OPERATIVNE PROCEDURE ZA FUNKCIONISANJE

OZNAKA DOKUMENTA	*MT12PRO01*	**DATUM IZDANJA**	*01-12-2023*
PRIMERAK BROJ	*01*	**IZDANJE**	*02*

AUTORIZACIJA	**IME I PREZIME**	**FUNKCIJA**	**POTPIS**
PRIPREMIO	Vladimir Miladinović	Menadžer ISMS	
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
1	System administrator
2	Menadžer za ISMS
3	IT podrška

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

Svrha ove procedure jeste određivanje odgovornosti i procedure za osiguranje ispravnosti i sigurnog rada sredstava za obradu informacija. Kontrolišu se sve promene u kapacitetima sredstava za obradu informacija, vrši se kontrola softvera. Uspostavljaju se dužnosti sa ciljem smanjenja rizika od namerne i nenamerne zloupotrebe sistema, menadžment tehničkim ranjivostima.

Ova procedura pokriva sledeće kontrole:

- 5.37 Dokumentovanje operativnih procedura
- 8.15 Logovanje
- 8.34 Zaštita Informacionih Sistema tokom audit testiranja

4 PODRUČJE PRIMENE

Ova procedura se odnosi na sve zaposlene u kompaniji.

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 systems), Sistem menadžmenta zaštite i bezbednosti informacija – ISO/IEC 27001:2022.

6 REFERENTNA DOKUMENTA

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

7 OPIS RADA

7.1 OPERATIVNE PROCEDURE I ODGOVORNOSTI

7.1.1 Operativna dokumentacija

Organizacija poseduje operativnu dokumentaciju koja sadrži sve detalje u vezi sa IT sistemom, koje koriste različiti timovi (organizacione jedinice) u organizaciji. Dokumentacija se sastoji od procedure i radnih uputstava sa sledećim detaljima :

- Opis IT sistema (mrežno povezivanje, konfiguracije, instalacijska uputstva itd.)
- Upravljanje informacijama u IT sistemima
- Backup procedure
- Instrukcije za upravljanje greškama
- Detalji o kontakt osobama i način izveštavanja u slučaju nepredviđenih prekida
- Procedure za restart i obnavljanje sistema
- Procedure i uputstva za održavanje sistema

Opis infrastrukture, servisa, segmenata i uređaja nalazi se u sklopu tehničke dokumentacije IT podrške.

Operativne procedure koriste se u svakodnevnom održavanju IT sistema i infrastrukture organizacije Meridian Tech d.o.o. Beograd , kako bi se obezbedila najbolja moguća primena ove informacione imovine.

Proceduru je potrebno izraditi u sledećim slučajevima:
a) kada aktivnost treba da obavlja na isti način više ljudi;
b) kada se aktivnost obavlja retko i kada se sledeći put izvodi postupak je verovatno zaboravljen;
c) kada je aktivnost nova i predstavlja rizik ako se ne obavlja pravilno;
d) pre predaje aktivnosti novom osoblju.

Promene u operativnim sistemima organizacije kontrolisane su formalno dokumentovanom procedurom za kontrolu promena.

Razvoj i okolina u kojoj se vrše testiranja su odvojeni od operativnog okruženja, kako bi se smanjio rizik slučajnih promena ili neovlašćenog pristupa.

Dokument dovoljno detaljno opisuje operativne procedure koje timovi u različitim odeljenjima koriste.

U okviru standardne procene rizika, proceniti sve značajne promene u glavnoj infrastrukturi (npr. mrežama, direktorijima) radi njihovog uticaja na bezbednost informacija.

Odvojiti razvoj i okruženje za testiranje putem najprikladnijih kontrola koje uključuju, ali nisu konačne, sledeće kontrole:

- Rad na odvojenim kompjuterima, domenima, instancama i mrežama,
- Različita korisnička imena i lozinke,
- Dužnosti onih koji imaju pristup i koji testiraju operativne sisteme.

7.1.2 Upravljanje promenama

Svi objekti ili komponente IT infrastrukture organizacije Meridian Tech d.o.o. Beograd , pokrivene su planom kapaciteta i procedurom za upravljanje promenama, kako bi se osiguralo da zahtevi za povećanjem snage i čuvanjem podataka budu pravovremeno i u potpunosti ispunjeni.

Ključne komponente IT infrastrukture, između ostalog uključuju:
- File servere
- Domain servere
- E-mail servere
- Web servere
- Štampače
- Mreže
- Kontrole okruženja uključujući fizički pristup, klimatizaciju, el. napajanje i dr.

