IT4biz
FULLY MANAGED IT

ISMS-POL-ISMS: Politika ISMS

Verzija 2.0

ZA JAVNU UPOTREBU

ISMS dokumentacija

Kontrola dokumenta

	Datum	Osoba	Funkcija
Predlog	06.06.2017.	Stanislava Cvetković	Predstavnik rukovodstva
Overa	07.06.2017.	Ljubiša Radivojević	Direktor
Odobrenje	07.06.2017.	Ljubiša Radivojević	Direktor

Revizija dokumenta

Verzija	Datum	Izmenio	Napomena
1.0	06.06.2017.	Stanislava Cvetković	Prva verzija
2.0	13.03.2018.	Tanja Tanasković	Izmena lokacije ISMS dokumentacije

Sadržaj

ISMS-POL-ISMS: Politika ISMS

Verzija 2.0

Namena

Predmet ove politike je da najviše rukovodstvo kompanije IT4biz d.o.o. (u daljem tekstu Kompanije) pokaže liderstvo i svoju posvećenost sistemu upravljanja bezbednošću informacija (ISMS) tako što:

- obezbeđuje uspostavljanje politike i ciljeva bezbednosti informacija, kao svog strateškog opredeljenja;
- obezbeđuje integraciju zahteva za sistem upravljanja bezbednošću informacija u procese Kompanije;
- obezbeđuje raspoloživost neophodnih resursa za potrebe ISMS;
- ukazuje na važnost efektivnog upravljanja bezbednošću informacija;
- promoviše stalno poboljšanje i
- usmerava operativno rukovodstvo Kompanije u pogledu njihove odgovornost u procesima upravljanja bezbednošću informacija;
- usmerava i podiže svest zaposlenih da daju doprinos efektivnosti ISMS.

Ciljevi ISMS-a Kompanije su:

- Zaštita informacija od neovlašćenog pristupa
- Zaštita resursa organizacije od neovlašćenog pristupa, nenamenskog korišćenja i zloupotrebe
- Održavanje poverljivosti informacija
- Zaštita integriteta informacija kroz zaštitu od neovlašćenog pristupa i izmena
- Očuvanje dostupnosti informacija za ovlašćena lica
- Usaglašenost sa zakonskim i ugovornim obavezama
- Dokumentovanje i istraživanje događaja i incidenata vezanih za sigurnost informacija
- Visok nivo svesti o potrebi zaštite informacija i resursa u organizaciji
- Konstantno unapređenje ISMS-a

Oblast primene

Ova Politika ISMS se primenjuje u svim poslovnim funkcijama Kompanije, od strane svih zaposlenih.

Veza sa drugim dokumentima

- ISO 9001:2015;
- ISO/IEC 27001:2013;
- Sva pravila ISMS

Uloge i odgovornosti

Direktor za ISMS je odgovoran za definisanje Politike i ciljeva bezbednosti informacija i odobravanje ove Politike ISMS. Za svoj rad odgovoran je Vlasniku firme.

Predstavnik rukovodstva za ISMS je odgovoran za dostupnost ove Politike ISMS i komponentne politike na koja se ova Politika ISMS poziva. Za svoj rad odgovoran je Direktoru.

Rukovodioci funkcija, kao vlasnici procesa, su odgovorni za sprovođenje ove Politike ISMS i komponentnih politika bezbednosti informacija na koja se ona poziva. Za svoj rad su odgovorni Direktoru.

Rukovodstvo organizacije je posvećeno ISMS-u i obezbediće da ova Politika bude distribuirana i objašnjena svim zaposlenima i zainteresovanim stranama, implementirana u celoj organizaciji i redovno revidirana kako bi se kontinuirano proveravala njena prikladnost.

Zaposleni su dužni da se pridržavaju pravila i ispunjavaju zahteve koji su definisani ovom Politikom i svom drugom dokumentacijom ISMS-a.

Outsource Organizacije su takođe dužne da se pridržavaju pravila i ispunjavaju zahteve koji su definisani ovom Politikom i svom dokumentacijom ISMS. Obaveze I odgovornosti u pogledu bezbednosti informacija se definišu ugovornih odnosom sa outsource organizacijama.

Opis politike

Principi

Najviše rukovodstvo Kompanije je uspostavilo ovu Politiku upravljanja bezbednošću informacija koja:

- odgovara svrsi organizacije i njenoj poslovnoj strategiji;
- obuhvata ciljeve bezbednosti informacija ili daje okvir za utvrđivanje ciljeva bezbednosti informacija;
- uključuje obavezu da zadovolji odgovarajuće zahteve koji se odnose na bezbednost informacija;
- uključuje posvećenost stalnom poboljšanju ISMS.

