Primena politike bezbednosti informacija i privatnosti, IT usluga i kontinuiteta poslovanja za cilj ima kontrolisan i bezbedan pristup dokumentima, informacijama i prostorijama, kako zaposlenim licima tako i korisnicima usluga i proizvoda privrednog društva Saga d.o.o. Beograd (u daljem tekstu Saga). Predmet i područje primene se odnosi na oblast rada vezanu za projektovanje i izvođenje radova telekomunikacionih mreža i sistema, proizvode i usluge na bazi informacionih tehnologija iz domena infrastrukture, tehnoloških servisa i rešenja. Svrha politike je da zaštiti informacije kao vrednu imovinu preduzeća od svih internih, eksternih, slučajnih ili namernih pretnji i ukaže na mogućnosti procesa za kontrolu organizacionih aktivnosti i resursa sa ciljem unapređenja i rasta vrednosti usluge, kao i da omogući funkcionisanje kompanije u predefinsanim kapacitetima tokom eventualnog poremećaja usled katastrofe

Bezbednost informacijaje jedna od osnovnih vrednosti organizacije, imajući u vidu da su bezbednost informacija i privatnosti, kao i očuvanje osnovnih bezbednosnih principa poverljivosti, integriteta i raspoloživosti kritični za operacije organizacije i u direktnoj su korelaciji sa strategijom preduzeća. Organizacijski pristup u upravljanju ciljevima Saga realizuje i usklađivanjem sa aktuelnim propisma i zakonima, zahtevima zainteresovanih strana, trenutnim i predviđenim pretnjama okruženja po bezbednost inforamacija i privatnosti. Svaki podatak nastao na informacionom sistemu preduzeća smatra se vlasništvom preduzeća.

Uspostavljanjem, implementacijom i primenom, praćenjem i preispitivanjem, održavanjem i stalnim unapređenjem sistema menadžmenta i teži se poboljšanju kvaliteta usluga, povećanju zadovoljstva zainteresovanih strana, umanjenju troškova, boljem iskorišćenju resursa, povećanju nivoa svesti o prirodi važnosti i značaju očuvanja bezbednosti informacija, upravljanju rizicima narušavanja kvaliteta IT usluga i kompromitacije bezbednosti informacija kroz detekciju ranjivosti i opasnosti i preduzimanju mera u cilju smanjenja nivoa rizika.

Najviše rukovodstvo preduzeća Saga je svesno svoje odgovornosti za obezbeđivanje visokog kvaliteta u svim segmentima poslovanja i to manifestuje i kroz uspostavljanje sistema menadžmenta usluga i sistema menadžmenta bezbednosti informacija i privatnosti u cilju očuvanja kvaliteta nivoa podrške poslovnih ciljeva i procesa, kao i kroz dodeljivanje odgovornosti kroz jasno definisane uloge. Politika bezbednosti informacija i privatnosti, IT usluge i kontinuiteta poslovanja je usaglašena sa propisima i zahtevima serije standarda ISO 20000-1, ISO 27001 i ISO 27701, ali služi i kao mera odgovora u slučaju vanrednih situacija, uključujući i katastrofe u skladu sa zahtevima standarda ISO 22301. Svi principi informacione bezbednosti se odnose i na bezbednost i zaštitu podataka o ličnosti koji su podskup informacione bezbednosti.Najviše rukovodstvo je fokusirano na dobrobit svakog pojedinca u celokupnom poslovanju, gde je lična sigurnost zaposlenih najveći prioritet. Kompanije Saga je takođe svesna da je zaštita ličnih podataka jedno od temeljnih ljudskih prava i preduzima sve mere kako bi osigurala da i svi njeni zaposleni ozbiljno shvataju privatnost podataka.

Najviše rukovodstvo uspostavlja ovu politiku tako da:

- odgovara svrsi Sage
- obezbeđuje okvir za postavljanje ciljeva
- uključuje posvećenost zadovoljavanju primenljivih zahteva i stalnom poboljšanju

Ovom Politikom organizacija izražava spremnost i obavezu stalnog unapređenja sistema menadžmenta kroz unapređenja u procesima i proizvodima sa ciljem povećanja kvaliteta i smanjenja gubitaka, uz definisane ciljeve kroz:

- obezbeđenja sigurnog okruženje za ostvarenje poslovnih ciljeva,
- minimalizovanje rizike po pitanju informacione bezbednosti i privatnosti, kao i kontinuiteta poslovanja,
- unapredeđenje porfolia security usluga i servisa,
- održavanje reputacionog ugleda i zadržanja liderske pozicije Sage u oblastima informacione bezbednosti.

