POVJERLJIVO

Bioinstitut d.o.o.
Korporativna sigurnost

Politika sigurnosti informacijskog sustava Bioinstitut d.o.o.

Izradio:	Nikola Patafta, mag. inf., viši savjetnik
Provjerio:	Matija Bogdan, glavni koordinator
Odobro	Saša Legen, direktor
Datum:	10.12.2024.

1. UVOD

1.1. Opseg i svrha dokumenta

Informacije su jedan od najvažnijih i najdinamičnijih elemenata u gospodarstvu te predstavljaju važan čimbenik u razvoju poslovanja i upravljanju.

Podaci i ostale informacije u vlasništvu Bioinstitut d.o.o.neovisno o tome kako se podaci ili informacije obrađuju, kako se njima upravlja ili na koji se način pohranjuju, uključujući sve sustave i naprave za prikupljanje, obradu, pohranu ili prijenos podataka ili informacija, smatraju se informacijskom imovinom Bioinstitut d.o.o.(u daljnjem tekstu: “Tvrtka”). Imajući na umu sve zajedno, ukupni zbir tih informacijskih imovina definira se kao "informacijska imovina tvrtke Bioinstitut d.o.o.“. Ta imovina je kao čimbenik konkurentnosti od ključne važnosti koja usmjerava donošenje strateških i taktičkih odluka i služi kao podrška poslovnim procesima Tvrtke.

U današnje vrijeme brzih promjena na tržištu i velikoj dinamičnosti, tehnološki razvoj ubrzava i olakšava prikupljanje i obradu informacija koje služe za unapređenje gospodarskih ciljeva Tvrtke.

Sve veća konkurencija potiče na traženje novih oblika odnosa s klijentima. S tim u vezi preferiraju se rješenja koja se temelje na najnovijim tehnologijama kao i razvoj inovativnih rješenja za prikupljanje i obradu stalno rastuće količine informacija.

Zbog toga je neophodno kontinuirano pratiti inovacije kako bi se brzo mogle osmisliti, planirati i primijeniti prikladne mjere za smanjenje i prevenciju rizika.

To će omogućiti primjereni odgovor na rastuće potrebe za sigurnošću, a koje se tiču klijenata, uz istovremenu zaštitu korporativnih vrijednosti i konkurentske prednosti.

Zaštita informacija i sigurno upravljanje informacijama također su važan čimbenik za sve strožu državnu i međunarodnu zakonsku regulativu koja zahtijeva takve vrste djelovanja, kontrolnih sustava i postupaka koji se usredotočuju na zaštitu informacija, kao i organizaciju istih na bazi cijele Tvrtke.

Zaštita informacijske imovine Tvrtke i zbog toga dobiva stratešku važnost te je temeljena na razvoju prikladnih standarda za upravljanje potrebnim organizacijskim, tehnološkim i regulatornim postupcima.

Ovaj dokument je sastavni dio grupe sigurnosnih standarda tvrtke Bioinstitut d.o.o.i sadrži zaštitne mjere koje se moraju usvojiti kako bi se zaštitila informacijska imovina

Tvrtke i odredio standard za organizaciju sustava upravljanja informacijskom sigurnošću.

1.2. Sadržaj dokumenta

Ovaj dokument predstavlja referentne smjernice o informacijskoj sigurnosti te postupke koji se moraju pokrenuti kako bi se zajamčilo ostvarivanje ciljeva tvrtke Bioinstitut d.o.o.u svrhu zaštite informacijske imovine Tvrtke.

Te se smjernice moraju primjenjivati kako je navedeno u dokumentu, osim u slučajevima kad su za određena područja definirana dodatna i/ili detaljnija pravila.

Ovaj je dokument podijeljen u poglavlja koja opisuju područja na kojima se moraju uspostaviti i početi primjenjivati mjere za zaštitu informacijske imovine Tvrtke.

Spomenute zaštitne mjere bi se trebale primjenjivati prema stupnju važnosti informacijske imovine u poslovanju Tvrtke, procjenjujući njihov stupanj povjerljivosti, integriteta i dostupnosti, kao i okruženje u kojima se koriste.

Načini primjene moraju biti u skladu s tehnološkim standardima na tržištu i procijenjenim rizicima te se moraju temeljiti na postupcima koji uključuju faze planiranja, implementacije, pregleda i poboljšanja.

Smjernice sadrže sigurnosne odredbe koje su usklađene s međunarodnim standardima ISO/IEC 27001:2005 i ISO/IEC 27002:2005, a koje istovremeno ne isključuju usvajanje daljnjih, možda strožih sigurnosnih mjera. Osim sadržaja ovog dokumenta, mora se osigurati i sukladnost s odredbama svih novih primjenjivih zakona, kao i s odlukama regulatornih tijela ili internim smjernicama i/ili pravilima postupanja.

Rječnik, koji je sastavni dio ovog dokumenta, daje definicije ključnih termina iz ovog dokumenta kako bi se osigurala jednoznačno, nedvosmisleno značenje.

1.3. Kome je dokument namijenjen

Ovaj je dokument namijenjen svim izvršnim instancama tvrtke Bioinstitut d.o.o., koje su odgovorne za osmišljavanje i, na vodećim funkcijama, provedbu radnji organizacijske, pravne i tehnološke prirode kako bi se osigurala zaštita informacijske

imovine u aktivnostima koje su povezane s određenim zadacima spomenutih izvršnih instanci, kao i svim trećim stranama koje imaju pristup spomenutoj imovini.

2. ORGANIZACIJA INFORMACIJSKE SIGURNOSTI

Učinkovita organizacija informacijske sigurnosti mora uključivati: nacrt i pravilno upravljanje aktivnostima, procesima, ulogama i odgovornostima; primjenu prikladnih kontrolnih mjera i mjera preispitivanja; održavanje i daljnji razvoj zaštitnih mjera, usklađivanje spomenutih aktivnosti, procesa, uloga i odgovornosti s poslovnim ciljevima te objavljivanje i ažuriranje sigurnosnih pravila.

2.1. Organizacijski model sigurnosti informacijske imovine

Mora se razviti takav organizacijski model koji sadrži potrebne zaštitne mjere, definira koje su funkcije Tvrtke uključene i na koji način one međusobno djeluju unutar sustava sigurnosti informacijske imovine, te dodjeljuje odgovornosti kako bi se osigurala pravilna primjena modela, stalni nadzor i provjera mjera, te kako bi se pružila potpora rukovodstvu u usmjeravanju sigurnosnih pravila.

2.1.1 Dodjela uloga i odgovornosti

Uloge i odgovornosti u upravljanju informacijskom sigurnosti moraju biti dodijeljene na takav način da se osigura homogeni pristup kroz cijelu Tvrtku na različitim upravljačkim razinama, uz istovremeno obuhvaćanje zaštite informacijske imovine Tvrtke.

Smjernice:

a) osigurati objedinjeni pogled, identificirati strateške smjernice, i usmjeravati sigurnosne inicijative (npr. točna dodjela ovlaštenja i odgovornosti i definiranje politika za upravljanje rizicima), uz istovremenu dodjelu pripadajućih zadataka organizacijskom tijelu koje uključuje i predstavlja izvršni menadžment, te objedinjavati specifične vještine vezane uz informacijsku sigurnost;
b) dodijeliti dobro definirane odgovornosti, u skladu s trenutno važećom zakonskom regulativom, kako bi se osiguralo prikladno pokrivanje svih potrebnih uloga i položaja u organizaciji upravljanja sigurnošću, u upravljanju rizicima i kontrolingu, kao i u planiranju, primjeni, radu i nadzoru protumjera koje su usvojene s ciljem zaštite informacijske imovine Tvrtke;
c) definirati i tijekom vremena uskladiti odnose među organizacijskim dijelovima (osiguravajući neovisnost kontrole i onog koji provodi navedenu kontrolu),

funkcionalnim operativnim poslovnim procesima i autonomijom proračuna i odgovornosti, kao i imenovati ovlaštenike i načine za upravljanje sigurnosnim rizikom;
d) dodijeliti dobro definirane odgovornosti za upravljanje sigurnošću, uzimajući u obzir pripadajuće zakonske akte, organizacijskim dijelovima koji razvijaju informacijske sustave i njima upravljaju;
e) dodijeliti odgovornosti kako bi se osigurala primjena internih pravila i onih zakonskih odredbi ili propisa koji se tiču sigurnosti;
f) odrediti odgovornosti i mehanizam za osiguravanje upravljanja izvanrednim sigurnosnim događajima i kriznim situacijama u skladu s regulatornim zahtjevima;
g) povezati i formalizirati administratorske račune s listom aktivnosti koje obavljaju;

2.1.2 Aktivnosti upravljanja sigurnošću

Moraju se odrediti aktivnosti kako bi se osiguralo trajno upravljanje aspektima koji su povezani sa zaštitom informacijske imovine Tvrtke.

Smjernice:

a) iznijeti ciljeve i strategije koji se tiču sigurnosti. Posebice, konačna odgovornost za razvoj strategija i politika za upravljanje rizikom je na direktoru Tvrtke;
b) osigurati homogeni pristup sigurnosti i upravljanju rizikom unutar Tvrtke, uključujući usklađivanje aktivnosti unutar Tvrtke kako bi se osigurao stalni stupanj pouzdanosti u sigurnosnim sustavima, u skladu s izdanim smjernicama Uprave Tvrtke:
c) uspostaviti i formalizirati metodologiju, u skladu s trenutno važećim politikama, pravilnicima i standardima, kojom će se voditi stvaranje sustava upravljanja informacijskom sigurnošću i nadzirati njegova dugoročna učinkovitost i djelotvornost;
d) uspostaviti metodologiju za analizu rizika informacijskog sustava, uzimajući u obzir trenutno važeće regulatorne zahtjeve, i primijeniti istu na poslovne procese i imovinu, uz istovremenu procjenu stupnja važnosti informacija koje su povezane s kriterijem povjerljivosti, integriteta i dostupnosti;
e) identificirati prikladne protumjere (fizičke, tehnološke i organizacijske) za različite razine rizika, provjeravajući i kontrolirajući pravilno održavanje uspostavljenih razina sigurnosti, u skladu s trenutno važećim zakonskim aktima;
f) osigurati, uspostavljajući politike i procedure, adekvatnu edukaciju osoblja o pitanjima sigurnosti na svim nivoima (npr. u sustavu unutarnjih kontrola), kao i razviti pojačanu svijest i osjetljivost na tu temu, pružajući adekvatne informacije zaduženim upravljačkim tijelima;
g) provjeriti i pregledati pravilnu primjenu uspostavljenih pravila, kao i pridržavanje istih, uz njihovu zamjenu drugim pravilima po potrebi;

h) nadgledati odnose s vlastima i vladinim i nevladinim tijelima i/ili agencijama (regulatorno tijelo, agencije za provedbu zakona/izvršni organi, trgovačka društva), uz istovremeno osiguravanje stalnog ažuriranja i dublje analize pitanja sigurnosti;
i) uspostaviti metodologiju radi uključivanja sigurnosnih stručnjaka tijekom planiranja i izvođenja projekta, kako za primijenjene tako i za tehnološke projekte, te radi osiguranja potpore funkcijama unutarnje kontrole prilikom njihove provjere;
j) jednom godišnje potvrditi da su uspostavljene minimalne sigurnosne mjere za zaštitu osobnih podataka sukladno zakonskoj regulativi.

2.1.3 Postupak uspostave, primjene i ponovne procjene sigurnosnih pravila

Postupak uspostave i ponovne procjene sigurnosnih pravila mora biti razvijen na takav način da osigura stalnu primjenu, prikladnost i učinkovitost istih.

Smjernice:

a) dodijeliti odgovornosti za definiranje, provjeru, izdavanje i ažuriranje sigurnosnih pravila nadležnim instancama koje se razlikuju od onih koje su odgovorne za upravljanje sigurnošću Tvrtke;
b) odrediti i dodijeliti odgovornosti za provjeru i ažuriranje izdanih sigurnosnih pravila;
c) izvršiti periodične provjere radi procjene učinkovite primjenjivosti takvih sigurnosnih pravila, njihove iscrpnosti i potrebe za ažuriranjem;
d) pravovremeno ažurirati sigurnosna pravila kao odgovor na svaku promjenu u specifičnom području primjene (npr. pravni, operativni, tehnološki kontekst ili kontekst u vezi s rizikom);
e) evidentirati, dijeliti i dostaviti na odobrenje svaku vrstu promjene ili nadopune sigurnosnih pravila, naknadno osiguravajući njihovo izdavanje u skladu s uspostavljenim najmodernijim praksama.

3. SIGURNOST U UPRAVLJANJU LJUDSKIM RESURSIMA

Sustav upravljanja informacijskom sigurnošću ne može se odvojiti od njegovog osnovnog elementa: ljudi koji rade s informacijskom imovinom Tvrtke, bez obzira radi li se o internim zaposlenicima ili ugovornim partnerima. Aspekti sigurnosti koji imaju utjecaj na upravljanje ljudskim resursima naglašavaju se tijekom cijelog radnog vijeka zaposlenika, od trenutka kada se pripremi ugovor o radu, kroz promjene u ulogama i opisu posla pa sve do raskida ugovora o radu.

3.1. Sigurnost u odabiru ljudskih resursa i upravljanju istima

Kao aktivni sudionici u procesu zaštite informacijske imovine Tvrtke, zaposlenici moraju biti propisno odabrani i informirani u odnosu na svoje različite operativne funkcije i odgovornosti koje se tiču informacijske sigurnosti kako bi se pravila o sigurnosti mogla na propisan način primijeniti tijekom izvršenja dodijeljenih poslovnih aktivnosti.

3.1.1. Odabir ljudskih resursa i upravljanje istima

Prikladne provjere potencijalnih zaposlenika moraju se temeljito provesti, bez obzira na to koji se položaj nudi određenoj osobi, i to tijekom faze selekcije zaposlenika, kao i uvijek kada se novom zaposleniku povjere različiti i/ili specifični zadaci ili uloge.

Smjernice:

a) osigurati da kandidat posjeduje adekvatne reference, osobne i profesionalne, a koje su u vezi s radnim mjestom na kojem će biti zaposlen i u skladu s trenutnim regulatornim zahtjevima;
b) uspostaviti proceduru za regulaciju dodjele opreme i osobnih identifikacijskih dokumenata osoblju. Zaposlenik mora imati i kopiju sigurnosnih pravila koja su obvezatna za određenog zaposlenika;
c) osigurati i nadzirati, tijekom radnog vijeka zaposlenika, da zaposlenik obavlja aktivnosti u skladu sa sigurnosnim pravilima.

3.1.2. Odgovornosti koje se tiču informacijske sigurnosti

Odgovornosti za upravljanje informacijama tijekom obavljanja korporativnih poslova moraju biti formalizirane kako bi se omogućio kontinuirani nadzor i kontrola sigurnosti informacijske imovine.

