PROCEDURA ZA UVOĐENJE, RAZVOJ I ODRŽAVANJE INFORMACIONIH SISTEMA

OZNAKA DOKUMENTA	*MT14PRO01*	**DATUM IZDANJA**	*02-12-2023*
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/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 stran.

3 SVRHA

Ova procedura je usvojena kako bi se ukazalo na ispravne smernice za uspešnu implementaciju unutrašnjih kontrola kao integralni deo informacionog sistema organizacije Meridian Tech d.o.o. Beograd uključujući bezbednost kao značajni deo faze specifikacije i dizajna informacionih sistema, razvoja i testiranja, upotrebe sistema u produkcionoj okolini i nadogradnji informacionih sistema.

Ova procedura pokriva sledeće kontrole:

- 8.25 Životni ciklus bezbednog razvoja
- 8.26 Zahtevi za bezbednost aplikacije
- 8.27 Arhitektura bezbednog sistema i principi inženjeringa
- 8.29 Bezbedno testiranje u razvoju i prihvatanju
- 8.30 Razvoj u outsourced-u
- 8.31 Razdvajanje razvojnog, testnog i proizvodnog okruženja

4 PODRUČJE PRIMENE

Ovaj dokument je namenjen tehničkom osoblju kompanije, koje učestvuje u procesu razvoja informacionog sistema kompanije.

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:

U dokumentaciji ISMS-a organizacije se koriste sledeće skraćenice:

ISMS – (Information security management Sistems), 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 BEZBEDNOSNE KONTROLE PRI UVOĐENJU NOVIH SISTEMA

Uvođenje novih sistema u organizaciju, kao i promene u postojećim, radi se isključivo prateći standarde o bezbednosti informacionih sistema. Da bi se postigla bezbednost informacija kao integralnog dela informacionog sistema, posebna se pažnja obraća na analizu i specifikaciju zahteva za nove ili izmene u postojećim sistemima. Tokom definisanja funkcionalnih i tehničkih zahteva za nove sisteme i promene u postojećim, obavezno se mora paziti da sveobuhvatno budu uključeni zahtevi za bezbednosne mere na informacionim sistemima. Sistemska poboljšanja za bezbednost informacija i procesa za implementaciju bezbednosnih mera integrišu se u ranoj fazi projekta. Menadžer ISMS-a je odgovoran za proveru i odobravanje projekta i kontrolu bezbednosnih mehanizma u njima. Kontrole uključene u fazi dizajna su značajno lakše i jeftinije za implementaciju nego one uključene u ili nakon faze implementacije.

7.2 KONTROLA TOKOM OBRADE INFORMACIJA U INFORMACIONIM SISTEMIMA

Za smanjenje rizika od greške, gubitka, neautorizovane promene ili upotrebu informacija u aplikativnim rešenjima, uključuju se sledeće kontrole u samom dizajnu aplikacije, i to tokom:

- **Validacije ulaznih podataka** – tokom inputa podataka u informacionim sistemima (preko aplikacije, poslovne transakcije, konfiguracionog parametra i sl.) obavezna je primena provere i validacija unetih podataka. Ove kontrole trebaju biti automatske i integrisane u samim sistemima uvek kade je to moguće. Pored ovih automatskih, sistemksih kontrola i validacije ulaznih podataka, periodično se radi i kontrola i revizija podataka, kao dopunska kontrola. Sistemske kontrole uključuju i adekvatne poruke o greškama koje su precizne i jednoznačne za korisnike. U procesu unosa informacija u informacioni sistem, uloga i funkcija svakog korisika je tačno definisana.
- **Kontrola obrade** – u aplikaciji su ugrađene validacione provere pri obradi podataka, sa ciljem detekcije i izbegavanja koraka pri obradi koji će dovesti do korupcije podataka. U kontekstu kontrola ovog tipa, posebna zaštita se koristi tokom akcija promene i brisanja podataka, u odnos na stroge kontrole i definisanje prava pristupa u aplikacijama, logovanje preuzetih aktivnosti, monitoring promena i slično.
- **Validacija izlaznih podataka -** izlazni podaci iz aplikacija su validirani kako bi se osigurala tačna i adekvatna obrada podataka u sistemima.

7.3 KRIPTOGRAFSKE KONTROLE

Ako postoje uslovi za implementaciju kriptografskih kontrola za zaštitu informacija, obavezno se uzima u obzir sledeće:

- Identifikovanje potrebnog nivoa zaštite, bazirano na analizi rizika i vodeći računa o tipu, jačini i kvalitetu traženog algoritma enkripcije,
- Korišćenje enkripcije za zaštitu osetljivih informacija koje se prenose putem mobilnih ili prenosnih medija, unutrašnjih ili spoljnih komunikacionih linija,
- Usvajanje metoda za zaštitu kriptografskih ključeva i bezbedno vraćanje enkriptiranih informacija u slučaju gubitka, oštećivanja ili kompromitiranja ključeva,
- Određivanje uloga i odgovornosti za:
    - Implementiranje politika
    - Upravljanje ključevima
    - Usvajanje standarda za efektivnu implementaciju, na nivo cele kompanije i različite sisteme u kompaniji.

