SAGA d.o.o. Beograd je preduzeće čija je oblast rada vezana za proizvode i usluge na bazi informacionih i telekomunikacionih tehnologija iz domena infrastrukture, tehnoloških servisa i rešenja.

Najviše rukovodstvo preduzeća je svesno svoje odgovornosti za obezbeđivanje visokog kvaliteta u svim segmentima poslovanja, a to manifestuje i kroz uspostavljanje sistema menadžmenta IT servisa i sistema menadžmenta bezbednosti informacija u cilju očuvanja kvaliteta nivoa podrške poslovnih ciljeva i procesa, a u skladu sa propisima i zahtevima standarda ISO 20000-1 i ISO 27001.

Bezbednost informacija je jedna od osnovnih vrednosti organizacije, imajući u vidu da su bezbednost informacija i očuvanje osnovnih bezbednosnih principa poverljivosti, integriteta i raspoloživosti kritični za operacije organizacije.
Uspostavljanjem, implementacijom i primenom, praćenjem i preispitivanjem, održavanjem i stalnim poboljšavanjem sistema menadžmenta IT servisa i bezbednosti informacija, teži se poboljšanju kvaliteta IT servisa, povećanju zadovoljstva zainteresovanih strana, umanjenju troškova, boljem iskorišćenju resursa, poboljšanju svesti o prirodi važnosti i značaju očuvanja bezbednosti informacija, upravljanju rizicima narušavanja kvaliteta IT servisa i kompromitacije bezbednosti informacija kroz detekciju ranjivosti i opasnosti i preduzimanju mera u cilju smanjenja nivoa rizika.

Ovom Politikom organizacija izražava spremnost i obavezu održavanja i stalnog unapređenja sistema menadžmenta IT servisa i bezbednosti informacija. Stalno unapređenje predstavlja pronalaženje malih poboljšanja u procesima i proizvodima sa ciljem povećanja kvaliteta i smanjenja gubitaka, kroz definisane ciljeve:

- obezbediti sigurno okruženje za ostvarenje poslovnih ciljeva,
- minimalizovati rizike po pitanju informacione bezbednosti i kontinuiteta poslovanja,
- unaprediti porfolio security usluga i servisa,
- održati reputacioni ugled i zadržati lidersku poziciju Sage u oblastima informacione bezbednosti.

Uspostavljanje procesa stalnog unapređenja u Sagi nastalo je kao potreba da se osigura kontinuitet pokušaja poboljšanja proizvoda, usluga i procesa što podrazumeva sistemsko i neprekidno traganje za izvrsnošću procesa i operacija i stalnu potrebu za novim idejama, aktivnostima i inicijativama, kao i primenu kontrola po oblastima svih sistema upravljanja uspostavljenih u organizaciji.

- Oblasti upravljanja IT servisima prema standardu ISO 20000-1:2011:
  1. Planiranje i implementacija novog i izmenjenog servisa
  2. Isporuka servisa
  3. Komunikacije i veze
  4. Razrešenje incidenata i problema
  5. Kontrole
  6. Prihvatanje novih verzija

- Oblasti upravljanja bezbednošću informacija prema standardu ISO 27001:2013:
  1. A5 Politike bezbednosti informacija
  2. A6 Organizovanje bezbednosti informacija
  3. A7 Bezbednost ljudskih resursa
  4. A8 Menadžment informacionom imovinom
  5. A9 Kontrola pristupa
  6. A10 Kriptografija
  7. A11 Fizička bezbednost i bezbednost u okruženju
  8. A12 Bezbednost funkcionisanja
  9. A13 Bezbednost komunikacija
  10. A14 Nabavka, razvoj i održavanje sistema
  11. A15 Odnosi sa isporučiocima
  12. A16 Menadžment incidentima narušavanja bezbednosti informacija,
  13. A17 Aspekti bezbednosti informacija kod menadžmenta kontinuitetom poslovanja,
  14. A18 Usklađenost

Uspešnost celokupnog sistema upravljanja IT servisima i bezbednošću informacija se ostvaruje kroz realizaciju sledećih usvojenih principa u organizaciji:

1. Ustanovljavanje opsega i definisanje pod-politika u skladu sa Politikom IT servisa i bezbednosti informacija, važećim zakonima, propisima i kontrolama bezbednosti informacija organizacije i informacione opreme kojoj eksterne strane pristupaju;
2. Poštovanje, sprovođenje i usklađivanje sistema sa međunarodnim i domaćim zakonskim propisima i regulativom, statutarnim ili ugovornim obavezama, kao i bilo kojim zahtevima za bezbednost;
3. Usaglašavanje procesa rada sa zahtevima odgovarajućih standarda, unapređenje procesa i organizacije rada i kontinuirano unapređenje efektivnosti i efikasnosti sistema menadžmenta;
4. Odgovorno upravljanje i prihvatljivo korišćenje informacione imovine kroz dodelu vlasništva i klasifikovanje informacija prema definisanim kriterijumima, u cilju osiguranja odgovarajućeg nivoa zaštite za informacije;
5. Detektovanje ciljeva i uspostavljanje procesa bezbednosti ljudskih resursa kroz definisanje sistema pravila ponašanja koja obavezuju zaposlene, ugovarače i korisnika treće strane na način da svi subjekti razumeju i prihvate svoje odgovornosti i uloge u vezi bezbednosti informacija u svim fazama pre, u toku i kod prestanka ili promene radnog angažovanja u organizaciji;
6. Upravljanje fizičkom bezbednošću oblasti i opreme radi sprečavanja prekida poslovanja organizacije, tj. sprečavanje neovlašćenog pristupa, oštećenja i ometanja u prostorijama i na informacijama organizacije, ili sprečavanje gubitka, oštećenja, krađe ili kompromitovanja imovine;
7. Uspostavljanje upravljanja rezervnim kopijama počev od određivanja informacija koje se čuvaju, definisanja učestanosti izrade u zavisnosti od klasifikacije informacija, testiranja, restauracije informacija do ispravne manipulacije medijumima za čuvanje rezervnih kopija;
8. Uspostavljanje sistema pravila ponašanja i kontrola za razmenu datoteka i softvera preko spoljne mreže s ciljem uklanjanja rizika izloženosti unosa malicioznog i neautorizovanog softvera;
9. Propisivanje pravila sigurnosti rada mobilnog koda i organizacionih pravila zaštite kao prevencije za detektovanje i uklanjanje malicioznog koda;
10. Propisivanje opsega korišćenja i razmene informacija kroz definisanje autorizovanih korisnika za korišćenje određene grupe ili cele klase informacija, i upoznavanje zaposlenih o pravima vlasništva nad informacijama organizacije;
11. Definisanje pravila o zabrani instalacije i korišćenja neautorizovanog softvera na uređajima koji pristupaju IT infrastrukturi organizacije, nezavisno da li su uređaji u vlasništvu preduzeća ili ne;
12. Upravljanje rizicima od neautorizovanog pristupa i posledično narušavanja integriteta i poverljivosti informacija kroz sistem kontrolnih mehanizama, kojima se vrši verifikacija korisnika na sistemu, autorizacija za obavljanje određenih zadataka i ostvaruje neporecivost preuzimanja odgovornosti za izvršenu akciju nad informacionom imovinom;
13. Uspostavljanje razgranate kontrole pristupa po svim nivoima IT infrastrukture, od poslovnih aplikacija, alata, operativnih sistema i drugog sistemskog softvera, mreže i mrežnih resursa, sve do posebno osetljivih mobilnih uređaja i mobilne infrastrukture i rada na daljinu;
14. Integrisanje zahteva za bezbednost informacija u životni ciklus informacionog sistema i medijuma nosilaca informacije, uz korišćenje naprednih tehnika kriptografije i uz postojanje sistema pravila o korišćenju kontrola za sve informacije koje organizacija klasifikuje kao poverljive i tajne uz upravljanje tehničkim ranjivostima;
15. Zaštita i tajnost informacija primenom bezbednosnih principa uključujući ponašanje, organizacione postupke i primenjene tehnološke metode u skladu sa definisanom bezbednosnom kategorijom kojoj informacija pripada, a u cilju sprečavanja rizika od neautorzovanog objavljivanja, obrade ili pristupa podacima;
16. Korišćenje proizvoda i sredstava, koji predstavljaju vlasništvo, u skladu sa zakonskim i drugim propisima i ugovornim zahtevima, u smislu prava intelektualne svojine;

17. Raspolaganje i prenošenje softvera drugima preko pravila iz domena sistematskog pristupa razvoju softvera za eksterne klijente, a u skladu sa politikom intelektualne svojine u smislu licenciranja softvera;
18. Upravljanje incidentima narušavanja bezbednosti informacija sa stanovišta prepoznavanja incidenata i uspostavljanja postupaka za blagovremeni i adekvatan odgovor na incidente, planovi za njihovo otklanjanje, izveštavanje o događajima u vezi sa bezbednošću informacija i slabostima, preduzete akcije praćenja incidenata i poboljšavanja;
19. Upravljanje kontinuitetom poslovanja kao meri odgovora u slučaju katastrofe, uz kreiranje plana oporavka aktivnosti sa definisanim timom i odgovornostima za incidentne situacije i obavezama testiranja i preduzimanja akcija posle svakog neželjenog događaja sa integrisanim postupcima za očuvanje bezbednosti informacija u nepredviđenim okolnostima;
20. Redovno osposobljavanje i motivisanje zaposlenih za kvalitetno obavljanje poslova iz domena IT servisa i bezbednosti informacija i podizanje svesti i ohrabrivanje zaposlenih sa ciljem da preventivno deluju, menjaju navike i uključe se u nastojanja organizacije da poboljša svoj učinak;
21. Uspostavljanje saradnje i održavanje efikasne komunikacije sa svim zainteresovanim stranama u cilju unapređivanja korporativne odgovornosti i bolje razmene informacija važnih za IT servise i bezbednost informacija;
22. Periodično preispitivanje sistema menadžmenta IT servisa i bezbednosti informacija u svrhu procene da li se primenjuju u potpunosti i da li su pogodni za ostvarivanje politika, ciljeva i strategija iz ovih oblasti sa ciljem ostvarenja održivog uspeha i poslovne izvrsnosti.

Ova Politika je prihvaćena od strane najvišeg rukovodstva i obavezujuća je za sve zaposlene u organizaciji kao i sve angažovane podizvođače i konsultante na projektima koji su odgovorni za njenu primenu. Politika se primenjuje integrisano sa Politikom sistema menadžmenta kvalitetom, kao i ostalim politikama u organizaciji.

Politika u potpunosti podržava viziju organizacije kao odgovorne IT kompanije. Organizacija se obavezuje da poštuje navedene bezbednosne i organizacione principe, kako unutar nje, tako i prilikom pružanja IT usluge eksternim korisnicima, a sve u skladu sa važećom zakonskom regulativom i zahtevima odgovarajućih standarda.

Direktor