Smjernice:

a) odrediti aktivnosti, procese i procedure za rukovanje i obradu svih informacija namijenjenih za potporu poslovanju Tvrtke
b) odrediti i formalizirati opće i specifične odgovornosti za zaštitu informacija;
c) odvojiti i razlikovati odgovornosti vezane za autorizaciju procesa od aktivnosti upravljanja i operativnih aktivnosti
d) osigurati mogućnost zamjene kritičnih resursa upravljanja sigurnošću

3.1.3. Svijest i edukacija o informacijskoj sigurnosti

Kako bi se smanjili rizici povezani s greškama u rukovanju ili obradi informacija, zaposlenici trebaju postati svjesni (putem specifičnih periodičkih edukativnih programa i prenošenja informacija prema njihovim ulogama i odgovornostima koje se tiču sigurnosti) važnosti strogog poštivanja i primjene pravila o sigurnosti.

Smjernice:

a) razviti i ažurirati edukacijske seminare o pravilnoj uporabi informacijskog sustava , sigurnosnim pravilima koja su na snazi, zahtjevima, procjenama i kontrolama koji se tiču sigurnosti, te potencijalnim prijetnjama;
b) osigurati da zaposlenici dobiju dodatnu obuku svaki put kada nastupe promjene koje se tiču njihovih uloga ili opisa posla, te da vode evidenciju o sudjelovanju zaposlenika na tečajevima;
c) razviti i uspostaviti metodologije ili procedure kako bi se osiguralo da sigurnosna pravila i svi dodaci te ažurirane nadopune budu u svako doba dostupne zaposlenicima.

3.1.4. Radni odnos i ugovori s vanjskim partnerima

Ugovori između Tvrtke i zaposlenika ili Tvrtke i vanjskih partnera moraju sadržavati odredbe kojom se štiti povjerljivost i integritet informacijskog sustava tvrtke, uz navođenje sankcija za uzrokovane štete, neovlaštenu uporabu ili prenošenje imovine

neovlaštenim primateljima. Spomenute ugovorne odredbe vrijedit će tijekom cijelog roka trajanja ugovora, posebice u slučaju promjena u ulogama ili opisu posla, kao i po raskidu ugovornog odnosa.

Smjernice:

a) prije nego što dobiju slobodan pristup informacijskom sustavu Tvrtke, svi zaposlenici moraju potpisati obvezujući sporazum o povjerljivosti prema kojem se obvezuju čuvati integritet i dostupnost informacijskog sustava;
b) revidirati gore navedene odredbe u slučaju promjena u radnom odnosu ili ugovornim uvjetima ili pak u slučaju svake promjene internih korporativnih pravila, pravnih odredbi ili drugih zahtjeva;
c) procijeniti mogućnost provedbe kontrola nad dobavljačima ili općenito vanjskim partnerima kako bi se provjerila njihova pouzdanost u slučaju da im se povjere uloge koje povlače za sobom interakciju s Tvrtkom;
d) održavati stalni nadzor kako bi se osiguralo da zaposlenici i vanjski partneri poštuju važeća sigurnosna pravila u skladu s ugovornim odredbama i uvjetima;
e) razviti i usvojiti prikladne disciplinske postupke u skladu s primjenjivim zakonima i obvezujućim ugovornim odredbama, a koji se moraju primijeniti u slučaju povrede ili kršenja sigurnosnih pravila;
f) svi zaposlenici trebaju potpisati izjavu da su pročitali i razumjeli pravila i procedure vezane za korporativnu sigurnost;
g) ugovori s vanjskim partnerima trebaju sadržavati odredbe da su upoznati s važećom regulativom vezanom za sigurnost.

3.1.5. Raskid ili promjena radnog odnosa

Raskid radnog odnosa ili ugovornog odnosa s vanjskim partnerom mora se provesti na pravilan način kako bi se osigurao povrat sve imovine Tvrtke i ukidanje svih pristupnih prava.

Promjena odgovornosti ili radnog odnosa u Tvrtki mora se provesti na takav način da se osigura da dodijeljena oprema i pristupnih prava informacijama budu u skladu s novim opisom posla.

Smjernice:

a) dodijeliti odgovornosti za pravovremeno prikupljanje informacija o raskidu ugovora s Tvrtkom kako bi se osigurao početak svih s time povezanih postupaka;

b) razviti postupak kojim se regulira povrat opreme Tvrtke i svi načini osobne identifikacije koji su povezani s Tvrtkom;

c) razviti postupak kojim se regulira ukidanje pristupnih prava;

d) u slučaju da zaposlenik ili treća strana promijeni opis posla ili se premjesti na neku drugu poziciju unutar Tvrtke, bez promjena u opisu posla, potrebno je osigurati da prethodna oprema i pristupna prava budu povučena te da se dodijele nova oprema i pristupna prava u skladu s novim zadatkom.

4. FIZIČKA SIGURNOST

Učinkovita zaštita informacijskog sustava zahtijeva pravilnu skrb o fizičkoj sigurnosti. Neadekvatnost na tom području može izazvati povredu sigurnosti informacijskog sustava Tvrtke, kao i ugroziti učinkovitost ostalih kontrolnih mjera.

Smjernice o fizičkoj sigurnosti u ovom poglavlju usklađene su sa zahtjevima kontrola i odredbama koje sadrži standard ISO 27001.

4.1. Zaštita fizičkih objekata

U svrhu zaštite poslovnih objekata i imovine Tvrtke od uništenja, oštećenja, otuđenja i drugih vidova ugrožavanja te sprječavanja neovlaštenog pristupa mora se odrediti i uspostaviti sustav fizičke kontrole pristupa zajedno sa svim sigurnosnim perimetrima (zonama fizičke sigurnosti). Posebna pažnja se mora obratiti na područje sistem sale i na sve ostale prostorije u kojima se nalazi pomoćna oprema, a koja je dio informacijskog sustava Tvrtke (npr. oprema koja osigurava visoku pouzdanost i pravilno funkcioniranje sustava).

4.1.1. Zone fizičke sigurnosti

Zone fizičke sigurnosti moraju se dobro planirati i uspostaviti na takav način da štite, putem odgovarajućih sigurnosnih mjera, objekte Tvrtke i područja koja sadrže informacijsku imovinu Tvrtke.

Smjernice:

a) kontinuirane, neprekinute sigurnosne zone moraju biti tako osmišljene da razgraničuju područja kojima je potrebna zaštita na temelju stupnja tajnosti ili kritičnosti informacijskog sustava ili specifičnih aktivnosti koje se provode na tom području;
b) zaštitne mjere moraju se planirati na takav način da budu usklađene što se tiče vrste, robusnosti i učinkovitosti s vrstom područja koje razgraničuju te imovinom koja se nalazi unutar tog područja, u skladu s trenutno važećim zakonskim smjernicama uzimajući u obzir upravljanje podacima;
c) odrediti kriterije za smještaj opreme koja je dio informacijskog sustava Tvrtke na sigurnom području na temelju razine klasifikacije opreme i informacija.

4.1.2. Zaštita sigurnih područja

Moraju se planirati i primijeniti kontrole radi regulacije pristupa u sigurna područja.

Smjernice:

a) postojanje i lokacija sigurnih područja, funkcije koje se obavljaju unutar tih područja i razina (stupanj) klasifikacije imovine koja se nalazi u tim područjima smatraju se povjerljivom informacijom te se povjeravaju osoblju samo ukoliko je to doista neophodno;
b) moraju se definirati procedure kojima će se regulirati pristup sigurnim područjima:
c) nadzirati akcije zaposlenika koji ne rade u sigurnim područjima, dopuštajući minimalni pristup samo ako je on doista neophodan uz istovremeni nadzor aktivnosti zaposlenika koji djeluju na sigurnim područjima.

4.2. Fizičke kontrole ulaza

Sigurna područja, posebno prostorije sistem sale, moraju biti zaštićene propisnim kontrolama ulaza kako bi se osigurao pristup samo ovlaštenih zaposlenika.

4.2.1. Kontrole ulaza

Moraju se primijeniti kontrolne mjere kojima se osigurava pristup u sigurna područja samo ovlaštenim zaposlenicima.

Smjernice:

a) planirati i primijeniti sve potrebne protumjere kako bi se spriječio neovlašten pristup prostorije Tvrtke;
b) definirati različita prava pristupa za različite tipove korisnika (npr. zaposlenici Tvrtke, stalni ugovorni partneri, povremeni ugovorni partneri, gosti/posjetitelji) i na temelju stupnja kritičnosti područja i imovine koja se nalazi na tim područjima;
c) odrediti minimum informacija za registraciju ulaza i izlaza korisnika;
d) odrediti pravila za izdavanje, zadržavanje, istek, prikaz i povrat korisničkih identifikacijskih iskaznica te osigurati da zaposlenici Tvrtke, zaposlenici ugovornog partnera i posjetitelji dobiju takve iskaznice;

e) odobriti autorizaciju za pristup u sigurno područje samo zaposlenicima s opravdanom poslovnom potrebom, nadzirući njihove ulaze i izlaze pomoću propisne registracije i mehanizama za praćenje;
f) trenutno poništiti prava pristupa u sigurna područja u slučaju svakog nepoštivanja procedure pristupa korisnika;
g) provjeriti i pregledati sva prava pristupa barem jednom godišnje;
h) odrediti načine osobne identifikacije za pomoćno servisno osoblje (radnici iz službe za održavanje, službe za čišćenje i sl.)

4.2.2 Sigurnost područja za dostavu i utovar

Sigurna područja moraju biti odijeljena od područja za dostavu i utovar. Područja za dostavu i utovar moraju imati primjerenu kontrolu i mjere zaštite.

Smjernice:

a) organizirati područja za utovar materijala i opreme na takav način da se maksimalno odvoje od sigurnih područja;
b) pristup područjima za dostavu i utovar smije se dozvoliti samo identificiranim i ovlaštenim osobljem;
c) definirati odredbe kojima će se dozvoliti pregled materijala i opreme koji se dostavlja i otprema u skladu s važećim zakonima i propisima.

4.3. Infrastruktura i sustavi podrške

Prostorije koje sadrže informacijsku imovinu moraju se planirati, uspostaviti i zaštititi te se moraju usvojiti prikladne mjere kako bi se osigurala zaštita i propisno funkcioniranje pomoćne opreme i pomoćnih sustava.

4.3.1. Sigurna područja

Moraju se usvojiti prikladne sigurnosne mjere što se tiče odabira, planiranja, dizajna područja i upravljanja područjima (uredima, prostorijama, objektima i sl.) koja sadrže informacijsku imovinu.

Dodatno, moraju se definirati i provesti sve potrebne mjere da se zaštite ta područja od potencijalne štete uslijed okolišnih ili vanjskih utjecaja.

Smjernice:

a) definirati i redovito ažurirati plan prostorija sistem sale i područja koja sadrže pomoćnu opremu ili pomoćne sustave;
b) definirati pravila (npr. zabranjena konzumacija jela i pića) kako bi se spriječila šteta na pomoćnoj opremi ili pomoćnim sustavima od strane korisnika koji su ovlašteni za ulazak u prostorije sistem sale ili područja koja sadrže opremu za podršku ili pomoćne sustave;
c) odvojiti pomoćnu opremu (npr. fotokopirni uređaj, faks) kako bi se spriječio neovlašteni pristup na sigurna područja;
d) pohraniti opće materijale i zalihe u namjenskim prostorijama koje su odvojene od prostorija sistem sale,vodeći posebnu brigu o tome da se na prikladan način te u skladu s primjenjivim zakonima, propisima ili standardima rukuje i pohrane eventualno opasni (npr. zapaljivi) materijali;
e) moraju se zaštititi vanjske pristupne točke kako bi se osigurala područja u prizemlju, i to pomoću mehanizama za zaštitu od provala;
f) prilikom odabira ili definiranja (izrade nacrta) sigurnih područja, planirati ili ispitati postojanje prikladnih sigurnosnih mjera za zaštitu imovine;
g) planirati prikladnu pomoćnu infrastrukturu za objekte u kojima se nalaze prostorije sistem sale kao i za područja koja sadrže kritičnu imovinu kako bi se osigurala adekvatna zaštita od okolišnih ili vanjskih utjecaja, poput neovlaštenog pristupa, požara, poplave, nestanka struje, kvarova klima uređaja i sl.

4.3.2. Smještaj opreme i zaštita

IT oprema mora biti smještena i zaštićena s obzirom na razinu klasifikacije informacija koje su na njoj pohranjene i koja se pomoću nje obrađuje kako bi se osiguralo pravilno funkcioniranje opreme.

Smjernice:
a) postaviti IT opremu, telekomunikacijsku opremu i pomoćnu opremu u skladu s optimalnim kriterijima obzirom na prostorne mogućnosti, instalacije i održavanje uvjeta visoke pouzdanosti;
b) instalirati IT opremu, telekomunikacijsku opremu i pomoćnu opremu u skladu s najboljom praksom, uputama proizvođača te smjernicama;
c) odrediti i dokumentirati zahtjeve pomoćnih sustava kako bi se mogla osigurati visoka pouzdanost IT opreme, uzimajući u obzir upute proizvođača i karakteristike okoliša u kojem su sustavi smješteni;

d) odabrati pomoćne sustave koji zadovoljavaju zahtjeve koji se tiču pouzdanosti i dostupnosti, te primijeniti prikladne kontrolne mjere kako bi osigurali spomenuti zahtjevi;
e) održavati pomoćne sustave u savršenom radnom stanju kako bi se osigurala visoka pouzdanost, planirati prikladne radove održavanja s ovlaštenim zaposlenicima, te izvršavati periodična testiranja sustava simuliranjem rada u slučaju nužde u skladu s proizvođačevim uputama za održavanje;
f) osigurati propisno dimenzioniranje i procjenu pomoćnih sustava kako bi se pružila podrška radu svih ovisnih sustava, testirati kapacitet spomenutih pomoćnih sustava kako bi podržale odstupanja u konfiguraciji sustava, trajanju rada i kapacitetu;
g) ograničiti fizički pristup mrežnoj opremi (vatrozidi, usmjernici, pristupne točke bežičnih mreža, itd.) i mobilnim uređajima samo ovlaštenim zaposlenicima.

4.3.3. Zaštita od vanjskih prijetnji i prijetnji iz okoliša

IT oprema mora biti zaštićena od prekida u opskrbi el. energijom, od električnih anomalija ili drugih vanjskih prijetnji ili prijetnji iz okoliša osiguravanjem prikladnih mehanizama.

Smjernice:

a) identificirati opremu i sustave za koje je potrebna neprekinuta opskrba električnom energijom te osigurati stalni dotok električne energije. to se može primjerice postići uspostavljanjem veza s alternativnim izvorima energije;
b) priskrbiti prikladne sustave za regulaciju električne energije, odrediti prikladna testiranja njihovog načina funkcioniranja i provoditi redovita održavanja kako bi se osigurao konstantan i pravilan rad;
c) prema potrebi opremiti zgrade sa sustavima za zaštitu od električnih izboja ili prenapona;
d) zaštititi komunikacije i komponente sustava opskrbe električnom energijom od eventualnog vandalizma, sabotaže ili kvarenja, usvajajući protumjere koje su prikladne za specifične razine rizika.

