I informisanje korisnika i saradnika (dobavljača, konsultanata i na drugi način angažovanih lica) u vezi informacione bezbednosti čime se smanjuje verovatnoća njihove greške kojima bi mogli ugroziti integritet i bezbednost IS.

Smeštanjem opreme u kojoj se čuvaju podaci u posebne prostorije, pravilima kojima se određuje pristup opremi, i uvedenom kontrolom pristupa dobrima značajno se smanjuje mogućnost zloupotrebe I narušavanja integriteta.

Iako najređi napadi spolja mogu da uzrokuju najveće štete je rim je cilj pribavlja zloupotreba informacija, njihovo menjanje ili uništavanje te je Zepter Internacional IT uveo niz mera u komunikaciji sa spoljnim svetom I ograničio se objavljivanjem samo neophodnih servisa da budu dostupni spolja čime se postiže nivo bezbednosti, a mogućnost napada svodi se na minimum.

3.5 Liderstvo

Top menadžment pokazuje svoje liderstvo i posvećenost ISMS kroz:

- Obezbedjivanje da je Politika informacione bezbednosti doneta i objavljena i da se implementira u procese organizacije;
- Obezbedjuje da je politika kao i ciljevi je uskladjena sa strategijom kompanije;
- Obezbedjuje resurse i njihovu dostupnost i podstiče ih i podržava da doprinose efektivnosti ISMS;
- Komunicira i podstiče važnost informacione bezbednosti i promoviše kontinuirana unapredjenja prema svim zainteresovanim stranama;
- Obezbedjuje da se postižu ciljevi informacione bezbednosti.

Internim aktima bliže su definisane organizacione uloge, odogovornosti i ovlašćenja u ISMS.

3.6 Planiranje

Rizici

Prilikom planiranja ISMS Zepter internacional IT planira aktivnosti da prepozna rizike i prilike, i kako da ih implementira i preispituje u okviru ISMS i sprovodi procenu rizika koja uključuje kriterijume za prihvatanje rizika, kriterijume procene i obezbedjuje da su rezultati procena uporedivi i konzistentni kao i da su rizici identifikovani kao i njihovi vlasnici, i obavezno da su izvršene analize i finalne provere rezultata procene rizika.

Ciljevi ISMSa

Zepter International IT je u postupku uspostavljanja ciljeva ISMS saglasno funkcijama i poziciji. Ovi ciljevi će biti merljivi i saglasni sa ovom politikom i procedurama. Ciljevi su jasno komunicirani prema svim funkcijama i pozicijama.

3.7 Podrška

Zepter Internaational IT je obezbedio potrebne resurse za ISMS na osnovu definisanih kompetencija. Zepter International IT sprovodi njihovo kontinualno obrazovanje i podizanje nivoa kompetencija koje se dokumentuje.

3.8 Funkcionisanje

Zepter international IT planira aktivnosti vezane za informacionu bezbednost. Kao prvi korak je realizovano uvodjenje ISMS sistema a zatim se fokusira na održavanje i unapredjivanje ISMS kao i planiranje daljeg razvoja.

3.9 Provera sprovodjenja ISMS

Zepter International IT prati, meri, analizira i proverava kako se sprovodi infomaciona bezbednost i efektivnost uvedenog ISMS. Ova aktivnost se vrši kako kroz planirane interne i eksterne audite u redovnim intervalima ili po potrebi, tako i na management review sastancima.

3.10 Kontinuirano unapredjenje

Kada se u sklopu provera ili kroz incidente ili prijavu od strane bilo koje zainteresovane strane ustanovi neusaglašenosti sa ISMS i standardom Zepter international IT odmah regauje odredjujući korektivne aktivnosti da otklanjanje neusaglašenosti i korektivne akcije. Zepter international IT je posvećen konstantnom unapredjenju ISMS, a svaki zaposleni kao i zainteresovane strane su pozvani da doprinese ovom procesu pokretanjem izmena ili inicijativama za unapredjenja.