Za podršku upotrebe kriptografskih tehnika u kompaniji, uvek kada je to moguće, mora se usvojiti sistem za upravljanje ključevima. Sistem se mora bazirati na procedurama i metodama za:

- Generisanje ključeva za različite kriptografske sisteme i različite primere,
- Generisanje i prihvatanje sertifikata za javne ključeve,
- Distribucija ključeva do korisnika, uključujući i aktiviranje dobijenih ključeva,
- Memorisanje ključeva, uključujući i to kako će autorizovani korisnici dobiti pristup ključevima,
- Promena ili obnova ključeva, uključujući i pravila kako se menjaju ključevi,
- Ponašanje sa otkrivenim (ugroženim) ključevima,
- Povlačenje ključeva, uključujući kako će ključevi biti povučeni i deaktivirani,
- Obnavljanje ključeva koji su izgubljeni ili oštećeni, kao deo upravljanja kontinuitetom poslovanja
- Arhiviranje ključeva, koji se koriste za arhiviranje ili backup
- Izvršavanje aktivnosti za audit procesa upravljanja ključevima.

7.4 BEZBEDNOST PRODUKCIONIH SISTEMA

Kako bi se osigurala bezbednost produkcionih sistema u organizaciji, pristup tim sistemima, na nivou operativnog sistema, sistemske datoteke, produkcione baze, aplikativnog servera i aplikacije, kao i izvornom kodu, strogo je kontrolisan. Sve IT aktivnosti redovnog održavanja sistema, kao i ostale projektne aktivnosti izvode se na bezbedan način. Kako bi se minimizirali rizici od oštećivanja produkcionih sistema, sve se promene u sistemima kontrolišu po sledećim uputstvima:

- Nadogradnju operativnih sistema, aplikacija, programskih biblioteka, radi samo administrator, sa odgovarajućim privilegijama i pravima pristupa,
- Produkcioni sistemi, sadrže jedino verzije izvršnog koda koje su odobrene, a nikako razvojne verzije koda,
- Aplikacije i softveri u produkcionim sistemima se mogu implementirati samo nakon uspešnog testiranja. Testiranje obuhvata testove funkcionalnosti, upotrebljivosti, bezbednosti. Testiranje je uvek urađeno na zasebnom sistemu, u zasebnoj testnoj okolini.
- Postoji ažurna tehnička dokumentacija za svaki produkcioni sistem,
- Tokom svake implementacije novog sistema ili nadogradnje postojećih produkcionih sistema, postoji procedura za vraćanje prethodnog stanja sistema,
- Svaka nadogradnja produkcionih sistema je detaljno evidentirana i logovana,
- Uvodi se sistem verzionisanja izvršnog koda, kako bi se pratile promene,
- Tokom svake nadogradnje produkcionih sistema, prethodna se verzija čuva. Stare verzije se arhiviraju zajedno sa propratnim informacijama i parametrima, procedurama, konfiguracionim detaljima.

Softver koji je implementiran od strane proizvođača, a koji se koristi u produkcionoj okolini sistema, održava se na verziji koja je podržana od proizvođača.

Nakon određenog vremena, proizvođači prekidaju podršku za starije verzije softvera. Kompanija treba da uvek razmatra i proceni rizike od korištenja softverskih verzija koje nisu podržane od strane proizvođača.

Svaka odluka o nadogradnji produkcionog sistema i prelazak na novu verziju uzima u obzir poslovnu opravdanost promene i bezbednost nove verzije. Softverske zakrpe se implementriaju uvek kada mogu da pomognu u otklanjanju i smanjivanju rizika od bezbednosnih/tehničkih ranjivosti. Pristup produkcionim sistemima dobavljača i osobama uključenim u implementaciju novih sistema i nadogradnju postojećih produkcionih sistema je omogućeno u skladu sa Politikom kontrole pristupa.

Razdvajanje na razvojnu, testnu i produkcionu okolinu, kao i zaštita podataka u testnoj okolini je definisana u dokumentu Operativne procedure za funkcionisanje.

7.4.1 Kontrola pristup izvornim programskom kodu

Pristup izvornom programskom kodu i srodnim datotekama i dokumentaciji, je strogo kontrolisan kako bi se sprečilo uvođenje neautorizovanih funkcionalnosti i kako bi se izbegle nenamerne izmene. Za izvorni programski kod, ovo se postiže formiranjem centralne lokacije za čuvanje tog koda. Obavezno se koriste sledeća uputstva sa ciljem kontrole pristupa tim bibliotekama, a sve zbog smanjenja mogućnosti oštećenja kompjuterskog programa:

- Zaposleni ne smeju da imaju neograničeni pristup izvornim programskim bibliotekam,

- Izmene u izvornim programskim bibliotekama i srodnim datotekama, kao i izdavanje dokumentacije i izvornog programskog koda programerima se obavlja nakon dobijanja odgovarajuće autorizacije,
- Liste sa programima se čuvaju na bezbednoj lokaciji,
- Čuva se audit zapis o svakom pristupu programskim bibliotekama,
- Održavanje i kopiranje progrmaskih biblioteka je pod strogom kontrolom procedura o promenama.