4.3.4. Zaštita električnih i mrežnih vodova

Električni vodovi, linije za prijenos podataka te audio prijenos moraju biti zaštićeni od šteta, prekida i presijecanja signala.

Smjernice:

a) postaviti upravljačke ploče za linije za električni prijenos, audio prijenos i prijenos podataka na zaštićenim područjima;
b) planirati mjere fizičke zaštite za električni prijenos, audio prijenos i prijenos podataka na zaštićenim područjima kako bi se spriječile štete na linijama ili prekid signala.

5. LOGIČKA SIGURNOST

Niže su navedene smjernice za usvajanje skupa tehničkih, organizacijskih i regulatornih mjera radi zaštite informacijskog sustava tvrtke Bioinstitut d.o.o.Sustavna primjena tih mjera osigurava kontrolu logičkog pristupa i sprečavanje neovlaštenog pristupa informacijskom sustavu.

Pristup informacijama u elektronskom obliku („logički pristup“) ovisi o postojanju i uporabi *korisničkih računa (credentials),* koji se sastoje od *korisničkog imena (userID, username)* i povjerljive komponente koja može biti kombinacija jedne ili više značajki u obliku:

- nečega što je poznato korisniku (npr. zaporka ili PIN);
- nečega što korisnik posjeduje (npr. pametna kartica, token);
- nekog biometrijskog obilježja korisnika (npr. otisak prsta, uzorak šarenice oka).

Komplet korisničkih prava pristupa predstavlja pristupni korisnički profil koji se korisniku dodijeli tijekom faze izrade profila u skladu s ustaljenim pravilima.

Kontrola logičkog pristupa uključuje sljedeće korake:

- ***identifikaciju***: Proces prepoznavanja korisnika putem provjere postojanja u sustavu preko predočenog korisničkog imena;
- **autentifikacija** (*potvrđivanje):* Postupak u kojem se podaci koje pruži identificirani korisnik uspoređuju s oni podacima koji su memorirani u sustavu kako bi se osiguralo da je navedeni korisnik u stvarnosti taj ili to za koga ili za što se predstavlja;
- ***autorizacija*****:** Postupak dodjele, ili automatske provjere, dozvole nekog korisnika da pristupi zatraženoj informaciji nakon što je korisnik potvrđen.

Regulacija logičkog pristupa ujedno povlači za sobom sposobnost da se rekonstruira svaki pristup i korištenje informacije pomoću mehanizama koji snimaju ili evidentiraju uporabu informacija.

Logička sigurnost se također postiže putem uporabe tehnika šifriranja (enkripcije) informacija kako bi se zaštitila povjerljivost i integritet informacija te osiguralo priznavanje operacija provedenih sa spomenutom informacijom.

5.1. Opći zahtjevi vezani za logičku sigurnost

Pristup informacijskom sustavu mora se odrediti na temelju potreba koje su povezane s operativnim aktivnostima korisnika. Nadalje, upravljanje spomenutim pristupom i njegova kontrola mora se provoditi odgovarajućim instrumentima ili postupcima (procesima) koji osiguravaju da ovlašteni korisnici mogu pristupiti samo informacijama koji su im neophodni za provedbu dodijeljenog zadatka, tj. funkcije.

5.1.1. Temeljni čimbenici u kontroli pristupa

Metode određivanja, dodjele i upravljanja pristupnim korisničkim računima te prikladni pristupni korisnički profili moraju osigurati da se pristup dozvoli samo za onu informaciju koja je neophodna za provedbu zadatka koji je dodijeljen korisniku.

a) osigurati uspješno izvršavanje koraka identifikacije, autentikacije i autorizacije prije nego što se dozvoli logički pristup informaciji koja nije javna;
b) razviti postupak (proceduru) za stvaranje, trajno upravljanje i opoziv korisničkih računa;
c) dodijeliti korisničko ime svakom korisniku informacijskog sustava. Korisničko ime mora biti osobna i nedvosmislena identifikacija u informacijskom sustavu Tvrtke te se ne smije dodjeljivati nekom drugom korisniku u slučaju opoziva;
d) uspostaviti procese i instrumente za definiranje i upravljanje pristupnim korisničkim profilima i s time povezanim pravilima za korisnike na temelju usvojenog modela izrade profila;
e) ažurirati korisničke račune i pristupne korisničke profile kada god postoje varijacije u operativnim potrebama;
f) provjeriti valjanost korisničkih računa i pristupnih korisničkih profila na strukturirani i ponavljajući način, uzimajući u obzir ulogu i opis posla korisnika te u skladu s primjenjivim propisima;
g) u slučajevima kada je nadležna instanca za pristupne korisničke profile eksternalizirana, formulirati prikladnu ugovornu odredbu kako bi se osiguralo da se pravila upravljanja pristupnim korisničkim profilima primjenjuju na pravi način te da je moguće provjeriti i potvrditi metode upravljanja koje koristi vanjski suradnik;
h) voditi evidenciju o izvršenim aktivnostima (poslovima) na informaciji na temelju razine klasifikacije spomenute informacije.

5.2. Identifikacija i potvrđivanje

Moraju se uspostaviti metodologije za definiranje, neprekinuto upravljanje i poništavanje (ukidanje) korisničkih računa.

5.2.1. Upravljanje korisničkim računima

Moraju se pripremiti procedure za definiranje, neprekinuto upravljanje i ukidanje korisničkih računa.

Smjernice:

a) uspostaviti metode za definiranje, neprekinuto upravljanje, onemogućavanje i ukidanje korisničkih računa;
b) odrediti korisničke račune koji su ekskluzivni i nedvojbeni čitavo vrijeme.
c) dodijeliti korisničke račune na takav način da se osigura nedvojbena veza sa specifičnim korisnikom:
d) odrediti korisnička imena na razini Tvrtke na temelju specifične „konvencije o imenovanju“
e) osigurati da znanje o korisničkom imenu ni na koji način ne može dovesti do otkrivanja prava pristupa korisnika;
f) odrediti zaštitne mjere i procedure omogućavanja za novo osmišljene korisnike kako bi se spriječila nepropisna uporaba pristupnih privilegija;
g) udovoljiti zahtjevima za ponovno omogućavanje ukinutih korisničkih računa samo nakon provjere identiteta podnositelja zahtjeva i prikladnosti zahtjeva.

5.2.2. Upravljanje povjerljivim komponentama korisničkih računa

Potrebno je definirati i implementirati procese, procedure i mehanizme za određivanje, distribuciju, zaštitu i obnavljanje povjerljivih komponenti korisničkih računa.

Smjernice:

a) definirati proceduru za upravljanje i distribuciju povjerljivih komponenti, kako logičkih tako i fizičkih, koja osigurava povjerljivost, integritet i dostupnost spomenutih komponenti i pravilno funkcioniranje autentikacije;
b) odrediti mjere za zaštitu novo osmišljenih povjerljivih komponenti korisničkih računa;

c) primijeniti određene tehnike identifikacije i autentifikacije u skladu s pravnim i regulatornim odredbama koje se tiču sigurnosti i privatnosti;
d) pripremiti sustave upravljanja za povjerljive komponente korisničkih računa. Sustavi moraju zahtijevati: barem inicijalnu promjenu zaporke, autonomnu promjenu zaporke od strane korisnika (nakon provjere korisničkog identiteta); standard sadržaja zaporke; minimalnu duljinu zaporke, datum isteka zaporke; pohranjivanje kriptirane zaporke;
e) definirati proces koji jamči dostupnost i tajnost povjerljivih komponenti korisničkih računa. Također, proces treba jamčiti identifikaciju osoba zaduženih za administraciju sustava upravljanja komponenti korisničkih računa koji su zaduženi za otklanjanje operativnih i sigurnosnih problema.

5.2.3. Putovi mrežnog pristupa

Moraju se odrediti zaštitni mehanizmi za mrežne veze.

Smjernice:

a) napraviti odredbe kako bi sve instance logičkog pristupa mreži bile zaštićene mehanizmom autentikacije;
b) odrediti specifične putove mrežnih veza s osobnih računala do ciljanog odredišta u sustavu kako bi se ograničila sposobnost korisnika da koristi mrežne putove za koje nema dozvolu;
c) definirati pravila prikladnog povezivanja s vanjskih lokacija prema informacijskom sustavu Tvrtke od strane zaposlenika i ugovornih partnera, u skladu s trenutnim zakonskim aktima.

5.2.4. Pristup zaposlenika s udaljenih lokacija

Potrebno je definirati i implementirati procese i procedure za pristup informacijskom sustavu Tvrtke s udaljenih lokacija.

Smjernice:

a) definirati procedure i mehanizme kako bi se osigurala da udaljena povezivanja s informacijskim sustavom Tvrtke odgovaraju odredbama o kontroli pristupa i poslovnim potrebama, ograničavajući udaljeni pristup isključivo za one funkcionalnosti

koje su prijeko potrebne korisniku, koristeći mehanizme jake autentikacije ukoliko zakonska regulativa navedeno propisuje;
b) spriječiti udaljena povezivanja preko samostalno instaliranih ili neovlaštenih uređaja (npr. vanjskih modema ili bežičnih pristupnih točaka).

5.2.5. Kontrola mrežnog prometa

Potrebno je definirati i implementirati tehničke sigurnosne mjere kako bi se nadzirao i filtrirao mrežni promet.

Smjernice:

a) nadzirati mrežni promet i korisnička povezivanja kako bi se ograničila uporaba specifičnih usluga ili njihovih funkcionalnosti u odnosu na poslovne potrebe (prijenos podataka prema van, ograničenja na veličinu priloga u e-mailu i sl.).

5.2.6. Procedure pristupa korisnika

Potrebno je definirati i implementirati sistemske i aplikacijske procedure prijave kako bi se spriječio neovlašteni pristup.

Smjernice:

a) obavijestiti korisnike da se pristupni sustavi i aplikacije smiju koristiti samo u poslovne svrhe;
b) spriječiti prikaz sustava i identifikatora aplikacija sve dok se pristupna procedura uspješno ne dovrši;
c) aktivirati proces provjere korisničkih računa samo nakon što se u cijelosti unese korisnički račun te se, u slučaju pogreške, ne smiju davati indikacije koji su elementi korisničkog računa netočni;
d) ograničiti broj uzastopnih pogrešnih pokušaja prijave/pristupa, blokirati/zaključati korisnički račun u slučaju prelaska maksimalnog broja uzastopnih pogrešnih pokušaja prijave;
e) uspostaviti kriterije za postavku maksimalnog dozvoljenog broja istovremenih prijava od istog korisničkog računa u isti sustav ili aplikaciju, osiguravajući da taj broj ne premašuje operativne potrebe korisnika i osiguravajući da se može ući u trag svim izvršnim operacijama.

5.2.7. Automatsko zaključavanje/automatska odjava i ograničeno vrijeme pristupa sustavu

Automatski mehanizam zaključavanja i, po mogućnosti, automatski mehanizam odjave (log-off) koji se uključuje nakon određenog razdoblja neaktivnosti mora se implementirati za osobna računala zajedno s ograničenjima što se tiče vremena pristupa sustavu.

Smjernice:

a) mora se aktivirati automatski mehanizam zaključavanja za privremenu neaktivnost korisnika koji je prijavljen na osobnom računalu, sprečavajući korisnika u daljnjem radu osim ako korisnik ne ponovni proces autentifikacije;
b) definirati kriterije za ograničavanje dozvoljenog vremena povezivanja na sustav;
c) uspostaviti pravila, gdje je to moguće, za automatski prekid prijave nakon određenog razdoblja neaktivnosti korisnika.

5.2.8 Rad s udaljene lokacije

Moraju se formalizirati specifični procesi za upotrebu i rad s informacijskom opremom s udaljene lokacije. Moraju se osmisliti prikladne zaštitne mjere i pravila za korisnike kako bi se spriječila krađa ili neovlašteni prijenos informacija Tvrtke.

5.3. Autorizacija

Potrebno je definirati i implementirati metode za određivanje i dodjelu prikladnih pristupnih korisničkih profila koji omogućavaju pristup isključivo onoj informaciji koja je strogo neophodna korisniku za izvršavanje dodijeljenih poslova.

5.3.1. Određivanje profila za pristup informacijama

Potrebno je definirati profile korisnika za pristup informacijama i dodijeliti ih na takav način da se spriječi neovlaštena promjena profila i nepravilna uporaba informacija ili usluga.

Smjernice:

a) analitičkim pristupom odrediti pristupne profile na temelju poslovnih potreba i razine klasifikacije informacije kojoj se pristupilo, s ciljem da se osigura povjerljivost, integritet i dostupnost informacije;
b) operacije koje se izvode na informaciji moraju biti autorizirane u skladu s kriterijima „odvajanja zadataka“ kako bi se dala dozvola u skladu s tipom izvedene operacije;
c) autorizacije koje zahtijevaju upotrebu više od jednog korisničkog računa u slučajevima kada je potrebno podići razinu sigurnosti;
d) primijeniti "Need to Know" kriterij i kriterij najmanje privilegije kako bi se dopustio pristup isključivo onoj informaciji koja je strogo neophodna za izvođenje zadataka koji su dodijeljeni korisniku;
e) uspostaviti kriterije za identifikaciju i obradu privilegirane informacije u skladu s pravnim odredbama i primjenjivim standardima
f) odrediti pristupne profile na takav način da se osigura propisno rukovanje privilegiranom informacijom u skladu s pravnim odredbama i primjenjivim standardima;
g) odvojiti odgovornost za upravljanje pristupnim profilima od odgovornosti za upravljanje aplikacijama, sustavima i mrežama;
h) oblikovati odvajanja, obzirom na operacije i upravljanje, između razvoja sustava, testiranja sustava i sustava produkcije kako bi se spriječile neželjene promjene softvera i podataka koji proizlaze iz aktivnosti koje su specifične za različite organizacijske dijelove.

5.3.2. Upravljanje pristupnim profilima s posebnim pravima

Potrebno je definirati i implementirati procese i procedure za uspostavu, uporabu, konstantno upravljanje, čuvanje i ukidanje pristupnih profila s posebnim pravima (npr. administrativni ili sistemski profili).

Smjernice:

a) definirati specifične procedure za dodjelu pristupnih profila s posebnim pravima te za njihovo upravljanje, provjeru i pregled na temelju ustaljenih pravila;
b) voditi evidenciju o aktivnostima korisnika s posebnim pravima, snimajući radnje koje se vrše na sustavima i informaciji u namjenskim prijavama i štiteći te prijave od neovlaštenog pristupa;

c) dodijeliti odgovornosti za upravljanje pristupnim profilima s posebnim pravima strukturama Tvrtke, osim onima kojima pripadaju korisnici te izbjegavati prepuštanje spomenute odgovornosti trećim stranama.

5.3.3. Sigurnost u uporabi mrežnih usluga

Pristup informacijama koje su dostupne preko mreže mora biti ograničen tako da se odredi prikladni pristupni profil za svaku mrežnu uslugu, bilo javnu ili internu.