3. DEO 2 - Primena kontrola standarda u ISMS

U skladu sa zahtevima standarda ISO 27001, Zepter international IT je u Politici IB i ostalim aktima i procedurama, definisao i primenjuje pravila, kontrole i mere i to:

A.5. BEZBEDNOSNE POLITIKE
- A.5.1 Politika informacione bezbednosti

A.6 ORGANIZACIJA INFORMACIONE BEZBEDNOSTI, ULOGE I ODGOVORNOSTI
- A.6.1 Organizacija Informacione bezbednosti

A.6.2 Mobilni uređaji i rad sa udaljenosti
A.7 BEZBEDNOST I LJUDSKI RESURSI
A.7.1 Pre zaposlenja
A7.2 Za vreme zaposlenja
Uloga management
Edukacija
Disciplinski proces
Promena pozicije ili napuštanje kompanije
A.8 UPRAVLJANJE IMOVINOM
A.8.1 Imovina
Popis imovine
Vlasništvo nad imovinom
Dozvoljeno korišćenje informacione imovine
Vraćanje imovine
A.8.2 Klasifikacija informacija
A.8.3 Rukovanje medijima
A.9 KONTROLA PRISTUPA
A.10 KRIPTOGRAFIJA
A.11 FIZIČKA BEZBEDNOST I BEZBEDNOST OKOLINE
A 11.2 Bezbednost opreme
Oprema
Bezbednost instalacija
Bezbednost kod kablova (kabliranja)
Održavanje opreme
Uklanjanje imovine
Obezbeđenje opreme i imovine van prostorija
Bezbedno odlaganje ili ponovno korišćenje opreme
Oprema bez nadzora korisnika
Politika čistog stola i ekrana
A.12 UPRAVLJANJE KOMUNIKACIJAMA I OPERACIJAMA
A.12.1 Procedure za rad i odgovornosti
Menadžment promenama (eng. Change Management)
Razdvajanje okruženja za razvoj, testiranje i operativni rad
A.12.2 Zaštita od malicioznog softvera
A.12.3 Izrada bezbednosnih kopija
A 12.4 Nadzor sistema I logovanje
A.12.5 Sinhronizacija sata
Kontrola operativnog softvera
A.12.6 Menadžment tehničkim ranjivostima
Upravljanje tehničkim ranjivostima
Ograničenja u pogledu instalacije softvera
u pogledu instalacije softvera
A.13 BEZBEDNOST U KOMUNIKACIJAMA
Transfer informacija
A.14 BEZBEDNOST U PROCESIMA NABAVKE, UVODJENJA, RAZVOJA I DRŽAVANJA IS
A.14.1 Zahtevi bezbedosti informaciong sistema
Analiza bezbednosnih zahteva i specifikacija
Obezbeđivanje aplikativnih usluga u javnim mrežama
Zaštita transakcija aplikativnih usluga

A.14.2 Bezbednost u procesima razvoja I podrške
A.14.3 Podaci o testiranju
A.15 ODNOSI SA DOBAVLJAČIMA
A.15.1 Bezbednost informacija u odnosima sa dobavljačima
A.15.2 Upravljanje uslugama koje pruža dobavljač
Lanac isporučilaca u informacionim i komunikacionim tehnologijama
Ugovor o poverljivosti
Isporuka usluge treće strane
Nadzor, preispitivanje usluga treće strane i upravljanje promenama
A.16 UPRAVLJANJE BEZBEDNOSNIM INCIDENTIMA IS
Prijava bezbednosnih incidenata I sumnji I ranjivosti
Upravljanje bezbednosnim incidentima i poboljšanja
A.17 UPRAVLJANJE KONTINUITETOM POSLOVANJA SA ASPEKTA INFORMACIONE BEZBEDNOSTI
A.17.1 Planiranje kontinuiteta bezbednosti informacija
Kontinuitet poslovanja i procena ritika
A.17.2 Redundanse
A.18 USKLAĐENOST
A.18.1 Uskladjenost sa propisima I ugovornim obavezama
Identifikacija primenljivih zakona
Intelektualno vlasništvo – autorska prava
Zaštita podataka i i privatnost ličnih podataka
Poštovanje ostalih ugovornih obaveza vezano za informacionu bezbednost
Čuvanje zapisa
Kriptografske kontrole
A.18.2 Preispitivanje bezbednosti informacija

4. ZAPISI BAZIRANI NA OVOM DOKUMENTU

Naziv I oznaka	***Retention time***
Dopisi saradnicima sa informacijom o uspostavljanju ISMS I Okviru ISMS u slobodnoj formi	Čuvaju se saglasno dužini čuvanja ugovora sa saradnicima

5. VALIDNOST

Ovaj dokument je validan od jula 2018.

Odobreno, u skladu sa R_14_1_2018_11.07.2018_Management review meeting Izvestajem.

Ovaj document se objavljuje na zvaničnom web site kompanije.