Sva odeljenja moraju obavestiti IT podršku i ISMS menadžera o potrebama za novim proizvodima ili bilo kakvim nadogradnjama, servisnim paketima, patches ili popravkama koje su neophodne postojećem sistemu.
Novi informacioni sistemi, nadogradnje proizvoda, patches i popravke moraju proći odgovarajući nivo testiranja, pre prihvatanja i puštanja u upotrebu.
Kriterijumi za prihvatanje moraju biti jasno identifikovani, dogovoreni i dokumentovani i odobreni od strane menadžmenta.
Aplikacije za servisne pakete i patches od trećih strana, takođe se moraju nadzirati.
Velike nadogradnje sistema moraju se pažljivo testirati, paralelno sa postojećim sistemom u bezbednosnom okruženju za testiranje.
Promene u IT sistemima kompanije kontrolišu se dokumentovanom Procedurom za upravljanje promenama u IT sistemima.

Procedura za upravljanje promenama u IT sistemima u sebi sadrži sledeće detalje:

- Opis promena i razlog za iste
- Informacije povezane za fazu testiranja
- Detalje o uticaju promena na IT sisteme
- Opis procesa odobravanje promena
- Komunikacija sa svim osobama koje utiču na promene

- Postupci vraćanja IT sistema u prvobitno stanje

Sve promene IT sistema u kompaniji se prethodno analiziraju i ocenjenjuje se sigurnosni rizik prilikom njihove realizacije.

7.1.3 Podela dužnosti

U kompaniji postoji jasna podela dužnosti svih zaposlenih, kako bi se onemogućilo da jedan od zaposlenih može sam da u potpunosti upravlja određenim IT sistemom.

Detalji vezani za pojedina prava svakog zaposlenog i za nivo pristupa su opisani u posebnom dokumentu, kojim se reguliše kontrola pristupa informacionim sistemima - Politika kontrole pristupa.

Uređaji koji ne podržavaju domensku autentifikaciju upravljaju se od strane jednog administratora, a *pristupne* šifre za uređaje čuvaju se u sefu i uzimaju se (isključivo uz prisustvo Menadžera ISMS-a ili Direktora) samo u slučaju potrebe.

Prijava na bilo kom sistemu u kompaniji se, takođe, radi isključivo sa svojim korisničkim profilom (user account). Zabranjeno je korišćenje admin user account osim u slučaju kada nije moguće kreiranje novih admin profila, i u tom slučaju profil je dodeljen, a šifru zna samo jedan zaposleni (kopija se čuva u sefu). Prijavu sa admin user account radi samo Sistem administrator uz prisustvo Menadžera ISMS-a. U specijalnim slučajevima kada Menadžera ISMS-a nije u mogućnosti da prisustvuje, a u cilju efikasnog obavljanja poslovnih zadataka, to može da se delegira drugom zaposlenom uz zapis o tome.

Svaki korisnik ima pravo pristupa informacionom sistemu prema pravima dodeljenim u skladu sa dokumentom Politika kontrole pristupa.

U redovnoj proceduri, šifre svih admin korisnika se moraju promeniti svaka 3 meseca, a za kontrolu je zadužen Menadžer ISMS-a. U slučaju kada Menadžer ISMS-a ima potrebu da podeli šifru od admin profila sa nekim od zaposlenih koji je odgovoran za obavljanje intervencije na serveru, šifra se mora promeniti odmah po završetku intervencije.

7.1.4 Podela na razvojnu, testnu i produkcionu okolinu

Aplikativni deo informacionog sistema organizacije je podeljen na razvojnu, testnu i produkcionu okolinu, sa ciljem smanjenja rizika od nekompatibilnost razvojnih verzija, identifikacije i rešavanja aplikativnih grešaka i nedostataka u programima, slučajnih promena ili neautorizovanih pristupa. Aplikativni deo podrazumeva potpunu redudantnost i u zavisnosti od arhitekture rešenja u sebi sadrži bazu podataka (tj. model baze podataka i podatke), aplikativni srever i aplikaciju. Podela na razvojnu, testnu i produkcionu okolinu odnosi se na aplikativna rešenja razvijena u organizaciji.

Razvojna okolina se koristi za razvoj aplikativnih rešenja. Razvojna okolina je kompletno nezavisna od testne i produkcione okoline. Razvojna okolina je dostupna isključivo timu za razvoj (dizajneri, programeri itd.), a nikada krajnim korisnicima.