Smjernice:

a) učiniti dostupnima mrežne usluge na kontrolirani način;
b) odrediti pristupne profile za mrežne usluge za djelatnike i ugovorne partnere koji su u skladu s poslovnim potrebama korisnika te s sigurnosnim pravilima;
c) osigurati da pristup mrežama i mrežnim uslugama uvijek nastupa na takav način da je u skladu sa sigurnosnim pravilima za zaštitu informacija.

5.3.4. Zaštita sustava

Moraju se primijeniti prikladne sigurnosne mjere radi kontrole pristupa sustavu.

Smjernice:

a) dozvoliti pristup sustavima u administrativne ili upravljačke svrhe samo kvalificiranim, identificiranim i autoriziranim zaposlenicima koji imaju profil u skladu s dodijeljenim zadacima:
b) dozvoliti pristup s udaljene lokacije s posebno identificiranih računala opremljenih odgovarajućim zaštitnim mjerama i ovlaštenih od strane nadležnog organizacijskog dijela, u skladu s trenutnim zakonskim aktima.

5.3.5. Upotreba funkcionalnosti sustava

Upotreba funkcionalnosti sustava koje mogu smanjiti učinkovitost sigurnosnih kontrola mora biti ograničena i nadzirana.

a) za svaki operativni sustav identificirati sve funkcionalnosti, servise i zapise koji nisu prijeko potrebni, a koji bi se mogli upotrijebiti za izbjegavanje primijenjenih

sigurnosnih mjera. Potrebno je ukloniti ili onemogućiti korištenje ukoliko to zahtijevaju trenutno važeći regulatorni akti;
b) odrediti pristupne profile koji dozvoljavaju pristup funkcionalnostima sustava na takav način da se može propisno nadzirati njihova upotreba.

5.3.6 Ograničenja aplikativnog pristupa informacijama

Aplikacije moraju imati prikladne kontrolne mehanizme za regulaciju pristupa funkcijama i operacijama koje se mogu provoditi na informaciji (čitanje, pisanje, uređivanje, brisanje) kako bi se osiguralo da je spomenuti pristup u skladu s poslovnim potrebama korisnika.

Smjernice:

a) kontrolirati pristup aplikacijama putem odgovarajućih sigurnosnih alata izvan aplikacija;
b) odrediti aplikativne pristupne profile obzirom na razinu klasifikacije informacije kojoj se pristupa, s ciljem osiguravanja povjerljivosti, integriteta i dostupnosti informacije;
c) odrediti pristup korisnika različitim funkcijama aplikacije kako bi spomenuti pristup bio strogo u skladu s potrebama pristupa informacijama i aktivnostima koje korisnik mora obaviti, pri čemu treba odvojiti funkcije upita od funkcija ažuriranja.
d) kontrolirati prava pristupa resursima aplikacija putem drugih aplikacija, pri čemu je potrebno provjeriti autorizaciju za sve zahtjeve prilikom pristupa.

5.3.7. Zaštita alata za reviziju i pregled sigurnosti

Alati koji se koriste tijekom revizije i pregleda sigurnosti moraju biti pouzdani i dobro zaštićeni.

Smjernice:
a) odvojiti podatke i alate za reviziju sigurnosti od ostalih područja djelovanja;
b) spriječiti neovlašteni pristup i uporabu podataka i alata za sigurnost i reviziju kako bi se osiguralo da se ne ugroze alati za sigurnost i rezultati revizije sigurnosti;
c) uspostaviti pouzdan sustav za pohranu podataka (storage) koji osigurava jasnoću i cjelovitost informacija, pohranu podataka po jedinstvenim kriterijima,

povijesne informacije i mogućnost provođenja integracije, u skladu s trenutno važećim regulatornim aktima.

5.4. Evidentiranje sigurnosnih događaja

Mora se planirati i omogućiti evidentiranje svih radnji koje korisnik izvrši na sustavima, aplikacijama i podacima.

5.4.1. Evidentiranje događaja

Potrebno je razviti primjerene postupke koji omogućuju evidentiranje događaja i aktivnosti s posebnim naglaskom na radnje korisnika s posebnim pravima.

Smjernice:

a) odrediti primjerne odgovornosti za evidentiranje;
b) definirati i dokumentirati popis događaja koji se moraju evidentirati za svaki sustav i aplikaciju, u skladu s regulatornim aktima;
c) kreirati evidencije događaja u sustavu i aplikacijama s dovoljnom količinom detalja, u okviru zakonskih granica, kako bi se identificirali korisnici ili procesi koji su odgovorni za specifični događaj i koji će biti korisni prilikom forenzičke analize u korist Tvrtke u pravnim postupcima;
d) implementirati sustave, usluge i aplikacije na način koji će osigurati aktivaciju i pravilan rad funkcija evidentiranja;
e) instalirati mrežnu opremu (npr. preklopnici, ruteri, vatrozidi) za evidentiranje relevantnih podataka s posebnim naglaskom na neuspjele pokušaje pristupa, pristupa od strane korisnika s administratorskim pravima, te modifikacijama i konfiguracijama.

5.4.2 Čuvanje evidencija

Informacije vezane uz pristup i aktivnost korisnika moraju biti zapisane, pohranjene i zaštićene kako bi se omogućila provjera i analiza svih aktivnosti koje potencijalno utječu na informacijski sustav u slučaju sigurnosnog događaja ili incidenata.

Smjernice:

a) zaštititi i pohraniti evidencije događaja sukladno sa regulatornim i operativnim zahtjevima, propisati adekvatne politike i procedure;
b) zaštiti evidencije događaja na primjeren način pri čemu se posebna pažnja usmjerava na sprječavanje neovlaštenog pristupa i osiguravanje nepromjenjivosti sadržaja evidencija i njihovu primjerenu pohranu uz praćenje pristupa i provedenim promjenama;
c) stvaranje sigurnosnih kopija sukladno standardu.

5.5. Kriptografija, hash i digitalni potpis

Potrebno je planirati kriptografske i hash metode kako bi se osigurala povjerljivost, integritet i neporecivost pohranjenih ili proslijeđenih informacija. Potrebno definirati i implementirati metode upravljanja kriptografskim ključevima.

5.5.1. Osnove korištenja kriptografskih i hash kontrola

Potrebno je procijeniti opciju korištenja specifičnih kriptografskih tehnika radi zaštite informacija.

Smjernice:

a) utvrditi kriterije za korištenje kriptografskih i hash tehnika za zaštitu informacija na temelju analize sigurnosnih rizika, u skladu s trenutno važećim zakonskim aktima.

5.5.2. Enkripcija

Kriptografske tehnike se moraju koristiti sukladno klasifikacijskom stupnju informacija o kojima se radi kako bi se zaštitila povjerljivost i integritet informacija.

Smjernice:

a) na temelju klasifikacijskog stupnja informacija odabrati karakteristike kriptografskih ključeva (npr. dužina) i tip algoritma koji će se koristiti;
b) upotrebljavati kriptografske tehnike za zaštitu povjerljivosti i integriteta informacija sukladno klasifikacijskom stupnju.

5.5.3. Digitalni potpis

Mehanizam digitalnog potpisa potrebno je implementirati na temelju razine klasifikacije informacije, kako bi se zaštitio integritet informacije, zajamčila autentičnost pošiljatelja i osigurala neporecivost.

Smjernice:

a) oristiti kriptografske tehnike na temelju para ključeva, javnog i privatnog, pri čemu se određuju primjerene zaštitne mjere povjerljivosti privatnog ključa;
b) utvrditi kriterije koji zahtijevaju korištenje tehnika neporecivosti utemeljenih na mehanizmima kvalificiranog digitalnog potpisa sukladno zakonskim, regulatornim i ugovornim odredbama.

5.5.4. Upravljanje ključevima i certifikatima

Ključevima koji se koriste u okviru kriptografskih tehnika treba upravljati na prikladan način te isti moraju biti primjereno zaštićeni.

Smjernice:

a) osigurati sigurno upravljanje kriptografskim ključevima i certifikatima na temelju utvrđenih odgovornosti, postupaka, metoda i pravila, pri čemu se kompromitirani ključevi ili istekli certifikati moraju odmah zamijeniti.

5.6. Elektronička trgovina

Potrebno je sistematizirati odgovornosti, procese, alate i metode vezane uz elektroničku trgovinu.

5.6.1. Sigurnost elektroničke trgovine

Potrebno je odrediti mjere za zaštitu informacija vezanih uz elektroničku trgovinu te ugovorom na primjeren način propisati načine razmjene između strana koje sudjeluju u transakcijama.

Smjernice:

a) odrediti i evidentirati postupke za identifikaciju i ovjeru vjerodostojnosti strana koje sudjeluju u transakciji;
b) odrediti i evidentirati tehničke protumjere za osiguravanje povjerljivosti, integriteta i dostupnosti proslijeđenih podataka;
c) identificirati mehanizme radi osiguravanja neporecivosti elektronske transakcije od strane sudionika;
d) osigurati da su svi zahtjevi za transakciju, provedba i potvrda od strane sudionika transakcije evidentirani;
e) identificirati mehanizme za otkrivanje neprimjerenog ponašanja ili radnji sudionika transakcije (npr. ponovljene radnje izvan područja uobičajenih poslovnih operacija) kako bi se omogućila podrška za otkrivanje zlouporaba u okviru elektroničke trgovine;
f) implementirati mehanizme radi otkrivanja i blokiranja pokušaja neovlaštenog pristupa sustavima koji se koriste u elektroničkoj trgovini;
g) sistematizirati sigurnosne zahtjeve i odgovornosti putem ugovornih odredbi između strana koje sudjeluju u transakciji te s pružateljima usluga koji sudjeluju u prijenosu podataka;
h) utvrditi pravila za strane koje sudjeluju u transakciji vezano uz pravilno korištenje usluge i naglašavanje rizika povezanih s istim.

5.6.2. Objavljivanje informacija

Informacije koje se objavljuju putem komunikacijskih kanala moraju se zaštiti od neovlaštenih modifikacija.

Smjernice:

a) dodijeliti uloge i odgovornosti te uspostaviti procese, procedure i primjerene razine ovlaštenja za objavu informacija radi osiguravanja točnosti informacija i zaštite ugleda Tvrtke sukladno s primjenjivim standardima i zakonskim aktima;
b) na primjeren način zaštiti sustave koji se koriste za objavljivanje informacija;
c) odrediti periodičan nadzor objavljenih informacija kako bi se osiguralo da su iste točne, nepromijenjene i aktualne, u skladu s trenutno važećim zakonskim aktima

6. RAD I UPRAVLJANJE APLIKACIJAMA, SUSTAVOM I MREŽOM

Zaštita informacijskog sustava Tvrtke zahtijeva praćenje čimbenika povezanih s operativnim upravljanjem aplikacijama, sustavima i mrežama kako bi se osigurao njihov pravilan rad u svakom trenutku. U određivanju uspjeha sustava upravljanja informacijskom sigurnošću posebno je važna integracija sigurnosnih, kontrolnih i verifikacijskih mjera u radu informacijskog sustava.

6.1. Operativno upravljanje

Organizacijski dijelovi (razvoj, testiranje, produkcija) u kojima se koriste, razvijaju i/ili održavaju sustavi i aplikacije moraju biti odvojeni kako bi se osigurali integritet i dostupnost tih sustava i aplikacija u bilo kojem trenutku. Pravilno upravljanje sustavima, aplikacijama i mrežama mora uključivati pripremu i zaštitu dokumentacije sustava vezane uz konfiguraciju, individualno prilagođene postavke i radne procedure koje osiguravaju sigurnost i točnost operacija.

Mjere vezane uz instalaciju, operativno provođenje i upravljanje u izvanrednim situacijama te zaštitu koda, moraju biti uspostavljene za aplikacije u produkcijskom okruženju kako bi se osigurala povjerljivost, integritet i dostupnost obrađenih informacija.

Sustave, aplikacije i mreže koje se smatra suvišnima, treba ukloniti.

6.1.1. Odvajanje okolina

Moraju se uspostaviti odvojene okoline za razvoj i testiranje korektivnih preinaka, preinaka u sklopu održavanja, prilagodbe i razvoja sustava, aplikacija i mreža. Te okoline moraju biti namijenjene isključivo za te svrhe i odvojene od produkcijskih okolina kako bi se osiguralo pravilno i sigurno izvršenje navedenih ciljeva.

Smjernice:

a) odvojiti, minimalno na logičkoj razini, okoline u kojima se izvode aktivnosti vezane uz životne cikluse aplikacija, sustava i mreža;

b) usvojiti zaštitne mjere za razvojne aktivnosti kako bi se osiguralo da se produkcijski podaci ne mogu povezati s osobnim podacima te da ostali podaci, koji su klasificirani kao kritični ostanu povjerljivi;
c) primijeniti zaštitne mjere za testne aktivnosti kako bi se osiguralo da se testni podaci ne mogu povezati s osobnim podacima te da ostali podaci, koji su klasificirani kao kritični ostanu tajni. Druga mogućnost je da se tajnost podataka zaštiti istim sigurnosnim mjerama koje se primjenjuju u produkcijskim okolinama;
d) osigurati da se barem jedan test obavi uz korištenje podataka koji su dosljedni s produkcijskim podacima;
e) opremiti organizacijske dijelove za razvoj, testiranje i stavljanje u produkciju automatskim procedurama za identifikaciju i praćenje svih radnih verzija, kako bi se omogućila rekonstrukcija slijeda svih provedenih modifikacija.

6.1.2 Dokumentacija i upravljanje operativnim procedurama

Operativne procedure moraju se dokumentirati, njima se mora upravljati, te se moraju održavati. Poseban naglasak mora se staviti na operativne procedure za upravljanje pohranom informacija, upravljanje greškama i povratom aplikacija, sustava i mreža.

Smjernice:

a) uspostaviti dokumentirane procedure za upravljanje aplikacijama, sistemskim i mrežnim aktivnostima koje pridonose njihovoj sigurnosti i pravilnom funkcioniranju, u skladu s trenutno važećim zakonskim aktima;
b) planiranje specifičnih automatskih procesa za provjeravanje točnosti operacija i za njihovo pravilno dokumentiranje.

6.1.3. Održavanje informatičke opreme

Informatička oprema se mora održavati u skladu s tehničkim specifikacijama proizvođača kako bi se osigurao njen integritet i funkcionalna dostupnost u bilo kojem trenutku.

Smjernice:

a) periodički provoditi odgovarajuće aktivnosti održavanja informatičke opreme prema preporukama proizvođača uz pomoć specijaliziranog osoblja. Bilježiti svaki otkriveni nedostatak te svaku provedenu aktivnost održavanja;
b) primijeniti specifične mjere za zaštitu informacija koje se nalaze na informatičkoj opremi, uz posebnu pažnju kod eksternaliziranja aktivnosti održavanja.

6.1.4. Zaštita dokumentacije sustava

Dokumentacija sustava koja specificira konfiguracije, individualno prilagođene postavke i operativne procedure mora biti odgovarajuće zaštićena.

Smjernice:

a) zaštititi dokumentaciju sustava;
b) omogućiti pristup dokumentaciji sustava samo ovlaštenim djelatnicima.

