CLOUD SERVIS

OZNAKA DOKUMENTA	*MT15POL02*	DATUM IZDANJA	*11-12-2023*
PRIMERAK BROJ	*01*	IZDANJE	*02*

AUTORIZACIJA	IME I PREZIME	FUNKCIJA	POTPIS
PRIPREMIO	Vladimir Miladinović	Menadžer ISMS-a	
ODOBRIO	Boris Čorni	Rukovodilac IT sektora	

SADRŽAJ

1 ZAPIS O DOPUNI

Datum	Brojevi strane(a)	Detalji izmene	Broj zahteva za izmenu dokumenta

2 DISTRIBUCIJA I KONTROLA

2.1 DISTRIBUCIJA

Rb. broj	Funkcija/odeljenje
1	Sistem administrator
2	Menadžer za ISMS
3	IT služba

2.2 KONTROLA

Nekontrolisani primerci ovog dokumenta se mogu izdati zainteresovanim stranama ili kupcima organizacije shodno odluci Direktora. Održavaće se zapisi o svakom nekontrolisanom primerku. Svaki primerak će se datirati i označiti sa **„NEKONTROLISANI PRIMERAK - UNIŠTITI NAKON UPOTREBE”** na naslovnoj strani.

3 SVRHA

Organizacije sve više premeštaju infrastrukturu i operacije kod hostovanih provajdera kako bi obezbedile podatke i alate zaposlenima efikasno i ekonomično. Bezbednosni položaj Cloud servis provajdera (CSP) mora da se proceni da bi se utvrdila usaglašenost sa bezbednosnim zahtevima organizacije pre nego što infrastruktura kojom upravlja odeljenje/sektor za IT organizacije može biti hostovana van okruženja organizacije.

IT sektor je odgovoran i posvećen za upravljanje poverljivošću, integritetom i dostupnošću mreža, sistema i aplikacija u okviru svojih ovlašćenja u okviru organizacije. Ovo uključuje obezbeđivanje gde god je to moguće da cloud okruženja u kojima se nalazi infrastruktura organizacije ispunjavaju određene bezbednosne kontrole i da ne ugrožavaju bezbednosni položaj organizacije do granica odgovornosti same organizacije.

Ova politika pokriva slede'u kontrolu:

- 5.23 Bezbednost informacija za upotrebu cloud servisa

4 PODRUČJE PRIMENE

Ova politika se primenjuje na sve IT sisteme kojima upravlja organizacija i koji se nalaze u infrastrukturi cloud rešenja. IT sektor će biti odgovoran za sprovođenje bezbednosti okruženja u cloud-u gde god je to moguće u skladu sa zahtevima ove politike.

5 TERMINI I DEFINICIJE

U cilju boljeg razumevanja ISMS-a organizacije, u nastavku su navedene definicije značajnijih pojmova koji se koriste u ovoj proceduri.

U dokumentaciji ISMS-a organizacije se koriste sledeće skraćenice:

ISMS – (Information security management Sistems), Sistem menadžmenta bezbednošću informacija - ISO/IEC 27001:2022.