Uspešnost celokupnog sistema upravljanja ITuslugama i bezbednošću informacija, se postiže realizacijom usvojenih principa za rukovanjem svim aktivnostima koje se odnose na bezbednost informacija i privatnosti organizacije, kroz ustanovljen opseg i implemtirane kontrole definisanih pod-politika u skladu sa važećim zakonima i propisima. Redovno osposobljavanje i motivisanje zaposlenih za kvalitetno obavljanje poslova iz domena IT servisa, bezbednosti informacija i privatnosti, kao i kontinuitata poslovanja, ima za cilj podizanje svesti i ohrabrivanje zaposlenih da preventivno deluju, menjaju navike i uključe se u nastojanja organizacije da poboljša svoj učinak.U cilju sprovođanja permanentnog informisanja o osnovama bezbednosti kao i informisanja o vanrednim događajima, uspostavljena je Log'on polisa sa ciljem da se zaposleni pravovremeno informišu o svojim osnovnim odgovornostima i obavezama.

Okvir upravljanja kontinuitetom poslovanja jasno definiše postupke i određuje timove za vanredne situacije, kao i odgovornosti za aktivnosti navedene u planovima. Aktivnosti okvira upravljanja kontinuitetom poslovanja obavezuju na kreiranje Plana kontinuiteta poslovanja i Plana oporavka aktivnosti u slučaju katastrofe. Odgovor na incidente podrazumeva preduzimanje akcija od strane nadležnih osoba na način koji demonstrira odgovorno komandovanje i kontrolu u vreme kriznih situacija.

Postupci planiranja kontinuiteta poslovanja, kao i oporavka aktivnosti u slučaju incidenata, zasnovani su na izvršenoj analizi uticaja na poslovanje, s posebnim naglaskom na:

- Identifikaciju kritičnih poslovnih procesa, resursa i servisa
- Proceni svih identifikovanih rizika, određivanju prihvatljivog nivoa rizika i planskog tretiranja rizika;
- Kreiranje i održavanje rezervnih kopija i sinhronizacije podataka između primarnog i rezervnog centra na način kako je DRP planom određeno;
- Usvajanje detaljnih Planova oporavka i utvrđivanje odgovornosti za njihovo sprovođenje;
- Usklađivanje sa zakonskom regulativom, ugovornim obavezama i očekivanjima svih zainteresovanih strana;
- Intezivno komuniciranje sa svim zainteresovanim stranama.

Okvir upravljanja kontinuitetom poslovanja organizacije Saga jasno definiše postupke i timove, odnosno odgovornosti u slučaju nastupanja kriznih situacija na osnovu definisanih Planova oporavka. Odgovor na poremećaje i katastrofe podrazumeva preduzimanje akcija na način koji demonstrira odgovorno komandovanje i kontrolu u vreme kriznih situacija.

Organizacija sprovodi obuke s ciljem obezbeđenja da svi zaposleni budu upoznati sa svojim ulogama i odgovornostima u slučaju nastupanja vanrednih situacija. Organizacija preduzima preispitivanje i gde je predviđeno i testiranje planova i podržavajućih dokumenata najmanje jednom godišnje i usklađuje ih sa svim promenama u poslovanju, tehnologiji, okruženju ili izmenama koje treba sprovesti u skladu sa rezultatima testiranja, kao i posle svakog neželjenog događaja ili krupnih promena, a u cilju poboljšavanja i održanja aktuelnosti i celovitosti okvira upravljanja kontinuitetom poslovanja.

Organizacija se obavezuje na stalno unapređenje procesa kontinuiteta poslovanja u skladu uspostavljenih integrisanih postupaka stalnog unapređenja sa drugim sistemima menadžmenta. Politika u potpunosti podržava viziju organizacije kao odgovorne IT kompanije. Saga se obavezuje da poštuje navedene bezbednosne i organizacione principe, kako unutar nje, tako i prilikom pružanja IT usluge eksternim korisnicima.

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.

Direktor