6.1.5. Pohrana i zaštita dokumentacije

Dokumentacija Tvrtke, tiskana i u elektroničkom obliku, mora biti odgovarajuće zaštićena, čuvana i održavana u skladu s zakonskim, regulatornim i internim odredbama i pravilima.

Smjernice:

a) dodijeliti odgovornost za utvrđivanje koje se informacije moraju čuvati prema zakonu te za određivanje i provođenje odgovarajućih sigurnosnih mjera za zaštitu informacija od gubitka, uništenja ili krivotvorenja;
b) odrediti odgovarajuće sigurnosne mjere koje omogućavaju pohranu, pristup i mogućnost korištenja dokumentacije u bilo kojem trenutku, u skladu s trenutno važećim zakonskim aktima.

6.1.6. Odvajanje kritičnih sustava

Kritični sustavi moraju biti odgovarajuće zaštićeni od neovlaštenog pristupa.

Smjernice:

a) procijeniti mogućnost instalacije kritičnih aplikacija na za to određene sustave;

b) dodijeliti odgovornost za upravljanje takvim sustavima.

6.1.7. Sinkronizacija satova

Satovi na svoj opremi moraju biti usklađeni.

Smjernice:

a) aktivirati odgovarajuće automatske procedure za provjeru i, po potrebi, ispravak, sinkronizacije satova u različitoj opremi ili sustavima.

6.1.8. Kontrola pristupa izvornom kodu aplikacija

Moraju se usvojiti sigurnosne mjere kako bi se zaštitio izvorni kod aplikacija.

Smjernice:

a) odgovarajuće zaštititi i kontrolirati pristup knjižnicama (eng. *libraries*) izvornog koda;
b) uspostaviti specifične procedure i koristiti odgovarajuće alate za rukovanje izvornim kodom, procedurama kompajliranja i izvršnim programima kako bi se osigurala pohrana, verzioniranje i praćenje promjena.

6.1.9. Interno izvršenje aplikacija

Moraju se odrediti specifične zaštitne mjere za pravilno, sigurno i provjerljivo upravljanje izvršenjem aplikacije. Mjere upravljanja bavit će se i implementacijom aplikacije u produkcijskom okruženju i verifikacijom trajne učinkovitosti sigurnosnih mjera.

Smjernice:

a) dodijeliti podešavanje produkcijskih okolina i instalaciju softvera ovlaštenim zaposlenicima;
b) spriječiti preinake izvornog koda i povezanog izvršnog koda u vrijeme integracije aplikacije u produkcijsko okruženje;

c) prije obavljanja bilo kakvih preinaka na aplikaciji, napraviti i zaštititi sigurnosne kopije aplikacije kako bi se osiguralo da se prethodna konfiguracija može vratiti u slučaju javljanja bilo kakvih problema;
d) procijeniti potrebu za kreiranjem dodatnih sigurnosnih kopija podataka u produkcijskom okruženju prilikom implementacije softvera koji bi mogao imati značajan utjecaj na baze podataka;
e) isključiti razvoj softvera i preinaka iz produkcijskog okruženja, uz iznimku hitnih korektivnih radnji održavanja;
f) spriječiti pristup produkcijskim podacima od strane zaposlenika koje radi na aplikacijama ili sustavima osim u slučaju hitnih radnji ili izričito odobrenih ili nadziranih radnji u svrhu osiguravanja pravilnog funkcioniranja sustava i aplikacija. U svakom slučaju, moraju se provoditi odgovarajući mehanizmi za zaštitu povjerljivosti, integriteta i dostupnosti podataka.
g) provoditi periodička testiranja aplikacije kako bi se osiguralo da implementirane sigurnosne mjere ostanu učinkovite tijekom vremena te provoditi sve potrebne korektivne mjere;
h) ustanoviti i zabilježiti odgovarajuće procedure za upravljanje aplikacijama koje su u aktivnoj upotrebi, u skladu s trenutno važećim regulatornim obavezama;
i) utvrditi sigurnosne mjere za zaštitu integriteta aplikacija i podataka koji se nalaze u produkcijskim okolinama;
j) ustanoviti procedure za regulaciju upotrebe i umnožavanja programa i aplikacijskih podataka koji se nalaze u produkcijskim okolinama, uz dozvolu izrade samo izričito potrebnih kopija;
k) uspostaviti procese i procedure za upravljanje životnog ciklusa softvera.

6.1.10. Eksternalizirano izvršenje aplikacija

Moraju se utvrditi specifične zaštitne mjere za pravilno, sigurno i provjereno upravljanje izvršenjem aplikacija u slučajevima eksternaliziranja izvršenja aplikacije.

Smjernice:

a) izrada provedba ugovora o eksternalizaciji koji su u skladu s internim izvršenjem aplikacije i pravilima upravljanja;
b) obavljati periodičke provjere kako bi se potvrdilo da vanjski izvršitelj obavlja aktivnosti u skladu s ugovornim odredbama;
c) izrada ugovornih odredbi koje definiraju obveze osoblja vanjskog izvršitelja vezano uz pristup podacima, softveru i dokumentaciji, u skladu s primjenjivim zakonskim aktima.

6.1.11. Hitne promjene aplikacija

Moraju se provesti odgovarajuće mjere za praćenje i kontrolu promjene aplikacije koje se obavljaju izravno u produkcijskom okruženju kao dio procedure upravljanja u izvanrednim situacijama.

Smjernice:

a) uspostaviti proceduru za raspodjelu odgovornosti, uz utvrđivanje potrebnih razina autorizacije i pronalaženje kriterija za promjenu aplikacija u izvanrednim situacijama;
b) pratiti sve aktivnosti, operacije i autorizacije povezane s upravljanjem u izvanrednim situacijama;
c) ustanoviti odgovarajuće procedure za osiguravanje pravilnog ponovnog usklađenja razvojnih, testnih i produkcijskih okolina tijekom faze oporavka nakon pojave izvanrednih situacija, te izvođenje svih testova propisanih u slučaju normalnih promjena.

6.1.12. Uklanjanje sustava, aplikacija i mreža

Trebaju se uspostaviti procedure za deinstalaciju sustava, aplikacija i mreža koji nisu u funkciji.

Smjernice:

a) utvrditi sve komponente koje treba ukloniti (podatke, softver, hardver, itd.);
b) odabrati tehnike i napraviti odgovarajuću pozadinsku dokumentaciju (npr. izgled bilješki) kako bi se zadržala čitljivost podataka u slučajevima kada se podaci moraju sačuvati za poslovne ili pravne svrhe;
c) u slučajevima kada nije moguće deinstalirati aplikaciju, sustav ili mrežu, spriječiti pristup korisnika trajnim uklanjanjem povezanih pristupnih profila.

6.2. Izrada sigurnosnih kopija informacija

Potrebno je implementirati alate i procedure za pravilno planiranje i upravljanje izradom sigurnosnih kopija za operativne sustave, softver, podatke i sistemske konfiguracije.

6.2.1. Izrada sigurnosnih kopija

Treba uspostaviti proceduru za razvoj odgovarajućih planova za izradu sigurnosnih kopija za operativne sustave, softver i podatke kako bi se osigurala mogućnost njihova vraćanja u skladu s ustanovljenim vremenskim okvirima i metodama.

Smjernice:

a) uspostaviti zahtjeve na dostupnost aplikacija, sustava i mreža;
b) definirati zahtjeve za izradu sigurnosnih kopija operativnih sustava, aplikacijskog softvera i podataka. Zahtjevi trebaju navoditi za koje sustave treba izraditi sigurnosne kopije te koliko često to treba raditi, kako pohraniti sigurnosne kopije te koliko kopija treba napraviti, u skladu sa zakonskim i poslovnim zahtjevima:
c) izraditi sigurnosne kopije podataka, operativnih sustava i aplikacijskog softvera na temelju ustanovljenih zahtjeva;
d) regulirati kopiranje informacija, ograničavajući ga na ono što je strogo što se tiče redundancije i umnožavanja;
e) čuvati arhivu o tome koje su sigurnosne kopije izrađene;
f) redovito provjeravati mogućnost vraćanja sigurnosnih kopija podataka spremljenih na medij za pohranu sigurnosnih kopija;
g) pohranjivati medije za pohranu podataka koji sadrže kopije podataka izvan produkcijskog okruženja te na dovoljno sigurnoj udaljenosti kako bi se osiguralo da jedan događaj ne može oštetiti i sigurnosne kopije i originalne podatke;
h) napraviti raspored i provesti testove kako bi se osiguralo da se sustavi i aplikacije mogu ponovo inicijalizirati ili pokrenuti sa sigurnosnih kopija te da se sve izvorne funkcije mogu vratiti.

6.3. Upravljanje informatičkom opremom i medijima za pohranu podataka

Informatička oprema mora biti dodijeljena, instalirana i korištena na način koji omogućava njen dugotrajan integritet i dostupnost. Uporaba svih dodijeljenih alata, opreme i informacijske imovine mora biti regulirana i kontrolirana, čak i ako se ona koristi izvan poslovnih objekata ili izvan uobičajenog poslovnog okruženja. Potrebno je definirati odgovarajuća pravila koja bi regulirala skrb nad i zaštitu ovih alata, opreme i informacijske imovine.

Moraju se utvrditi sigurne metode za skrb, ponovno korištenje, umnožavanje, fizički transport i uništavanje prijenosnih medija za pohranu podataka kako bi se osiguralo da ne dođe do njihova uništenja, krađe ili neovlaštenog pristupa.

6.3.1 Ovlaštenje za uporabu opreme

Mora se utvrditi procedura ovlaštenja za dodjelu informatičke opreme (osobnih računala, prijenosnih računala, PDA, itd.) ili bilo koje druge opreme koja može sadržavati ili služiti za prijenos informacija (telefoni, faksovi, itd.) osoblju. Ova procedura mora se temeljiti na odgovarajućim kriterijima za dodjeljivanje takvih uređaja.

Smjernice:

a) ustanoviti odgovarajuće procedure za predaju zahtjeva te kriterije za dodjeljivanje opreme koja može sadržavati ili služiti za prijenos informacija;
b) ustanoviti pravila za korisnike koja zabranjuju uporabu opreme za obradu informacija, osim onih koje Tvrtka dodijeli korisniku i tehnološkim rješenjima, osim ako nije specifično ovlašten drugačije, te koja zabranjuju korištenje neovlaštenih sredstava spajanja na druge uređaje, sustave ili mreže;
c) dodijeliti odgovornost korisniku, na temelju ustanovljenih pravila, za zaštitu opreme koja mu/joj je dodijeljena;
d) podjela odgovornosti na temelju uspostavljenih pravila.

6.3.2. Sigurnost informatičke opreme dodijeljene korisnicima

Treba ustanoviti mehanizme i korisnička pravila vezano uz zaštitu i korištenje informatičke opreme koja je stavljena na raspolaganje korisnika. Uz osobna računala, to uključuje uređaje poput prijenosnih računala, printera, PDA uređaja, mobitela, fiksnih telefona, fotokopirnih uređaja, faks uređaja, itd. Svrha ovih mehanizama i pravila je zaštititi sigurnost informacija koje se izmjenjuju putem ove opreme. Nadalje, moraju se ustanoviti pravila za korisnike vezano uz zaštitu informacija kojima se korisnici koriste.

Smjernice:

a) odrediti metode upravljanja za informatičku opremu, i fiksnu i mobilnu, koja je stavljena na raspolaganje korisnika u poslovne svrhe;

b) dodijeliti odgovornost korisnicima kako bi se osiguralo da se informatička oprema koristi isključivo u poslovne svrhe u skladu s ustanovljenim pravilima;
c) ustanoviti korisnička pravila za pravilnu uporabu informacijske imovine Tvrtke kako bi se osigurala zaštita informacija koje su sadržane u ili povezane s navedenom imovinom;
d) odrediti odgovarajuće metode za autorizaciju korištenja informatičke opreme i informacijske imovine općenito izvan poslovnih objekata Tvrtke, uključujući izvedbu periodičkih i specifičnih provjera ili inspekcija kako bi se osiguralo da je ta uporaba u skladu s ustanovljenim pravilima;
e) utvrditi mehanizme i pravila za fizičku i logičku zaštitu te skrb nad informatičkom opremom i informacijskom imovinom općenito, kada se koristi izvan poslovnih objekata Tvrtke. Ti mehanizmi i pravila, moraju biti bar onoliko strogi kao oni koji vrijede za uporabu navedene opreme i imovine unutar poslovnih objekata te moraju uzeti u obzir posebne rizike povezane s uporabom izvan poslovnih objekata;
f) nabaviti i implementirati sustav za snimanje, označavanje i praćenje uporabe informacijske imovine u skladu sa zakonskim odredbama i internim pravilima koja su na snazi.

6.3.3. Vraćanje, ponovna dodjela i održavanje opreme

Kada se informatička oprema povlači iz uporabe, ponovno dodjeljuje ili podvrgava održavanju, informacije pohranjene na opremi moraju se presnimiti te zatim izbrisati na siguran način kako bi se osiguralo da se one ne mogu vratiti.

Smjernice:

a) odrediti i kopirati, koristeći odgovarajuća sredstva, informacije koje se nalaze na informacijskoj opremi koja se vraća, ponovno dodjeljuje ili je podvrgnuta radovima održavanja;
b) nakon kopiranja informacija koje se nalaze na informatičkoj opremi koja se vraća, koja je ponovno dodijeljena ili podvrgnuta radovima održavanja, izbrisati navedene informacije na siguran način te provjeriti da se informacije ne mogu vratiti;
c) nakon izvođenja aktivnosti navedenih pod točkama a) i b), informatička oprema koja se vraća, ponovno dodjeljuje ili odlaže mora biti u potpunosti preformatirana pomoću sigurnih i nepovratnih metoda;
d) u slučaju da se aktivnosti iz točaka a), b) i c) eksternaliziraju, moraju se razviti odgovarajuće kontrole i mjere pregleda te unijeti u ugovor s vanjskim izvršiteljem kako bi se osiguralo da će navedene operacije biti propisno izvršene. Nadalje, Tvrtka mora

biti sposobna obaviti te kontrole i metode provjere uz potpun i neometanu autonomnost.

6.3.4. Sigurnost izmjenjivih medija za pohranu podataka

Moraju se odrediti odgovarajuće metode za upravljanje izmjenjivim medijima za pohranu podataka.

Smjernice:

a) popisati inventar izmjenjivih medija za pohranu podataka i označiti ih u odnosu na razinu klasifikacije;
b) dozvoliti pristup izmjenjivim medijima za pohranu podataka samo ovlaštenim zaposlenicima;
c) odrediti kriterije i metode za bilježenje i praćenje pristupa izmjenjivim medijima za pohranu podataka od strane zaposlenika;
d) planirati i implementirati sigurnosne mjere za skrb nad i pohranu izmjenjivih medija za pohranu podataka;
e) planirati i implementirati pravila i procedure za povrat ili ponovno korištenje izmjenjivih medija za pohranu podataka, uz što je potrebno osigurati da se bilo koje informacije koje se na njima nalaze ne mogu vratiti;
f) ustanoviti pravila za korisnike za upravljanje izmjenjivim medijima za pohranu podataka koji su na raspolaganju korisniku;
g) u slučajevima kada se upravljanje izmjenjivim medijima za pohranu podataka eksternalizira, pripremiti specifične ugovorne odredbe kojima se osigurava sukladnost s ustanovljenim pravilima.