Ova Politika daje smernice podrške za upravljanje bezbednošću informacija, u skladu sa postavljenim zahtevima organizacije i relevantnim zakonskim, regulatornim i ugovorenim zahtevima. Ona je:

- na raspolaganju kao dokumentovana informacija;
- saopštena u svim organizacionim delovima Kompanije u kojima je implementiran ISMS;
- raspoloživa zainteresovanim stranama prema ukazanoj potrebi.

Ciljevi bezbednosti informacija i planovi za njihovo postizanje

Kompanija je uspostavila principe za definisanje i dokumentovanje svojih ciljeva bezbednosti informacija na relevantnim funkcijama i nivoima. Ti ciljevi:

- su u skladu sa ovom Politikom ISMS i komponentnim politikama na koju se ova politika poziva;
- merljivi (kad je to moguće);
- uzimaju u obzir važeće primenljive zahteve za bezbednost informacija, kao i rezultate procene i tretmana rizika;
- se saopštavaju;
- se ažuriraju prema potrebi.

Prilikom planiranja načina postizanja svojih ciljeva bezbednosti informacija organizacija utvrđuje:

- šta će biti urađeno;
- koji resursi će biti potrebni;
- ko će biti odgovoran;
- kad će biti realizovani;
- da se ažuriraju prema potrebi;
- kako će se rezultati ispunjenih ciljeva proceniti.

Organizacija čuva dokumentovane informacije o ciljevima bezbednosti informacija.

Upravljanje bezbednošću informacija

Bezbednost informacija i procesi podrške imaju presudni značaj za održanje poslovnog sistema organizacije, finansijskih i komercijalnih tokova, pravne usklađenosti i poslovnog ugleda. Informacije, koje se u organizaciji javljaju u različitim oblicima (štampane, pisane, arhivirane u elektronskom obliku i sl.), predstavljaju imovinu koja je od suštinskog značaja za poslovanje Kompanije. U kom god obliku da se informacije nalaze, uvek se na odgovarajući način štitite od mnoštva pretnji i ranjivosti.

Upravljanje bezbednošću informacija predstavlja zaštitu od svih pretnji na način koji obezbeđuje kontinuitet poslovanja i svođenja rizika na najmanju moguću meru.

Komponentne politike bezbednosti informacija, gde je to potrebno, pozivaju na dokumentovane procedure, uputstva, organizacionu strukturu, softverske i hardverske funkcije. Ciljevi kontrola i kontrole su uspostavljene u sprezi sa svim procesima upravljanja poslovanjem organizacije. Kontrole se permanentno preispituju, u cilju ispunjavanja zahteva bezbednosti informacija.

Ovom Politikom i njenim komponentnim politikama, Informacioni sistem i mreža organizacije se stavlja pod stalnu kontrolu upravljanja bezbednošću informacija.

Bezbednost informacija, kao i zaštita kritičnih infrastruktura organizacije, podjednako je važna u svim njenim funkcijama. Upravljanje bezbednošću informacija funkcioniše kao mehanizam koji omogućava potpunu kontrolu pristupa koja obezbeđuje isključivanje ili umanjivanje svih rizika po bezbednost informacija. Međusobno povezivanje mreže organizacije i javne mreže, kao i zajedničko korišćenje informacionih resursa otežava ostvarivanje kontrole pristupa. Distribuirani rad računara slabi efikasnost kontrole pristupa.
Bezbednost informacija koja se ostvaruje tehničkim sredstvima je ograničena, pa iz tih razloga ona mora biti podržana odgovarajućim upravljanjem propisanim dokumentovanim komponentnim politikama, procedurama i uputstvima za sve zaposlene i isporučioce koji su uključeni u procese Kompanije.

Uspostavljanje zahteva za bezbednost

Kompanija je identifikovala svoje suštinske zahteve za bezbednost informacija. Utvrdio je tri glavna izvora zahteva:

- Procenjivanje rizika, uzimajući u obzir ukupnu poslovnu strategiju i njene ciljeve, prema proceduri SPR.6.1.2 Ocenjivanje rizika po bezbednost informacija i postupanje sa rizikom, identifikuju se pretnje po imovinu, vrednuju se ranjivosti i verovatnoća njihovog pojavljivanja i predviđaju se moguće posledice.
- Relevantni zakonski, regulatorni i ugovorni zahtevi koje Kompanija i njeni isporučioci moraju da ispune.
- Poseban skup principa, ciljeva i poslovnih zahteva za obradu informacija koje je organizacija razvila za podršku svog rada u okviru svog sistema upravljanja kvalitetom (QMS).