6 REFERENTNA DOKUMENTA

ISO 27001:2022 *Sistem menadžmenta bezbednošću informacija - Zahtevi*

7 OPIS RADA

Organizacija će, kroz formalne smernice, definisati zahteve za nabavku, korišćenje, upravljanje i izlazak iz usluga u cloud-u, a koje treba da budu uspostavljene u skladu sa zahtevima organizacije za bezbednost informacija. Postupak se sprovodi kroz upravljanje dobavljačima. Organizacija će komunicirati sa svim relevantnim zainteresovanim stranama u okviru svoje politike upravljanja dobavljačima, koja takođe uključuje CSP-e. Korišćenje cloud servisa podrazumeva zajedničku odgovornost za bezbednost informacija i zajednički napor između CSP-a i organizacije koja deluje kao korisnik cloud servisa. Odgovornosti i za CSP i za organizaciju koja deluje kao korisnik cloud servisa biće definisane i sprovedene u skladu sa poslovnim zahtevima i zahtevima drugih relevantnih strana, uključujući zahteve zakona i drugih pravnih akata. Okvir politike zasnovana je na najboljim praksama i standardima zvanično međunarodno priznatim u svetu. Politika služi kao autoritativno prilagođavanje posebnim zahtevima kako bi se zadovoljile poslovne i operativne potrebe organizacije. Upotrebom usluga CSP, organizacije mogu imati koristi u ekonomičnom smislu. Međutim, korišćenje CSP-a centralizuje upravljanje informacijama i aplikacijama pošto su podaci i obrada izuzeti iz direktne kontrole različitih IT bezbednosnih grupa. Prilikom korišćenja usluga CSP-a, bezbednosni timovi moraju da uvedu skup (CSP i operativnih) kontrola u skladu sa uputstvima ove politike kako bi upravljali i ublažili rizike, pomažući da se osigura bezbednost organizacije, operacija i IT resursa.
Rešenja za upotrebu cloud servisa koje koristi organizacije trebalo bi da imaju strukturu za konfiguraciju, primenu i upravljanje koja mogu da zadovolje bezbednosne zahteve, zahteve za privatnost i druge zahteve organizacije gde god je to moguće kako bi se pristupalo ili zaštitila poverljivost, dostupnost I integritet podataka.
Ako organizacija odluči da koristi cloud servis, rešenja moraju da obuhvate preispitivanje sledećih oblasti koje će biti regulisane formalnim sporazumom između pružaoca usluge i organizacije kao korisnika usluge:

- svi relevantni zahtevi za bezbednost informacija u vezi sa korišćenjem cloud servisa;
- kriterijumi za izbor cloud servisa i obim korišćenja cloud servisa;
- uloge i odgovornosti u vezi sa korišćenjem i upravljanjem cloud servisa;
- kojim kontrolama bezbednosti informacija upravlja provajder, a kojima upravlja organizacija kao korisnik cloud servisa;
- kako dobiti i koristiti mogućnosti bezbednosti informacija koje pruža provajder cloud servisa;
- kako dobiti garanciju o kontrolama bezbednosti informacija koje sprovode provajderi;
- kako upravljati kontrolama, interfejsima i promenama usluga kada organizacija koristi više usluga u cloud-u, posebno od različitih provajdera;
- procedure za rukovanje incidentima bezbednosti informacija koji se javljaju u vezi sa korišćenjem cloud servisa;
- njegov pristup praćenju, pregledu i proceni tekućeg korišćenja cloud servisa za upravljanje rizicima po bezbednost informacija;

- kako da promenite ili prestanete da koristite cloud servis, uključujući izlazne strategije.

7.1 PRELIMINARNI ZAHTEVI

Svi provajderi koje koristi organizacija, a koji mogu pristupiti podacima o ličnosti (PII) moraju ispuniti minimalne zahteve navedene u nastavku.

➢ Usklađenost sa bezbednosnim standardima organizacije

CSP moraju biti u stanju da ispoštuju zahteve utvrđene u okviru relevantnih bezbednosnih politika organizacije, uključujući ovaj dokument.

IT sektor za bezbednost pre nabavke usluge mora da obavi bezbednosni pregled cloud servisa.

Ako je zakonom zahtevano relevantno nadzorno telo mora da odobri skladištenje podataka u cloud okruzenju, uz obavezu organizacije predvidi i ublaži rizike gde je to moguće za podatke i resurse smeštene u cloud-u u skladu sa Politikama bezbednosti informacija organizacije.

➢ Procena CSP

IT sektor za bezbednost će proceniti CSP-a koji može da pristupa osetljivoj i kritičnoj imovini organizacije, kao i podacima o ličnosti kojima upravlja organizacija, kako bi se osiguralo da CSP može da radi u skladu sa zahtevima navedenim u nastavku.