Testna okolina se koristi za testiranje aplikativnih rešenja, identifikaciju problema i aplikativnih grešaka, odobravanja funkcionalnih zahteva i slično u slučaju postavljanja novih informacionih sistema ili menjanje verzije postojećih.

Zadužen za postavljanje i održavanje testne okoline, obezbeđivanje odgovarajućih prava pristupa, kontrolu i upravljanje podacima, i uništavanje po isteku upotrebe, jeste tim odgovoran za kontrolu kvaliteta, u kojem su Menadžer ISMS-a, testeri ili krajni korisnici u ulozi testera. Tim za kontrolu kvaliteta direktno sarađuje sa razvojnim timom.

Testna okolina je dostupna timu za kontrolu kvaliteta ili, po potrebi, i krajnim korisnicima ako su u ulozi testera kvaliteta. U slučaju da krajni korisnici imaju ulogu testera aplikativnih rešenja, njihove privilegije su iste sa pravima pristupa koje imaju u produkcionoj okolini. Prava pristupa funkcijama i podacima u testnoj okolini su ista sa pravima pristupa funkcijama i podacima u produkcionoj okolini.

Prilikom postavljanja novih verzija, testna okolina se kreira replikacijom (virtuelizacija ili druga metoda) produkcione okoline, koja omogućava identično okruženje i testiranje u realnim uslovima. Pri tome se posebna pažnja posvećuje replikaciji: uvek kada je moguće izbegava se korišćenje produkcionih tj. realnih podataka pri testiranju. U slučaju kada to nije moguće, radi se obavezno skrembliranje podataka. Testiranje na realnim podacima u testnoj okolini je dozvoljeno samo uz saglasnot Menadžera ISMS-a i samo od strane zaposlenih koji imaju pravo pristupa tim informacijama.

Produkciona okolina je namenjena isključivo za obavljanje poslovnih funkcija. Pristup produkcionoj okolini imaju krajni korisnici, u skladu sa dodeljenim pravima pristupa.

Svaki identifikovani problem na produkcionoj okolini se reprodukuje i ponavlja na testnoj okolini. Popravke se rade isključivo na razvojnoj okolini, postavljanjem nove verzije, ili rešenjem (bug fix, patch itd.) koje se testira na testnoj okolini. Nakon uspešnog testiranja i dobijanja pozitivnih rezultata, nova verzija ili rešenje se postavlja u produkcionu okolinu. Administrativne aktivnosti u produkcionoj okolini (postavljanje nove verzije, inslalacija bug fix, patch itd.) se obavljaju isključivo van radnog vremena, uz prethodno isplanirane procedure impelementacije.

7.1.5 Upravljanje kapacitetima

Organizacija ima uspostavljene mehanizme za monitoring kapaciteta sistema čime se omogućava planiranje potrebnih kapaciteta.

Upravljanje ključnim sistemskim resursima se odnosi na:

- Serversku infrastrukturu
- Mrežnu infrastrukturu
- Štampače
- Radne stanice i laptopove
- Radnu snagu
- Radni prostor

Sve organizacione jedinice moraju da informišu Menadžera ISMS-a o zahtevima za nove resurse ili nadogradnju već postojećih novijom verzijom.

Svi novi informacioni sistemi (resursi), nadogradnja resursa i sigurnosne zakrpe, prolaze odgovarajući nivo testiranja pre nego se prihvati njihova implementacija na produkcionoj okolini. Kriterijumi za prihvatanje promena su jasno utvrđeni i usvojeni od strane menadžmenta organizacije. Veće sistemske nadogradnje se temeljno testiraju u paralelnoj testnoj okolini koja je isto kofigurisana kao i produkciona.

7.1.6 Zaštita od zlonamernih servisa

Sve radne stanice i serveri u kompaniji su zaštićeni od zlonamernih softvera. Zaštita je omogućena korišćenjem softverskih alatki i redovnom obukom zaposlenih. S tim ciljem je uspostavljena Antimalware politika.

7.1.7 Nadogradnja

Sve nadogradnje (nove verzije ili zakrpe) moraju biti instalirane odmah nakon objavljivanja od strane proizvođača i nakon uspešnog testiranja i prihvatanja promena.

7.2 BACKUP

7.2.1 Izrada sigurnosnih kopija

Regularni backup informacionog sistema radi se zbog povratka svih podataka u slučaju incidenta, katastrofe, problema sa medijima i ostalih problema.