6.3.5. Sigurnost transporta fizičkih medija za pohranu podataka

Mora se ustanoviti procedura za implementaciju sigurnosnih mjera u fizičkom transportu medija za pohranu podataka i podataka u papirnatom obliku u skladu s razinom klasifikacije informacija koje se nalaze na medijima ili tiskanim kopijama.

Smjernice:

a) ustanoviti procedure i odgovornosti za transport medija za pohranu podataka i podataka u papirnatom obliku, u skladu s trenutno važećim zakonskim aktima;

b) otpremati medije za pohranu podataka i podatke u papirnatom obliku tek nakon što su implementirane odgovarajuće sigurnosne mjere u skladu s raznim klasifikacije informacija koje se na njima nalaze;
c) mediji za pohranu podataka i podaci u papirnatom obliku koji ulaze u Tvrtku, moraju biti provjereni kako bi se osigurao njihov integritet, a primitak medija ili papirnatih materijala mora se evidentirati.

6.3.6. Zaštita ulazne i izlazne informacijske imovine

Sigurno rukovanje ulaznom i izlaznom informacijskom imovinom mora se regulirati u pogledu povezanih rizika (npr. posao, ugled Tvrtke, strateški, gubitak).

Smjernice:

d) u skladu s primjenjivim zakonima, implementirati sustav provjere kako bi se otkrili pokušaji krađe informacijske imovine ili kršenja povjerljivosti istih;
e) dvostruko provjeriti ulaznu i izlaznu imovinu naspram pripadajuće administrativne dokumentacije (računi za pošiljke, obavijesti o dostavi, itd.).

6.4. Praćenje aplikacija i sustava

Pristup i korištenje sustava, aplikacija i podataka mora se provjeriti kako bi se omogućila identifikacija i prevencija radnji koje nisu u skladu s pravilima Tvrtke. Moraju se utvrditi djelotvorni kriteriji za prikupljanje i analizu podataka, a svi padovi sustava ili aplikacija moraju se evidentirati, zajedno s aktivnostima povezanim s povratom navedenih sustava i aplikacija.

6.4.1. Praćenje uporabe sustava i aplikacija

Moraju se utvrditi odgovarajući kriteriji za prikupljanje i pregled podataka vezano uz uporabu sustava i aplikacija od strane korisnika, moraju se pripremiti povezane analitičke procedure kako bi se pronašli sumnjivi događaji ili zabranjene aktivnosti, te se moraju planirati odgovarajuće korektivne mjere.

Smjernice:

a) utvrditi procedure za uporabu arhive korisničkih aktivnosti, u skladu s primjenjivim zakonskim odredbama;
b) konfigurirati sustave nadzora kako bi se osigurala dostupnost, pouzdanost i ažurnost arhiviranih podataka;
c) implementirati odgovarajuće zaštitne mjere za datoteke koje sadrže podatke vezane uz nadzor, koje bi regulirale pristup navedenim datotekama;
d) pronaći odgovarajuće mehanizme za korelaciju podataka o uporabi sustava;
e) pregledati skupljene informacije i analizirati probleme koji proizlaze iz nadzornih operacija s ciljem određivanja odgovarajućih korektivnih mjera.

6.4.2. Povrat sustava

Moraju se arhivirati informacije o padovima sustava i aplikacija te informacije o njihovom naknadnom povratu, uz poseban naglasak na provjeravanje jesu li korektivne mjere propisno odobrene u skladu s ustanovljenim pravilima te da u procesu nisu ugrožene sigurnosne mjere.

Smjernice:

a) utvrditi odgovornosti i procedure za odobravanje i upravljanje aktivnostima povrata;
b) utvrditi informacije koje se moraju zabilježiti vezano uz pad i povrat sustava i aplikacija;
c) provjeriti jesu li aktivnosti povrata propisno provedene, je li povezani pristup informacijskom sustavu propisno ovlašten te jesu li sigurnosne mjere općenito kompromitirane.

6.5. Planiranje kapaciteta

Kapaciteti informacijskih sustava, kao i kapacitet uslužnih sustava koji podržavaju njihov rad moraju se planirati unaprijed kako bi se osiguralo da kapacitet procesiranja ovih sustava bude dovoljan za sprječavanje neispravnog rada uslijed preopterećenja sustava.

6.5.1. Dizajn kapaciteta sustava

Izvedba osnovnih sredstava informacijskih sustava (memorija, procesori, diskovni prostor, itd.) moraju se redovito provjeravati da bi se mogle planirati moguće potrebne korektivne mjere s ciljem osiguranja odgovarajućih razina izvedbe.

Smjernice:

a) utvrditi zahtjeve na izvedbu za pravilno definiranje kapaciteta sustava tijekom faze planiranja novih sustava;
b) dodijeliti odgovornosti za odobrenje i prihvaćanje konfiguracija sustava;
c) ustanoviti i zabilježiti procedure za prikupljanje podataka o razinama izvedbe i određivanje parametara prihvatljivosti;
d) utvrditi koji sustavi i aktivnosti moraju biti podložni mjerenjima, provjeriti njihovu izvedbu i prenijeti saznanja o njihovim nedostacima odgovarajućim funkcijama u Tvrtki;
e) analizirati prikupljene podatke o kapacitetu dijelova sustava s ciljem osiguranja mjerila za praćenje postojećih sustava, omogućiti utvrđivanje budućih potreba i dozvoliti implementaciju odgovarajućih korektivnih mjera za poboljšanje izvedbe sustava, uz dokumentiranje svakog navedenog elementa;
f) osigurati da su uslužni i drugi sustavi koji podržavaju rad informacijskih sustava odgovarajuće veličine kako bi mogli zadovoljiti potrebe čak i nakon promjena u konfiguraciji, trajanju rada i kapacitetima informacijskih sustava.

6.6. Zaštita od malicioznog ili mobilnog koda

Moraju se osigurati odgovarajući alati i infrastruktura, uključujući sustave antivirusne zaštite, kako bi se spriječio upad i djelovanje potencijalno štetnog softvera (maliciozni kod). Moraju se utvrditi odgovornosti i procedure za instalaciju i ažuriranje sustava antivirusne zaštite te za određivanje metoda odgovora i mjera u slučaju otkrivanja i potencijalnog širenja malicioznog koda u informacijskom sustavu Tvrtke.

6.6.1. Sigurnosne mjere protiv malicioznog i mobilnog koda

Moraju se usvojiti odgovarajuće mjere i blokirati kompjuterski virusi te drugi potencijalno štetni softver kako bi se osigurala brza identifikacija, prekid širenja i uklanjanje navedenog, kao i popravak njegovih učinaka. Moraju se planirati tečajevi za obuku zaposlenika u svrhu podizanja svijesti o problemu.

Smjernice:

a) dodijeliti odgovornosti za upravljanje odgovarajućim alatima i infrastrukturom za sprječavanje upada i posljedičnog djelovanja potencijalno štetnog softvera;
b) dodijeliti odgovornosti za centralizirano upravljanje, instalaciju i ažuriranje sustava antivirusne;
c) definirati odgovarajuća korisnička pravila vezana uz prevenciju i zaštitu od malicioznog koda;
d) spriječiti autonomnu instalaciju softvera od strane korisnika;
e) ustanoviti odgovarajuća pravila za zaposlenike koji razvijaju softver, s naglaskom na zabranu korištenja softvera koji nije prethodno procijenjen sa sigurnosnog stajališta te odobren za instalaciju;
f) instalirati i konstantno ažurirati antivirusni softver na svim serverima i osobnim računalima te primjenjivati mjere koje sprečavaju onemogućavanje od strane korisnika, provjeravati je li antivirusni softver pravilno instaliran i omogućen na svim sustavima koji bi potencijalno mogli biti predmet upada malicioznog koda. Antivirusni softver mora uvijek biti aktivan i ažuran, Antivirusni softver mora generirati i logove ukoliko to zahtijeva zakonska regulativa;
g) Planirati i implementirati automatske alate za filtriranje datoteka i filtriranje sadržaja kako bi se smanjili rizici povezani s uporabom elektronička pošta i interneta na način da se filtriraju virusi i druge potencijalno štetne komponente;
h) u slučajevima kada je softver razvijen od strane ugovornih partnera, utvrditi metode koje osiguravaju zaštitu od potencijalno štetnih komponenti;
i) utvrditi mjere odgovora koje se trebaju primijeniti u slučaju da jedan ili više virusa ili bilo koji drugi potencijalno štetni softver bude otkriven u informacijskom sustavu Tvrtke;
j) u slučajevima kad je softver instaliran od strane ugovornog partnera, usvojiti preventivne kontrolne mjere kako bi se osiguralo od prisutnosti potencijalno štetnog koda.

6.7. Elektronička pošta i internet

Mediji koji se koriste za razmjenu informacija putem elektroničke pošte i interneta (za prijenos informacija ili obavljanje elektroničkih transakcija), moraju biti primjereno zaštićeni, obzirom na vrstu informacija koje se njima prenose, putem formulacije odgovornosti, procesa, alata i metoda za razmjenu informacija.

6.7.1. Sigurnost u korištenju elektroničke pošte i interneta

Mora se omogućiti sigurno korištenje elektroničke pošte i interneta putem razvoja i implementacije odgovarajućih tehničkih protumjera i korisničkih pravila.

Smjernice:

a) definirati smjernice Tvrtke za korištenje elektroničke pošte;
b) definirati smjernice Tvrtke za korištenje interneta;
c) definirati korisničke smjernice za korištenje elektroničke pošte i interneta uz navođenje povezanih rizika i kontrola koje bi se mogle primjenjivati te odrediti tehničke protumjere za zaštitu informacija;
d) upravljati infrastrukturom i bazama podataka koje sadrže e-mail poruke kako bi se osigurala dostupnost usluge, kontrolirani pristup i zaštita od izvanrednih događaja;
e) utvrditi kriterije za primjenu kriptografskih tehnika za zaštitu poslanih ili sačuvanih e-mail poruka;
f) osigurati logičke kontrole pristupa elektroničkoj pošti i internetu;
g) osigurati da se arhiva o pristupu elektroničkoj pošti i internetu čuva u skladu s primjenjivim zakonom;
h) iznijeti politike koje treba usvojiti u slučaju kaznenih prekršaja i/ili delikata i/ili djela iz nemara i/ili pogrešaka počinjenih u sklopu korištenja elektroničke pošte;
i) napraviti raspored za i implementirati odgovarajuće sigurnosne kontrole za korištenje interneta kako bi se spriječila neprikladna uporaba.

6.8. Upravljanje telekomunikacijskim mrežama

Moraju se usvojiti odgovarajuće mjere kako bi se osigurala sigurnost mreža i opreme koja podržava ili omogućava primjeren i siguran protok informacija. Potrebno je dodijeliti i odvojiti odgovornosti za upravljanje navedenim mrežama i odgovornosti za upravljanje operativnim sustavima.

Mreža, njene komponente i usluge koje pruža moraju biti zaštićeni od nedozvoljenog pristupa, bilo lokalnog ili udaljenog, na odgovarajući način, uz procjenu mogućnosti segmentacije mreže i/ili praćenja i kontrole prometa.

6.8.1. Segmentacija mreža

Moraju se utvrditi tehnička sigurnosna rješenja za segmentaciju mreža:

Smjernice:

a) ustanoviti i ažurirati kriterije za logičku podjelu mreže koji bi bili u skladu s pristupnim profilima uslugama mreže;
b) kreirati neovisne mrežne segmente koje je potrebno barem logički odvojiti korištenjem odgovarajuće opreme i alata (npr. *gateways, firewalls*);
c) podesiti alate za filtriranje komunikacije između mrežnih segmenata i blokirati sav neovlašteni promet.

6.8.2. Utvrđivanje mrežnih sigurnosnih mjera

Mora se uspostaviti procedura za identifikaciju i implementaciju odgovarajućih sigurnosnih mjera, tehničkih i organizacijskih, za zaštitu informacijskog sustava Tvrtke i mrežnih usluga. Takve mjere mogu uključivati procjene ranjivosti i tehnike otkrivanja upada u informacijski sustav Tvrtke.

Smjernice:

a) dodijeliti odgovornosti za upravljanje mrežom, uz odvajanje odgovornosti vezanih za aktivnosti koje se provode na mrežnoj opremi od odgovornosti vezanih za aktivnosti koje se provode na sustavima spojenim na mrežu;
b) dizajnirati mrežu uzimajući u obzir povjerljivost, integriteta i dostupnost informacija i uzimajući u obzir uporabu alata i rješenja za filtriranje i kontrolu mrežnog prometa;
c) dizajnirati mrežne pristupne točke uz posebnu pažnju na javne točke;
d) osigurati siguran prijenos informacija u mreže izvan informacijskog sustava Tvrtke kako bi se zaštitila povjerljivost, integritet i dostupnost prenošenih informacija;
e) bilježiti i odobriti sve faze (dizajn, testiranje, produkcija) razvoja i implementacije novih mrežnih usluga;
f) utvrditi kriterije za određivanje kritičnih događaja koje je potrebno bilježiti;
g) periodički provoditi pregled i ažuriranje konfiguracija i sigurnosna pravila mrežne opreme;
h) bilježiti svaku promjenu u konfiguraciji mrežne opreme;
i) zaštititi informacije o mrežnim adresama i konfiguracijama od neovlaštenog pristupa;
j) implementirati sustave za sprečavanje i otkrivanje upada i sustave za nadzor mreže;

k) planirati uporabu odgovarajućih sigurnosnih mjera (npr. kriptografija, sigurnosne kopije, digitalni potpis) kako bi se osigurala povjerljivost informacija, integritet i neporecivost;
l) utvrditi odgovarajuće mjere kako bi se osigurala dostupnost mreže u skladu sa zahtjevima poslovnih procesa;
m) osigurati da se događaji nadziru i bilježe u skladu s mogućnostima koje nudi mrežna oprema;
n) periodički provoditi testove provjere i upada kako bi se otkrila ranjivost koja predstavlja potencijalnu prijetnju integritetu informacijskog sustava Tvrtke, u skladu s primjenjivim trenutno važećim zakonskim aktima;
o) u slučaju da se izričito traži u zakonskim aktima potrebno je pohraniti standardne konfiguracije s mrežnih uređaja

6.8.3. Zaštita mrežne opreme

Mrežni sustavi i oprema moraju biti odgovarajuće zaštićeni.

Smjernice:

a) zaštititi konfiguracijske datoteke, dijagnostičke i administrativne priključke mrežnim sustavima i opremi s lokalnim i udaljenim pristupom, u skladu s trenutno važećim zakonskim aktima;
b) ograničiti pristup mrežnoj opremi (vatrozidi, ruteri, itd.), s adekvatnim sigurnosnim mehanizmima, za aktivnosti upravljanja i administracije isključivo nadležnom i ovlaštenom tehničkom osoblju koje ima odgovarajući korisnički profil, u skladu s trenutno važećim zakonskim aktima.