Ocenjivanje rizika po bezbednost

Zahtevi za bezbednost informacija se identifikuju prema pomenutoj proceduri. Troškovi kontrola su u ravnoteži sa štetom u poslovanju koja bi mogla nastati kao rezultat otkaza bezbednosti.
Rezultati ocenjivanja rizika uslovljavaju primenu procesa tretmana rizika koji se sprovodi na bazi plana: Plan tretmana rizika. Prihvatanje preostalog rizika je u ravnoteži sa troškovima daljeg smanjenja rizika.
Rezultati ocenjivanja i tretmana rizika omogućavaju utvrđivanje i uvođenje dodatnih kontrola za zaštitu od rizika i odgovarajućih akcija prioriteta kod upravljanja preostalog rizika po bezbednost informacija.

Ocenjivanje rizika se ponavlja periodično kako bi se obuhvatile izmene koje mogu uticati na rezultate ocenjivanja rizika.

Izvor kontrola

Izvršenom GAP analizom je utvrđen relativno visok nivo zrelosti pozitivne prakse upravljanja bezbednošću informacija u Kompaniji. Međutim, procenjeni nivo zrelosti nije dovoljan za usaglašenost sistema upravljanja bezbednošću informacija sa zahtevima međunarodnog standarda ISO/IEC 27001:2013. Neusaglašenosti utvrđene GAP analizom koje se moraju otkloniti se odnose na uvođenje obaveznih kontrola koje zahteva pomenuti standard koje se dalje moraju permanentno primenjivati i njihova primena dokumentovati.
Kompanija je uspostavila odgovarajući okvir za postavljanje ciljeva kontrola i samih kontrola, uključujući identifikaciju i ocenjivanje rizika, kao i upravljanje tretmanom rizika, kako bi se obezbedilo da se rizici potpuno isključe ili smanje na prihvatljiv nivo.
Kontrole se uvode na osnovu dokumentovanih komponentnih politika, procedura i uputstava koje propisuje i odobrava rukovodstvo Kompanije. One se zasnivaju na kriterijumima za prihvatljivost rizika, opcijama postupanja sa rizicima, kao i na opštem pristupu upravljanju rizicima koji organizacija primenjuje prema odgovarajućim zakonskim zahtevima.
Sve kontrole sigurnosti informacija su podržane komponentnim politikama, koje strukturirano daju odgovore na potrebe određenih ciljnih grupa organizacije, kao što su:

- Kontrole pristupa;
- Klasifikacija informacija;
- Fizičko obezbeđenje;
- Odgovornost za sredstva;
- Sigurnost komunikacija;
- Korišćenje mobilnih uređaja;
- Odnos sa spoljnim saradnicima (outsource)
- Odnos sa isporučiocima.

Sve komponentne politike su saopštene zaposlenima, spoljnim saradnicima i isporučiocima u obliku koji je relevantan, dostupan i razumljiv njihovim korisnicima.
U zavisnosti od domena primene, komponenetne politike za upravljanje bezbednošću informacija definisane su kao pojedinačna dokumenta za specifične kontrole koje se primenjuju u specifičnim organizacionim funkcijama kao što je informaciona tehnologija (IT), ili kao zbirni dokument za više poltika kao što je komponentna politika za bezbednost ljudskih resursa, koja se primenjuju u svim organizacionim funkcijama Kompanije.

Izrada komponentnih politika, procedura i uputstava

Pozitivna praksa organizacije predstavlja polaznu osnovu za izradu komponentnih politika, procedura, uputstava, zapisa koji dokumentuju primenu kontrola i zahteva za usklađenost koji su od posebnog značaja za Kompaniju, uključujući:

- usklađenost sa zakonskim, regulatornim i ugovornim zahtevima;
- zahteve za obrazovanjem, obukom i podizanjem svesti iz domena bezbednosti;
- upravljanje kontinuitetom poslovanja;
- posledice kršenja politike bezbednosti.