Ako su ugovori o cloud servisima unapred definisani od strane CSP-a i nisu predmet pregovora, organizacija će, na osnovu specifične ponude i performansi usluge koje garantuje provajder usluga, izabrati opciju koja ispunjava definisane zahteve u vezi sa poverljivošću, integritetom, dostupnošću i rukovanju informacijama sa odgovarajućim ciljevima nivoa cloud servisa i ciljevima kvaliteta cloud servisa. U ovom slučaju, izbor provajdera takođe mora biti uključen u proces procene rizika.

➢ Kompetentnost provajdera

Organizacija mora da se pozabavi dužnom pažnjom i sprovede temeljnu analizu mogućnosti i bezbednosnih mera provajdera. Ovo se može uraditi pomoću sredstava kao što su:

- Detaljan upitnik dat CSP-u
- Istraživanje kompanije (dostupni relevantni izvori informacija)
- Eksterni izveštaji o proceni dobavljača ili rezultati provere
- Prethodne izjave klijenata

➢ Ugovorne obaveze

- Pisani ugovor koji sadrži jasne mere mezbednosti i precizne odgovornosti ugovarača.
- Ugovore treba ponovo proceniti nakon svake značajne promene kod CSP-a (npr. kupovina od strane druge kompanije, bankrot, i drugo)

Ugovor između provajdera cloud servisa i organizacije, koja deluje kao korisnik cloud servisa, uključiće sledeće odredbe o zaštiti podataka organizacije i dostupnosti usluga:

- pružanje rešenja zasnovanih na industrijski prihvaćenim standardima za arhitekturu i infrastrukturu;
- upravljanje kontrolama pristupa uslugama u oblaku kako bi se ispunili zahtevi organizacije;
- implementacija rešenja za praćenje i zaštitu od zlonamernog softvera;
- obradu i čuvanje osetljivih informacija organizacije na odobrenim lokacijama (npr. u određenoj zemlji ili regionu) ili u okviru ili pod određenim jurisdikcijama;
- pružanje namenske podrške u slučaju incidenta bezbednosti informacija u okruženju cloud servisa;
- obezbeđuje da su zahtevi organizacije za bezbednost informacija ispunjeni u slučaju da se cloud servisi dalje ugovaraju sa spoljnim provajderom (ili zabranjuje podugovaranje);
- podrška organizaciji u prikupljanju digitalnih dokaza, uzimajući u obzir zakone i propise za digitalne dokaze u različitim jurisdikcijama;
- obezbeđivanje odgovarajuće podrške i dostupnosti usluga za odgovarajući vremenski okvir kada organizacija želi da izađe iz cloud servisa;
- obezbeđivanje neophodnih rezervnih kopija podataka i informacija o konfiguraciji i bezbedno upravljanje rezervnim kopijama po potrebi, na osnovu mogućnosti provajdera cloud servisa koje koristi organizacija, koji deluje kao korisnik cloud servisa;
- pružanje i vraćanje informacija kao što su konfiguracioni fajlovi, izvorni kod i podaci u vlasništvu organizacije, kao korisnika usluge u cloud-u, kada se to zahteva tokom pružanja usluge ili po završetku usluge.

➢ Kontinuirana procena

▪ Gde je moguće, organizacija treba da pregovara sa CSP-ima kako bi omogućila tekuću evaluaciju od strane ovlašćenih relevantnih lica kako bi se osiguralo da se mere bezbednosti pravilno primenjuju.

▪ Svako kršenje bezbednosnih mera koje utiče na bezbednost informacija organizacije koje organizacija otkrije mora biti saopšteno CSP-u što je pre moguće nakon otkrivanja kako bi CSP mogao da reši problem.

Usklađenost sa zahtevima, CSP-a bi trebalo da, kao deo svoje procene, budu u stanju da pokažu usklađenost sa primenljivim opšte priznatim zahtevima kao što su: ISO ili drugi standardi iz ove oblasti PCI DSS, HIPAA, CSA, SSAE16 (SOC1-finansije, SOC2-IT kontrole, SOC3-atest).