7.5 PRINCIPI ZA INŽENJERING SIGURNIH SISTEMA

Organizacija treba da uzme u obzir principe "nultog poverenja" kao što su:
a) pod pretpostavkom da su informacioni sistemi organizacije već probijeni i da se stoga ne oslanjaju samo na sigurnost perimetra mreže;
b) korištenje pristupa „nikad ne veruj i uvek verifikuj“ za pristup informacionim sistemima;
c) obezbeđivanje da su zahtevi upućeni informacionim sistemima šifrovani od kraja do kraja;
d) verifikaciju svakog zahteva upućenog informacionom sistemu kao da potiče iz otvorene, eksterne mreže, čak i ako su ovi zahtevi nastali interno u organizaciji (tj. bez automatskog verovanja ničemu unutar ili izvan njenog perimetra);
e) korištenjem tehnika "najmanje privilegija" i dinamičke kontrole pristupa. Ovo uključuje proveru autentičnosti i autorizaciju zahteva za informacijama ili sistemima zasnovanim na kontekstualnim informacijama kao što su informacije o autentifikaciji, korisnički identiteti, podaci o korisničkom krajnjem uređaju i klasifikacija podataka;
f) uvek provera autentičnost lica koje je uputilo zahtev i uvek potvrđivanje zahteva za autorizaciju informacionim sistemima na osnovu informacija uključujući informacije o autentifikaciji i korisničke identitete, podatke o korisničkom krajnjem uređaju i klasifikaciji podataka, na primer, nametanje jake autentifikacije (npr. višefaktorska autentifikacija).

7.6 TEHNIČKE RANJIVOSTI SISTEMA

Za smanjenje rizika od iskorišćavanja objavljenih tehničkih slabosti, kompanija implementira upravljanje tehničkim ranjivostima, kao efikasnu, sistematsku i redovnu proceduru sa merljivom efikasnošću. U razmatranje se uzimaju operativni sistemi i sve ostale aplikacije.

U cilju postavljanja efikasnog procesa upravljanja tehničkim ranjivostima, moraju se poštovati sledeća uputstva:

- Organizacija definiše i uspostavlja uloge i odgovornosti kao i upravljanje tehničke ranjivostima, procenu rizika, nadogradnje,
- Identifikuju se sistemi (softver i ostale tehnologije) koji se koriste u identifikaciji važnih tehničkih ranjivosti. Lista ovih sistema se ažurira u saglasnosti sa promenama sredstava, ili kada se pronađu novi korisni resursi.

- Definiše se vremenski period aktivnosti koje obaveštavaju o potencijalno važnim tehničkim ranjivostima.
- Jednom kad je potencijalna ranjivost identifikovana, organizacija identifikuje ostale rizike, kao i akcije koje se trebaju sprovesti. Ove akcije obuvhvataju popravku ranjivoga sistema i primenu ostalih kontrola.
- U zavisnosti od hitnosti rešavanja tehničke ranjivosti, preuzima se akcija u skaldu sa kontrolom upravljanja izmenama, ili u skladu sa procedurama za odgovor na bezbednosne incidente.
- Ako je zakrpa, popravka, dostupna, procenjuje se rizik od implementacije te zakrpe,
- Zakrpe se testiraju i ocenjuju pre njihove instalacije, kako bi se obezbedilo da su one efikasne i da nemaju propratne efetke koji se ne mogu tolerisati. Ako zakrpa nije dostupna, potrebno ja razmotriti ostale kontrole kao što su:
  - ❖ Isključiti servise i sisteme na koje se odnosi ranjivost,
  - ❖ Prilagoditi ili dodati kontrole pristupa ,
  - ❖ Pojačati praćenje kako bi se detektiovali ili sprečili napadi,
  - ❖ Pojačati svest o postojećoj ranjivosti, putem infrormisanja svih dotičnih strana.
- Čuva se audit zapis o svim aktivnostima,
- Proces upravljanja tehničkim ranjivostima se redovno posmatra, proverava i ocenjuje, kako bi se obezbedila efikasnost i efektivnost,
- Prvo se moraju adresirati sistemi sa visokim rizikom.

Na nivou operativnih sistema, testiranje i autorizacija ažuriranja i popravki (updates and patches) se radi od strane IT podrške. Instalacija autorizovanih zakrpa po radnim stanicama se radi automatski i kontrolisano je domenskim politikama.

Na serverima, inslataciju vrše ovlašćeni administratori u periodima smanjene aktivnosti na serverima.

8 ODGOVORNOSTI I OVLAŠĆENJA

ISMS Menadžer je odgovoran za sprovođenje ove procedure u saradnji sa IT podrškom kao i za nadzor nad njihovim radom u vezi sa planiranjem i organizovanjem aktivnosti. Za kontrolu primene politike ovlašćen je Direktor.

9 ZAPISI

Sve informacije vezane za dokumentovani postupak upravljanje uvođenjem, razvojem i održavanjem informacionih sistema 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.