6.8.4. Kontrola spajanja na mrežu

Na osnovu mehanizama za prepoznavanje (npr. vatrozida) mrežne adrese klijenata i servera potrebno je definirati tehničke mjere sigurnosti za nadzor i ograničavanje spajanja.

6.8.5 Upravljanje mrežom

Potrebno je definirati proces upravljanja mrežom.

Smjernice:

a) izraditi i ažurirati mrežnu dokumentaciju (u smislu topologije, aktivnih servisa itd.), u skladu s trenutno važećim regulatornim aktima

6.9. Životni ciklus sustava i mreže

Moraju se utvrditi odgovarajuće odgovornosti, procedure i kriteriji prihvatljivosti za dizajn, razvoj, promjene i zamjenu sustava i mreža.

6.9.1. Sigurnosni zahtjevi

Sigurnosni zahtjevi novih sustava i mreža moraju se analizirati kako bi služili kao smjernice u izboru sigurnosnih mjera za zaštitu informacija koje ti sustavi i mreže koriste.

Smjernice:

a) iznijeti i zabilježiti sigurnosne zahtjeve sustava i mreže koji osiguravaju povjerljivost, integritet i dostupnost informacija koje koriste navedeni sustavi i mreže;
b) na temelju sigurnosnih zahtjeva utvrđenih u točki a), odrediti odgovarajuće sigurnosne mjere u skladu s onima iz povezanog informacijskog okruženja;
c) odrediti koja će poslovna jedinica verificirati implementirane mjere u skladu sa sigurnosnim zahtjevima utvrđenim u točki a), što se tiče točnosti, potpunosti i kompatibilnosti s postojećom sigurnosnom infrastrukturom.

6.9.2. Dizajn i izrada sustava i mreža

Tehnička rješenja moraju biti dizajnirana i razvijena u skladu s rezultatima analiza sigurnosnih zahtjeva.

Smjernice:

a) dizajnirati i dokumentirati rješenje je u skladu s utvrđenim sigurnosnim zahtjevima, tehnološkim kontekstom i uputama proizvođača sustava;

b) obaviti razvoj i testiranje promjena sustava i mreže u propisno konfiguriranim okruženjima kako bi se osigurala pouzdanost rezultata testiranja;
c) izraditi dizajn i razvoj novih komponenti softvera u skladu sa standardima i pravilima razvoja aplikacija.

6.9.3. Kriteriji prihvatljivosti sustava

Moraju se definirati kriteriji prihvatljivosti za implementaciju sustava i mreže kako bi se omogućila procjena njihovog pravilnog funkcioniranja.

Smjernice:

a) definirati i formalizirati proceduru koja bi osigurala utvrđivanje kriterija i zahtjeva prihvatljivosti sustava i mreže, kako bi se oni prihvatili, dokumentirali i propisno potvrdili i sa strane sigurnosti.

6.9.4 Upravljanje izmjenama mreže i sustava

Odgovornosti i procesi povezani s upravljanjem izmjenama sustava i mreže moraju biti formalizirane. Posebnu pažnju treba obratiti na promjene operativnih sustava koje mogu imati utjecaj na funkcioniranje mreže i sustava.

Smjernice:

a) dodijeliti odgovornosti za upravljanje promjenama sustava i mreža, za utvrđivanje potrebnih ili odgovarajućih promjena i za instalaciju ažuriranih verzija, ispravaka ili sigurnosnih zakrpa.
b) odrediti kriterije za klasifikaciju odgovarajućih promjena sustava na temelju prioriteta, razina autorizacije i sigurnosnih mjera te osigurati da razine i mjere odgovaraju navedenim promjenama;
c) utvrditi koje instance mogu zahtijevati preinake, uz određivanje odgovarajuće metode za rješavanje zahtjeva (predaja, autorizacija, dokumentacija i registracija);
d) procijeniti moguće utjecaje promjena sustava i mreža na aplikacije sa stanovišta informacijske sigurnosti;
e) osigurati da sve potrebne sigurnosne kopije budu napravljene i zaštićene prije bilo kakvih promjena sustava ili mreža u svrhu osiguravanja mogućnosti povrata sustava ili mreža u prethodno stanje;

f) planirati i provesti odgovarajuće sigurnosne procedure kako bi se spriječile neovlaštene promjene sustava i mreža;
g) obaviti promjene nabavljenih sustava i mreža prema ugovornim odredbama;
h) pohranjivati zapise o svim poduzetim aktivnostima;
i) pratiti funkcionalnosti sustava koje mogu izmaći sigurnosnoj kontroli, uz uklanjanje ili onemogućavanje onih koje nisu potrebne, praćenje onih koje ostaju instalirane i omogućene te provjeru da su ovlaštenja pravilno dodijeljena

7. RAZVOJ I ODRŽAVANJE APLIKACIJA

Pravilno upravljanje informacijskom sigurnošću zahtijeva razvoj i nadogradnju aplikacija koji se odvija na strukturiran i kontroliran način.

Aplikacije čine važan element upravljanja informacijskim sustavom Tvrtke i moraju se zaštiti na primjeren način kako bi se zajamčila povjerljivost, integritet i raspoloživost informacija koje obrađuju.

U svrhu postizanja, jačanja i održavanja sigurnosti aplikacija u svim se fazama životnog ciklusa aplikacija mora upravljati na kontrolirani način. Spomenute faze obuhvaćaju sljedeće:

a) razvoj: određivanje zahtjeva, dizajna, implementacije i testova jedinica;
b) certifikacija: testiranje funkcija i zahtjeva;
c) održavanje i modifikacija: upravljanje korektivnim, evolucijskim modifikacijama i modifikacijama prilagodbe i održavanja.

7.1. Sigurnosni zahtjevi

Potrebno je identificirati primjerene mjere kako bi se osigurali zahtjevi povjerljivosti, integriteta i dostupnosti informacija. Prilikom razvoja tih mjera potrebno je obratiti pažnju na okolinu i na način na koji će se koristiti, kako će se integrirati u postojeće sustave i na njihovu sukladnost sa zakonskim propisima i internim pravilima.

7.1.1. Analiza sigurnosnih zahtjeva

Proces razvoja aplikacija mora se planirati i implementirati na način koji obuhvaća sigurnosne zahtjeve analitičke faze novih i modificiranih aplikacija.

Spomenuti zahtjevi predstavljaju smjernicu pri odabiru sigurnosnih mjera za zaštitu informacija koje se obrađuju putem aplikacija.

Smjernice:

a) obrazložiti i dokumentirati sigurnosne zahtjeve aplikacija te osigurati njihovu primjerenost klasifikacijskoj razini informacija koje se obrađuju putem aplikacija;

b) identificirati modele uporabe informacija koje se obrađuju putem aplikacija, ograničiti suvišno na minimalno neophodnu mjeru;
c) razviti procese i postupke radi utvrđivanja i naglašavanja prikladnih zaštitnih mjera na temelju sigurnosnih zahtjeva propisanih u točki a);
d) identificirati organizacijski dio Tvrtke koji će verificirati da su implementirane mjere u skladu sa sigurnosnim zahtjevima propisanim u točki a), u pogledu točnosti, potpunosti i sukladnosti s postojećom sigurnosnom infrastrukturom, te provesti formalnu validaciju (potvrđivanje valjanosti) aplikacija prije njihove implementacije na produkcijskoj okolini;
e) izvršiti periodične provjere tijekom razvoja softvera aplikacija kako bi se osigurala pravilna implementacija sigurnosnih zahtjeva.

7.2. Kontrole sigurnosti aplikacija

Pristup aplikacijama dozvoljen je isključivo ovlaštenim zaposlenicima korištenjem eksternih mehanizama (izvan aplikacije) za identifikaciju, provjeru autentičnosti (autentikaciju) i autorizaciju.

Mehanizmi nadzora, potvrđivanja valjanosti (validacije) i evidentiranja aktivnosti koje se provode nad informacijama moraju biti planirani i implementirani sukladno s zakonima. Trebaju se razviti primjerene metode za kontrolu koda (sigurni kod) i primjerene protumjere za osiguravanje dostupnosti informacija i neporecivost.

7.2.1. Implementacija kontrola pristupa

Potrebno je implementirati mehanizam koji će ograničiti pristup aplikacijama isključivo ovlaštenim zaposlenicima sukladno s poslovnim potrebama. Spomenuti mehanizmi trebaju biti primjereni poslovnim potrebama i trebaju onemogućiti neprimjerenu uporabu, modifikacije ili neovlašteno prosljeđivanje informacija poštujući pritom načelo najmanjeg prava.

Smjernice:

a) implementirati kontrole za autentikaciju i autorizaciju radi regulacije pristupa aplikacijama od strane korisnika. Spomenute kontrole trebaju sadržavati zajedničke infrastrukturne procedure i komponente izvan samih aplikacija;

b) dizajnirati i strukturirani aplikaciju na način da se pristup informacijama ili postupci obrade (čitanje, umetanje, brisanje, uređivanje) mogu razlikovati i razvrstati radi omogućavanja primjerenog profiliranja pristupa.

7.2.2. Validacija ulaznih podataka

Potrebno je odrediti postupke i kontrole, sintaktičke i semantičke, radi validacije ulaznih podataka za aplikaciju.

Smjernice:

a) odabrati mehanizam za provjeru valjanosti ulaznih podataka, dodijeliti odgovornosti zbog pouzdanog rada mehanizama.

7.2.3. Interne kontrole

Potrebno je planirati i implementirati primjerene mehanizme za očuvanje integriteta podataka za vrijeme procesnih faza. Također je potrebno implementirati mehanizme za otkrivanje i ispravljanje grešaka u obradi podataka.

Smjernice:

a) razviti interne aplikativne kontrole za verifikaciju pravilne obrade podataka radi sprečavanja pogrešaka ili nedozvoljenih radnji koje bi mogle ugroziti integritet podataka.
b) planirati i implementirati postojanje logova kako bi se evidentirale radnje izvedene pomoću aplikacija.

7.2.4. Zaštita podataka prilikom prijenosa

Potrebno je implementirati mehanizme za zaštitu integriteta podataka prilikom prijenosa.

Smjernice:

a) implementirati primjerene protumjere radi onemogućavanja neovlaštenog presretanja ili modifikacije sadržaja poslane informacije.

7.2.5. Validacija izlaznih podataka

Potrebno je odrediti postupke i kontrole, i sintaktičke i semantičke, radi validacije izlaznih podataka za aplikaciju.

Smjernice:

a) razviti primjerene kontrole i postupke radi provjere izlaznih podataka obzirom na greške u obradi i dodijeliti odgovornosti radi osiguravanja pouzdanog funkcioniranja protumjera.

7.2.6. Dostupnost aplikacijskih podataka

Potrebno je planirati i implementirati primjerene mehanizme radi osiguravanja dostupnosti podataka.

Smjernice:

a) definirati zahtjeve za izradu sigurnosnih kopija aplikacijskih podataka kojima se propisuje za koje se podatke trebaju stvarati sigurnosne kopije, koliko često i na koji način ih je potrebno pohraniti, sukladno s poslovnim potrebama i zakonskim propisima;
b) u suradnji s nadležnim rukovodstvom, potrebno je identificirati primjerene arhitekturne postavke (postavke aplikacija, sustava i mreže) radi osiguravanja primjerene razine dostupnosti aplikacija.

7.2.7. Potencijalno štetan kod

Potrebno je planirati i implementirati zaštitne i kontrolne mjere (siguran kod) radi onemogućavanja ulaska potencijalno štetnog softvera (maliciozan kod) u aplikacije.

Smjernice:

a) utvrditi postupke i kontrole za onemogućavanje ulaska potencijalno štetnog koda u aplikacije i nadzor aplikacija obzirom na prisutnost takvog koda, neovisno o tome jesu li aplikacije razvijene interno ili od strane ugovornog partnera.

7.2.8 Uporaba kriptografskih kontrola

Na temelju klasifikacijske razine informacija koje se obrađuju putem aplikacija potrebno je analizirati mogućnost uporabe kriptografskih tehnika

Smjernice:

a) razmotriti mogućnost uporabe kriptografskih kontrola na temelju vrijednosti informacija koje se obrađuju aplikacijama i specifičnih zahtjeva aplikacija ili zakonskih odredbi s ciljem osiguravanja povjerljivosti, integriteta i nemogućnosti nijekanja.

7.3. Siguran razvoj aplikacija

Sigurnosni aspekti moraju se kontrolirati na primjeren način i dokumentirati za vrijeme implementacije aplikacije i faza modifikacije radi osiguravanja pouzdanog rada aplikacija. Posebice je važno provesti dodjelu odgovornosti putem postupka autorizacije kako bi se procesom razvoja, neovisno o tome vrši li se interno ili od strane ugovornog partnera, moglo upravljati na kontroliran način s mogućnosti provjere.

7.3.1. Interni razvoj novih aplikacija

Potrebno je odrediti specifične zaštitne mjere za kontrolirano, sigurno upravljanje fazama razvoja aplikacija s mogućnosti verifikacije.

Smjernice:

a) osigurati kontrolu, evidentiranje i dokumentiranje povijesti određene aplikacije za cjelokupan razvoj i održavanje softvera;
b) provoditi aktivnosti razvoja aplikacija u odvojenom IT okruženju, okruženje bi trebalo biti usklađeno s produkcijskom okolinom u pogledu verzije i ažuriranja. Usvojiti sigurnosne mjere kako bi se spriječilo povezivanje produkcijskih podataka s osobnim podacima te osigurala povjerljivost svih kritičnih podataka;
c) implementirati sigurnosne zahtjeve propisane i verificirane u fazi analize sigurnosnih zahtjeva (vidi 7.1.1);
d) dokumentirati implementirane sigurnosne mjere, odnosno utvrđene sigurnosne zahtjeve;
e) zaštiti izvorni kod od svih vrsta neovlaštenih promjena;

f) koristiti podatke koji se ne mogu povezati s produkcijskim podacima u okviru svih radnji vezanih uz razvoj i testiranje;
g) koncipirati tehničku i operativnu dokumentaciju razvojne faze koja ujedno obuhvaća i testiranje funkcionalnosti.

7.3.2. Modifikacije aplikacija

Potrebno je odrediti primjerene postupke za kontrolu implementacije promjena na aplikacijama.