➢ Kontrole privatnosti i bezbednosti za cloud okruženje

Organizacija će proceniti potencijalnog CSP koji će pristupati podacima o ličnosti kojima upravlja organizacija kako bi osigurao da CSP može da radi sa svim primenljivim

funkcionalnostima navedenim u nastavku. Oni mogu biti uključeni u upitnik ili druge metodologije procene potencijalnog CSP-a koje organizacija smatra relevantnim tokom njihpove evaluacije.

Organizacija mora da se uveri da procesi i smernice CSP-a ne ugrožavaju privatnost i bezbednost podataka o ličnosti kojima upravlja organizacija, a koje hostuje CSP.

Gde je to moguće, organizacija mora da obezbedi da se hostovani sistemi ili usluge nadgledaju u pogledu radnog vremena, dostupnosti i bezbednosne funkcionalnosti.

Arhitektura organizacije mora da podržava primenljive osnovne tehnologije koje CSP koristi za hostovanje usluga i kako se integrišu sa trenutnom infrastrukturom organizacije ako takva integracija postoji.

- Upravljanje identitetom i pristupom

Organizacija mora da se uveri da su postavljene relevantne zaštitne mere koje obezbedjuju autentifikaciju, autorizaciju i druge funkcije upravljanja identitetom i pristupom u skladu sa zahtevima navedenim Politici kontrole pristupa.

CSP-i moraju da garantuju mogućnost izolacije za hostovane podatke i operacije od drugih zakupaca gde je to moguće, i da to mogu i da dokažu.

Dostupnost mora biti regulisana SLA-om sa CSP-om, kao i obaveza obaveštavanja o prekidu usluge, kao i nastavak kritičnih operacija u dogovorenom roku.

- Odgovor na incidente

Definisati obavezu da CSP mora obavesti organizaciju u razumnom roku nakon što je otkrivena povreda koja direktno utiče na resurse ili podatke organizacije.

7.2 IZUZIMANJA

Ako je potrebno izuzeće od ove politike, potrebno je podneti zahtev relevantnom rukovodstvu i u njemu treba jasno da se navedu razlozi za izuzeće. Nakon podnošenja zahteva, obavezno je sprovesti procenu operativnog rizika da bi se identifikovali rizici povezani sa ovim izuzećem. Ako organizacija može prihvatiti rizik, može se odobriti izuzeće od ove politike.

8 ODGOVORNOSTI I OVLAŠĆENJA

IT sektor bezbednosti je odgovoran za upravljanje bezbednosnim procenama za organizaciju u skladu sa utvrđenim zahtevima. Svi sistemi koji su pod upravljanjem organizacije sa zahtevima koji odstupaju od ovih smernica za bezbednost upotrebe cloud servisa moraju da podnesu zahtev za izuzeće od smernica na razmatranje i potencijalno odobrenje.
Svaki pokušaj osoblja da zaobiđe ili na drugi način povredi ovu politiku ili bilo koju prateću politiku tretiraće se kao kršenje bezbednosti i podleže istrazi. Rezultati istrage mogu povlačiti pismenu opomenu, suspenziju, prekid, a moguće i krivične i/ili građanske kazne..

9 ZAPISI

Sve informacije vezane za dokumentovani postupak upravljanje odnosima sa dobavljačima formiraju deo dokumentovanih informacija organizacije Meridian Tech d.o.o. Beograd. Dokumentovane informacije se moraju zadržavati i održavati u skladu sa ovim postupkom.

U realizaciji ovog postupka nastaju zapisi, odnosno dokumentovane informacije navedeni u tabeli.

Naziv	Referentna oznaka obrasca	Vreme čuvanja	Mesto čuvanja	Odgovorno lice

10 PRILOZI

Nema.