Komponentne politike upravljanja bezbednosti informacija obezbeđuju podršku upravne strukture. Ona su:

- u skladu sa ovom politikom i laka za razumevanje,
- usklađena sa kulturom rada i okruženjem,
- racionalna i omogućavaju postizanje poslovnih ciljeva,
- obavezna i zahtevaju realizaciju,
- afirmativna i ističu šta treba uraditi (*treba, mora,..*),

- važeća za sve klase informacija, opremu i mreže
- uravnotežena sa nivoom kontrola zaštite i nivoom efektivnosti,
- prilagođena veličini organizacije.
- saopštena i ukazuju šta treba da zaštite i u kom obimu,
- sadrže informaciju na koga se odnose,
- sadrže razloge za propisivanje i ko ih je propisao,
- objašnjavaju kako će biti sprovedena i ko je odgovoran za to,
- definišu koja su odstupanja dopuštena,
- definišu i identifikuju neophodne informacije za izveštavanje o incidentu.

Komponente politike upravljanja sigurnosti informacija su:

ISMS-POL-REMOTE	Politika udaljenog pristupa
ISMS-POL-EMP	Politika bezbednosnih mera za zaposlene
ISMS-POL-SENS	Politika klasifikacije i zaštite informacija
ISMS-POL-MED	Politika rashodovanja medijuma (politika rashodovanja i uništavanja)
ISMS-POL-ACCCTRL	Politika kontrole pristupa
ISMS-POL-PWD	Politika izbora i korišćenja lozinki
ISMS-POL-CRYPTO	Politika odabira kriptografskih metoda
ISMS-POL-PHY	Politika kontrole fizičkog pristupa
ISMS-POL-HW	Politika upravljanja hardverom
ISMS-POL-CLEAN	Politika čistog stola
ISMS-POL-ACCNT	Politika upotrebe naloga
ISMS-POL-AUSE	Politika prihvatljivog korišćenja računara
ISMS-POL-CHANGE	Politika upravljanja i kontrole promena
ISMS-POL-MAL	Politika zaštite od malicioznog softvera
ISMS-POL-BCK	Politika pravljenja sigurnosnih kopija podataka (BackUp)
ISMS-POL-SW	Politika upravljanja softverom
ISMS-POL-NETCTRL	Politika kontrole pristupa računarskoj mreži
ISMS-POL-INFO	Politika prenosa informacija
ISMS-POL-EMAIL	Politika upotrebe elektronske pošte
ISMS-POL-PROGRESS	Politika sigurnosti razvoja i podrške
ISMS-POL-BCP	Politika upravljanja kontinuitetom poslovanja
ISMS-POL-OUTSRC	Politika odnosa sa isporučiocima

Navedeni set komponentnih politika bezbednosti informacija je definisan, odobren od strane direktora, objavljen i saopšten zaposlenima i relevantnim eksternim stranama. Tamo gde je potrebno, ove komponenetne politike se pozivaju na relevantne procedure i uputstva za primenu.

Preispitivanje politike bezbednosti informacija

Najviše rukovodstvo organizacije preispituje ovu Politiku ISMS i komponentne politike bezbednosti informacija na koja se ona poziva, u planiranim intervalima (najmanje jednom godišnje), ili vanredno u slučaju pojave značajne promene uslova bezbednosti informacija, kako bi se obezbedila njena stalna pogodnost, adekvatnost i efektivnost, kao i potrebni postupci za njenu primenu.
Politika ISMS i komponenetne politike bezbednosti informacija imaju svoje vlasnike koji imaju potvrđenu rukovodnu odgovornost za razvoj, preispitivanje, procenu mogućnosti za poboljšanje i vrednovanje.

Preispitivanje Politike ISMS i komponentnih politika upravljanja bezbednošću informacija uključuje njihovo stalno poboljšanje, kao odgovore na promene organizacionog okruženja, poslovnih okolnosti, zakonskih i regulatornih zahteva, ili tehničkog okruženja.
Preispitivanje politike i komponentnih politika bezbednosti informacija odvija se prema postupku preispitivanja od strane menadžmenta tokom interne provere.

Važenje i upravljanje dokumentom

Ovaj dokument važi od 07.06.2017.

Vlasnik ovog dokumenta je direktor, koji mora proveravati i ako je potrebno, ažurirati ovaj dokument najmanje jednom godišnje.
Za evaluaciju efikasnosti i adekvatnosti ovog dokumenta moraju se razmotriti sledeći kriterijumi:

- broj incidenata koji se desio zbog nejasnih definicija unutar ove Politike
- broj korektivnih akcija koje su preduzete zbog nejasnih definicija unutar ove Politike

Zapisi i obrasci

Naziv dokumenta	Odgovorna osoba	Period čuvanja	Lokacija
Izjava rukovodstva o prihvatanju politike bezbednosti informacija	Stanislava Cvetković	3 godine	https://it4bizdoo-my.sharepoint.com/