U cilju ostvarenja osnovnih poslovnih zahteva, redovni i pouzdani backup, organizacija je usvojila Backup politiku. Svi zaposleni imaju dužnost da svoje podatke sa lokalnih kompjutera čuvaju (kopiraju) na server ili u folder namenjenu za to. Svaki zaposleni ima pristup isključivo svom privatnom folderu u kome mora pri kraju svakog radnog dana da kopira svoje bitne podatke. Menadžera ISMS-a je zadužen za backup ličnih podataka svih zaposlenih sa servera. Svi podaci koji nisu kopirani na privatnim serverskim folderima, nisu predmet backup procedure, i u slučaju oštećivanja ili gubljenja odgovoran je isključivo zaposleni.

7.2.2 Vraćanje informacija sa sigurnosnih kopija

Backup informacija i softvera se redovno izrađuje, ispituje i proverava.

Deo podataka koji ima veliku važnost za kompaniju se automatski kopira (replicira) na posebni server.

7.3 MREŽNA BEZBEDNOST

U cilju ostvarenja osnovnih poslovnih zahteva, pristup mreži organizacije je ograničen, organizacija je usvojila Politiku mrežne bezbednosti.

Svrha ove Politike ja da definiše implementirane kontrole u mreži organizacije Meridian Tech d.o.o. Beograd u cilju sprečavanja neovlašćenog pristupa mrežnim servisima.

7.4 UPRAVLJANJE MEDIJIMA ZA PRENOS INFORMACIJA

7.4.1 Prenosivi medeiji

Mediji na kojima se čuvaju podaci između ostalih uključuju:

- Hard Drive-ove (interne and eksterne)
- CD
- DVD
- Optičke diskove
- USB memorijske stikove
- Čitače medijskih kartica
- MP3 Player-e
- Digitalne kamere
- Backup kasete

Prenosni kompjuterski mediji (npr. trake i štampani izveštaji) su zaštićeni, kako bi se sprečilo njihovo oštećenje, krađa ili neovlašćen pristup.
Prilikom transporta, mediji na kojima se čuvaju podaci su zaštićeni od neovlašćenog pristupa, zloupotrebe ili korupcije.
Sistemska dokumentacija je zaštićena od neovlašćenog pristupa. Ona uključuje ugovornu dokumentaciju koju je kreirao IT sektor ili bilo ko od osoblja iz IT odeljenja (Nisu uključena opšta uputstva za upotrebu koja su dostavljena sa softverom).
Primer dokumetacije koja treba da se zaštiti, između ostalog uključuje opise:

- Aplikacija
- Procesa
- Procedura

- Struktura podataka
- Detalje o autorizaciji

Treba voditi dokumentovane procedure o backup medijima koji se redovno razmenjuju između kancelarijskih zgrada. Skladišta sa medijima su u bezbednom okruženju.
Dogovoriti odgovarajuće aranžmane koji će u budućnosti omogućiti dostupnost podataka koji će biti potrebni i nakon roka važenja backup medija.
Kad se pojavi potreba za kuririma, treba sastaviti spisak pouzdanih i poverljivih kurira (kurirskih službi).
Ukoliko je prikladno, trebale bi se koristiti fizičke kontrole, poput kodiranja ili posebnih zaključanih spremnika.
Treba se pobrinuti da su mediji koji više nisu potrebni bezbedno uklonjeni, kako bi se sprečilo curenje informacija.
Treba primenjivati efektivne verzije kontrola na svu dokumentaciju i skladišta u kojima se ona čuva.

Korisnicima je zabranjeno korišćenje USB uređaja u privatne svrhe. Zabranjeno je snimanje poverljivih dokumenata na USB bez prethodnog odobrenja. Takođe, svi su zaposleni informisani da manje štampaju i da koriste informacije sa hartije samo u slučaju kada je to neophodno. Svi spoljni uređaji, kao USB, spoljni diskovi i ostali prenosivi mediji, podložni su zloupotrebi i zato svaki zaposleni snosi odgovornost o dodeljenom mediju. Zabranjeno je ostavljanje medija bez nadzora i obavezno je čuvanje u skladu sa uputstvima proizvođača.

7.4.2 Uništavanje medija za prenos informacija

Ukolio se neki mediji (HDD, SSD, DVD, Blu-Ray, USB) više ne koriste, isti se moraju uništiti bez mogućnosti da neko pročita informacije na njima. Ukoliko se koristi eksterna firma za odstranjivanje otpada, firma mora da ima odgovarajuće procese i kontrolu rada.

Postupci za uništavanje medija se svode na njihovo formatiranje, a potom i na fizičko uništenje, tj. mehaničko uništenje tupim predmetom bez mogućnosti ponovnog korišćenja medija u nekom drugom uređaju.

7.4.3 Transport medija za prenos informacija

Svaki mediji koji se transportuje mora biti zaštićen od neautorizovanog pristupa, zaloupotrebe ili narušavanju integriteta informacija.

U situacijama gde se transport vrši od strane eksternih lica (ili kompanija), obavezno je potpisivanje dogovora koji obavezuje zadovoljavanje određenih sigurnosnih procedura. Uvek kada je primenjljivo, koristi se enkripcija podataka ili specijalne zaključane kutije.

7.4.4 Bezbednost sistemske dokumentacije

Sistemska dokumentacija se čuva u folderu sa ograničenim i potpuno kontrolisanim pristupom. Pristup dokumentaciji imaju samo osobe koje imaju potrebu za to.

7.5 RAZMENA INFORMACIJA

7.5.1 Procedure za razmenu informacija

Organizacija ima implementirane kontrole za zaštitu razmene informacija.

Kontrole omogućavaju zaštitu od:

- presretanja komunikacije
- kopiranja
- modifikacije
- preusmeravanja komunikacije
- uništavanja

Informacije se štite odgovarajućim stepenom njihove klasifikacije tj. poverljivosti.

7.5.2 Dogovori oko razmene informacija

U slučaju razmene informacija između organizacije i drugih organizacija, celi se proces mora regulisati formalnin dogovorima. Isto važi i za kompanije koje nude servis za dostavu informacija.

Dogovor mora da sadrži klasifikaciju informacija i kontrole koje su uspostavljene za zaštitu istih.

7.5.3 Online transakcije

Organizacija koristi usluge e-bankarstva.
Pristup web servisima se radi korišćenjem SSL (Secure Sockets Layer) enkriptovane konekcije. Plaćanje se vrši nakon autentifikacije korisnika i putem sertifikata koji se nalazi na tokenu/smart kartici. Svakim tokenom je zadužen konkretni zaposleni, o čemu se čuva zapis. Zabranjeno je korišćenje ili razmena tokena između zaposlenih.

Pazi se da passwordi ne budu komplikovani i da se često menjaju, skladu sa Politikom korisničkih šifri.

Uvid u račune i izdavanje naloga za plaćanje imaju zaposleni u odeljenju za finansije.

Nalog koji je kreiran od strane zaposlenog u odeljenju za finansije ne može biti realizovan pre nego isti bude potpisan od strane Direktora, koji ima sertifikat na tokenu. Pristup sertifikatu se dobija ne samo fizičkim posedovanjem tokena već i unošenjem šifre kojom je sertifikat zaštićen. Tim načinom je obezbeđena dvofaktorska autentifikacija i viši nivo sigurnosti u slučaju da token bude ukraden ili izgubljen.

7.5.4 Dostupnost informacija

U ovoj oblasti se primenjuje Zakon o zaštiti podataka o ličnosti i ostali zakoni.

Ukoliko se prilikom razvoja i testiranja aplikativnog softvera koriste lični podaci, oni moraju biti zaštićeni i kontrolisani u skladu sa Zakonom o zaštiti podataka o ličnosti i kada postoji mogućnost, treba ih učiniti nepersonalizovanima.

Ukoliko se koriste operativni podaci, trebaju se koristiti sledeće kontrole:

- Proces autorizacije
- Uklanjanje operativnih podataka iz sistema za testiranje nakon upotreba
- Kompletan audit trial povezanih aktivnosti
- Svi lični ili poverljivi podaci moraju se zaštititi kao da nisu u javnosti

Javno dostupne informacije o kompaniji su objavljene na web strani organizacije. Ista je hostovana na web serveru u inostranstvu. Pristup serveru i mogućnost objavljivanja informacija ima samo odgovorni zaposleni. Pre nego se bilo koja informacija objavi na sajtu, zaposleni iz marketinga daje predlog i traži dozvolu Direktora.

7.6 POLITIKA KORIŠĆENJA SOFTVERA

Organizacija Meridian Tech d.o.o. Beograd koristi softver u svim aspektima svog poslovanja, kako bi pružila podršku poslovima koje obavljaju njeni zaposleni.
Svaki deo softvera treba da ima licencu i organizacija neće koristiti niti jedan softver za koji nema licencu.

Kanali za nabavku softvera su ograničeni, kako bi se osiguralo da organizacija ima kompletnu evidenciju o svim softverima koje je kupila za svoje računare i koji mogu da se registruju, podrže i nadograde.

Ovim su obuhvaćeni i softveri koji mogu da se preuzmu i/ili kupe na internetu. Ovaj softver je vlasništvo softverske kompanije i njegovo kopiranje predstavlja kršenje autorskih prava, osim ako ga nije odobrio proizvođač softvera.

Za *Shareware*, *Freeware* i softver u javnom vlasništvu važe iste politike i procedure kao i za ostale softvere.

Svi softveri koji su potrebni organizaciji moraju se nabaviti uz znanje ISMS menadžera.

Softver mora biti registrovan na ime organizacije i odeljenja u kojem će se koristiti.

IT podrška održava registar svih softvera u organizaciji i vodi biblioteku softverskih licenci.

Softver na LAN-u ili na više uređaja koristiće se samo u skladu sa ugovorom o licenci.
IT podrška može da instalira softver tak kada su svi zahtevi za registraciju ispunjeni.
Sve promene u softveru moraju se odobriti, pre nego što se implementiraju.
Ni u kom slučaju se ne sme dozvoliti instaliranje ličnih ili neovlašćenih softvera (oni uključuju screen saver-e, igrice, pozadine, itd.) na računare u organizacije jer oni nose ozbiljan rizik od unošenja virusa.
S obzirom da se zaposleni menjaju, softver se nikad ne registruje na ime pojedinačnog korisnika.
Softver ne sme menjati niti jedan korisnik, osim ako za to ne postoji jasna poslovna potreba.
Svaki korisnik u kompaniji koji kreira, nabavlja ili koristi neovlašćene kopije softvera biće podvrgnut disciplinskim merama u skladu sa okolnostima. Organizacija ne odobrava ilegalno dupliranje softvera niti će ga tolerisati.

7.7 MONITORING

U dnevnicima audita (*audit logs*) moraju se nalaziti bar sledeće informacije:

- Identitet sistema
- Identifikacija korisnika
- Uspešno/neuspešno prijavljivanje
- Uspešno/neuspešno odjavljivanje
- Neovlašćeni pristupi aplikaciji
- Promene u konfiguraciji sistema
- Korišćenje privilegovanih naloga (npr. za upravljanje nalogom, politiku promena, konfiguraciju uređaja)

Dnevnike u kojima su se vodili zapisi o izuzecima i ostalim događajima, vezanim za bezbednost, čuvati bar šest meseci.
Zaštititi pristup dnevnicima od neovlašćenih pristupa koji mogu da dovedu do krađe ili brisanja zabeleženih informacija.
Sprečiti samoinicijativno brisanje ili deaktiviranje dnevnika od strane sistemskih administratora.
Kada je to moguće, odvojeno arhivirati poverljive od nepoverljivih podataka.

Svi satovi na kompjuteru trebaju biti usklađeni prema GSI vremenskoj zoni, kako bi se obezbedila tačnost svih dnevnika audita, jer će možda biti korišćeni prilikom istrage incidenta.

U mreži je instaliran Zabbix sistem za monitoring. Sistem prati sve bitne parametre sistema (hardverske i softverske) i loguje sve promene u slučaju da je potrebna naknadna forenzička analiza.

U slučaju problema (narušeni rad operativnog rada sistema, system health check) sistem šalje email poruku administratoru. Monitoring se radi za sve važne servere, aplikacije, mrežnu opremu i štampače.

NAS server loguje sve neuspešne pokušaje prijave na server. U slučaju pokušaja prijave pogrešnim korisničkim imenom ili šifrom, šalje se email poruka administratoru.

Svi administratorski logovi se čuvaju u različitim fajlovima, i pristup njima ima samo System administrator.

Jednom dnevno administrator pregleda logove sa ciljem analiziranja i otkrivanja netipičnih ili nedozvoljnenih aktivnosti.

Svi se logovi čuvaju i bekapuju i skladu sa backup procedurom.

Osnovni preduslov da logovani podaci budu relevantni jeste da svi serveri imaju sinhronizovano vreme sa istog izvora.

8 ODGOVORNOSTI I OVLAŠĆENJA

Svi zaposleni koji prekrše ove Operativne Procedure biće predmet Disciplinskih mera, pa čak i mera prestanka radnog odnosa.

9 ZAPISI

Sve informacije vezane za dokumentovani postupak upravljanje operativnim funkcionisanjem 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.