Smjernice:

a) definirati aktivnosti za upravljanje promjenama aplikacija, neovisno o tome provode li se iste interno ili od strane ugovornog partnera. Spomenute aktivnosti trebaju specificirati radnje koje je potrebno provesti i odgovornosti osoblja koje sudjeluje u različitim fazama, uključujući faze autorizacije. Navedenim aktivnostima se specificiraju i mehanizmi kontrole i nadzora zbivanja prilikom migracije aplikacija s jedne okoline na drugu;
b) organizirati promjene aplikacija na strukturiran način kako bi se iste grupirale prema izdavanju, logički i/ili kronološki te u skladu s zahtjevima korisnika i prihvatljivim razinama rizika;
c) definirati postupke za obnavljanje stanja prije promjene te procijeniti učinak koji bi to obnavljanje imalo na dostupnost povezanih sustava;
d) napraviti sigurnosnu kopiju izvornog koda i izvršnog koda prije provođenja bilo koje vrste promjena na aplikacijama;
e) odrediti i implementirati kriterije za upravljanje različitim verzijama aplikacije;
f) provesti promjene aplikacija u namjenskom okruženju za razvoj;
g) utvrditi i implementirati aktivnosti za obnavljanje primjerne razine zaštite sukladno sa sigurnosnim zahtjevima aplikacije na kojoj se provode promjene;
h) utvrditi metodologije i vremenske okvire za izdavanje promjena u produkcijsko okruženje s ciljem očuvanja kontinuiranog poslovnog procesa i minimalizacije prekida usluge;
i) modifikacije se ne smiju implementirati u produkcijskoj okolini prije nego li što se verificiraju i prihvate putem specifičnog procesa autorizacije; potrebno je voditi evidenciju o svim provedenim promjenama;
j) nakon svake promjene potrebno je ažurirati dokumentaciju.

7.3.3. Tehnički pregled aplikacija nakon provedbe promjena na sustavu

Potrebno je verificirati ispravan rad aplikacija te po potrebi poduzeti korektivne mjere slijedeći radnje za održavanje operativnih sustava.

Smjernice:

a) prije izdavanja promjena ili ažuriranja operativnih sustava na produkcijskoj okolini, s iznimkom specifičnih hitnih slučajeva koji su na primjeren način autorizirani i zabilježeni, potrebno je osigurati da su funkcionalnosti aplikacija, uključujući one vezane uz sigurnost informacija, testirane i verificirane te da su izvršene sve potrebne ili prikladne izmjene programa, kontrola i postupaka.

7.3.4. Razvoj aplikacija od strane ugovornog partnera

Potrebno je definirati i unijeti primjerne kontrole u ugovore kako bi se osigurala kvaliteta i sigurnost svakog softvera koji se razvija ili održava od strane ugovornog partnera.

a) osigurati da se usvoje minimalno iste zaštitne mjere poput onih definiranih za interni razvoj novih aplikacija, ako razvoj obavlja ugovorni partner. Iste mjere se moraju sistematizirati u vidu prikladnih ugovornih odredbi i nadopuniti specifičnim mjerama za pokrivanje rizika provođenja tih radnji od strane ugovornog partnera;
b) utvrditi pravila koja ponavljaju ugovorne odredbe za vanjske djelatnike koji sudjeluju u razvoju aplikacija;
c) verificirati sukladnost sigurnosnih funkcionalnosti nabavljenog softvera s primjenjivim sigurnosnim pravilima Tvrtke.

7.3.5. Nabavka aplikacijskih paketa od treće strane

Potrebno je odrediti primjerene metode i postupke za odabir i nabavku aplikacijskih paketa od trećih strana.

Smjernice:

a) utvrditi pravila odabira i nabavke aplikacijskog softvera radi osiguravanja verifikacije usvojenih sigurnosnih zahtjeva i onih potrebnih za instalaciju i upravljanje proizvodom;

b) izrada prikladnih ugovornih odredbi radi osiguravanja sukladnosti softverskih paketa sa sigurnosnim pravilima Tvrtke u pogledu sigurnosti i pružanja usluge, te sa zakonskim i propisnim odredbama u pogledu sigurnosti; te ujedno osigurati kompatibilnosti softvera s implementiranim sigurnosnim upravljanjem i kontrolnim alatom;
c) koristiti aplikacijski softver zaštićen autorskim pravom sukladno s odredbama u provedivim ugovorima o licenciranju;
d) verificirati sukladnost sigurnosnih i operativnih funkcionalnosti nabavljenog softvera sa specifikacijama ugovora.

7.3.6 Modifikacije nabavljenog aplikacijskog softvera

Aplikacijski softver nabavljen izvan Tvrtke smije se modificirati isključivo u skladu s odredbama ugovora.

Smjernice:

a) modificirati, prilagoditi i konfigurirati nabavljen softver i hardver isključivo na način naveden u primjenjivim ugovorima;
b) čuvati master kopije i dokumentaciju aplikacijskog softvera nabavljenog izvan Tvrtke na sigurnom mjestu;
c) verificirati da korisničke postavke ne ugrožavaju razinu sigurnosti aplikacije.

7.3.7. Certificiranje funkcionalnosti aplikacije

Aplikacije se trebaju testirati i certificirati. Postupak certificiranja obuhvaća testiranje primjerenosti implementiranih funkcionalnosti ujedno i u okviru specificiranih i dokumentiranih sigurnosnih zahtjeva. Aplikacije moraju slijediti specifičan proces autorizacije kako bi se mogle implementirati na produkcijskoj okolini.

Smjernice:

a) provesti provjeru i ovjeru funkcionalnosti aplikacije u vidu integracije i međusobnih odnosa s postojećom infrastrukturom i aplikacijama, pri čemu se posebna pažnja treba posvetiti pristupnim korisničkim profilima te drugim sigurnosnim aspektima;

b) provesti provjeru i ovjeru funkcionalnosti aplikacija na IT okolinama koje su odvojene od produkcijske okoline, ali sukladno s odredbama sigurnosnih mjera i konfiguracija;

c) provesti barem jedan test koristeći podatke koji su sukladni produkcijskim podacima. Koristiti zaštitne mjere prilikom provođenja testova kako bi se osigurala povjerljivost podataka koji su klasificirani kao *kritični* te spriječilo povezivanje osobnih podataka s produkcijskim podacima. Alternativu predstavlja čuvanje povjerljivosti podataka koristeći jednake sigurnosne mjere kao i na produkcijskoj okolini;

d) dodijeliti provjeru i ovjeru funkcionalnosti aplikacija osoblju koje nije izravno sudjelovalo u razvoju tih aplikacija;

e) provesti testiranje funkcionalnosti aplikacija na temelju testnih slučajeva dobivenih od nadležnih instanci Tvrtke i zabilježiti sve nedostatke vezane uz sigurnosne zahtjeve;

f) utvrditi metodologije i postupke za provjeru funkcionalnosti kojima se specificiraju alati i tehnike koji bi se trebale koristiti;

g) provoditi primjerene testove za verifikaciju kapacitetnih mogućnosti aplikacije prilikom najvećih opterećenja u vidu broja istovremenih korisnika i količine podataka koji se obrađuju;

h) dokumentirati provedene slučajeve testiranja i s njima povezane rezultate;

i) provoditi sve korektivne mjere potrebne za uklanjanje uočenih anomalija u razvojnoj okolini i ponoviti testove;

j) identificirati koji će organizacijski dio ispitati rezultate testiranja i procesa provjere funkcionalnosti i formalno autorizirati implementaciju aplikacija u produkcijskoj okolini;

k) implementirati sve potrebne izmjene ili dodatke planovima za kontinuitet poslovanja uz sudjelovanje odgovornih organizacijskih dijelova prije implementacije aplikacije na produkcijskoj okolini;

l) omogućiti da se podaci i korisnički računi korišteni za potrebe testiranja uklone prije aktivacije / distribucije sustava i aplikacija.

8. KONTINUITET POSLOVANJA I OPORAVAK NAKON KATASTROFE

Smjernice za kontinuitet poslovanja u izvanrednim uvjetima predlažu strukturirani pristup koji obuhvaća sljedeće:

- *Upravljanje kontinuitetom poslovanja*: inicijative i mjere usmjerene na redukciju šteta do prihvatljivih razina, pri čemu su štete posljedice incidenata ili katastrofa, a izravno ili neizravno utječu na poslovanje;
- *Plan kontinuiteta poslovanja*: dokument u kojem su sistematizirana načela, zadani ciljevi i opisani postupci za kontinuitet upravljanja *kritičnim poslovnim procesima*;
- *Plan oporavka nakon katastrofe*: tehničke i organizacijske protumjere kojima se odgovara na događaje koji prekidaju rad sistem sale i osiguravaju rad vitalnih informacijskih procesa na alternativnim lokacijama. Plan oporavka nakon katastrofe je sastavni dio Plana kontinuiteta poslovanja.

Pritom se *proces* smatra *kritičnim* kada bi njegovim prekidom nastale znatne štete za Tvrtku. Kritični procesi u Tvrtki stoga potražuju visoki kontinuitet poslovanja koji se postiže putem preventivnih mjera i mjera za odgovor u izvanrednim uvjetima koje bi se trebale implementirati u slučaju incidenta koji ugrožava sigurnost.

Informacije o kontinuitetu poslovanja navedene u ovom poglavlju sukladne su s kontrolama i odredbama navedenim u standardu ISO 27001 i iscrpnim zahtjevima sustava za upravljanje informacijskom sigurnošću. Daljnje analize i ažurirane procjene povezanih problematika sadržane su u dotičnim smjernicama.

8.1. Upravljanje kontinuitetom poslovanja

Dostupnost informacijskih usluga koje podupiru procese od *sistemske važnosti,* načelno i specifično vezano uz upravljanje odnosima s klijentima i upravljanje računima, mora biti zajamčena putem razvoja primjerenih planova za reakciju kako bi se osiguralo obnavljanje funkcionalnosti u okviru unaprijed određenih vremenskih okvira za posljedice nepredvidljivih zbivanja, koja imaju određeni učinak na pružanje tih usluga.

8.1.1. Plan upravljanja u hitnim i kriznim situacijama

Potrebno je razviti Plan upravljanja u hitnim i kriznim situacijama. Navedeni plan mora sadržavati postupke koji se trebaju implementirati u okviru koordiranog pristupa upravljanju koji osigurava jasnu podjelu odgovornosti i ovlasti. Ovi postupci predstavljaju sastavni dio šireg sustava za upravljanje incidentima.

Smjernice:

a) odrediti odgovornosti, uspostaviti i periodički testirati djelotvoran i uspješan plan kontinuiteta poslovanja i plan oporavka nakon katastrofe, na način da vezane procedure može koristiti i nestručno osoblje;
b) dodijeliti i dokumentirati odgovornosti za upravljanje hitnim i kriznim situacijama.

8.1.2. Analiza utjecaja na poslovanje

Potrebno je identificirati prioritete u okviru obnavljanja poslovnog procesa putem strukturiranog metodološkog pristupa analizi i predviđanju utjecaja prekida usluge i razvitkom najprimjerenijih mjera obnove.

Smjernice:

a) razviti i dokumentirati metodologije analize radi utvrđivanja procesa Tvrtke koji imaju najveću utjecaj na poslovanje i definirati iste kao kritične procese. Analizirati i ažurirati te kritične procese dokumentiranjem imovine koja ih podržava;
b) identificirati mjere radi osiguravanja kontinuiteta procesa na temelju rezultata analiza navedenih u točki a);
c) rezidualni rizici, kojima se ne upravlja u planu kontinuiteta poslovanja, moraju biti jasno dokumentirani i odobreni od strane rukovodstva.

8.1.3. Razvoj i implementacija planova za kontinuitet poslovanja

Planovi za kontinuitet procesa moraju se sistematizirati, pregledati i ažurirati putem dodjele odgovornosti, razvojem, dokumentacijom i implementacijom postupaka i obukom osoblja. Nadalje, potrebno je detaljno razviti kriterije i pravila kako bi se osigurala potpunosti i ispravnost informacija za vrijeme faze obnove koja slijedi nakon hitnih situacija.

Smjernice:

a) dodijeliti uloge i odgovornosti radi određivanja planova kontinuiteta za svaki proces, u skladu s trenutno važećim regulatornim aktima;
b) utvrditi planove kontinuiteta za svaki proces, uzimajući u obzir operativne procedure i uključene resurse;
c) neprestani nadzor planova kontinuiteta radi osiguravanja njihove sukladnosti s realnim stanjem sustava i aplikacija i referentnim scenarijem;
d) izvršiti obuku osoblja u pogledu postupaka u hitnim situacijama i aktivnostima radi osiguravanja kontinuiteta svakog individualnog procesa.

8.1.4. Plan kontinuiteta poslovanja

Potrebno je razviti plan kontinuiteta poslovanja koji uključuje komponentu oporavka nakon katastrofe. Putem integracije planova kontinuiteta za svaki individualni proces i primjernih pravila za implementaciju plana kontinuiteta poslovanja, upravljanje hitnim slučajevima i ponovno uspostavljanje normalnog poslovanja, plan kontinuiteta poslovanja treba osigurati da se prekid usluge uzrokovan greškama, padom sustava ili nezgodama svede na utvrđene prihvatljive granice.

Smjernice:

a) odrediti odgovornosti za razvoj planova kontinuiteta poslovanja i oporavka nakon katastrofe koji se tiču procesa, sustava i eksternaliziranih aktivnosti;
b) razviti planove kontinuiteta poslovanja i oporavka nakon katastrofe, uzimajući u obzir i aspekte definirane trenutno važećim regulatornim aktima;
c) odrediti i uspostaviti programe za informiranost i obuku osoba u Tvrtki koji su zaduženi za upravljanje i primjenu plana u izvanrednim situacijama i implementaciju mjera radi osiguravanja kontinuiteta poslovanja Tvrtke.

8.1.5. Testiranje, održavanje i izdavanje planova za kontinuitet poslovanja

Planovi kontinuiteta poslovanja moraju se redovito testirati i ažurirati.

Smjernice:

a) obavljati periodična testiranja reakcijskih mjera na incidente, nepravilnosti u radu, kvarove ili nezgode kako bi se osigurao njihov ispravan rad i potvrdilo da je ponašanje svih uključenih zaposlenika u skladu s utvrđenim procedurama.

8.2. Oporavak nakon katastrofe

Mogućnost uspostave svih potrebnih funkcionalnosti informacijskog sustava Tvrtke nakon izrazito ozbiljnih prekida (katastrofa) mora biti osigurana u svako doba.

8.2.1. Kriteriji za planiranje oporavka nakon katastrofe

Primjerene tehnološke mjere moraju se razviti kako bi se osigurala uspostava svih potrebnih funkcionalnosti informacijskog sustava nakon katastrofe.Te mjere moraju biti sukladne s prioritetima obnove definiranim u Analizi utjecaja na poslovanje (BIA).

Smjernice:

a) odabrati neovisnu fizičku lokaciju za pomoćni (sekundarni) sustavi i infrastrukturu koji služe za obnovu informacijskih usluga. Spomenuta alternativna lokacija mora biti izvan istog grada i dovoljno udaljena i odvojena od primarne lokacije i pružati odgovarajuću servisnu podršku između primarne i sekundarne strane, kako bi se osiguralo da zbivanja koja utječu na jednu lokaciju neće utjecati i na drugu;
b) odrediti primjerene mrežne veze kako bi se omogućilo korištenje informacijskih usluga koje omogućuje alternativna lokacija;
c) razviti primjerene sustave za oporavak nakon katastrofe i mjere u svrhu omogućavanja pouzdanog rada informacijskog sustava pri najvećim opterećenjima koja su uočena za vrijeme uobičajenih poslovnih aktivnosti i slučaju eventualnih gubitaka malih količina podataka, u skladu s trenutnim regulatornim zahtjevima;
d) odrediti mjere koje će omogućiti obnovu sistemskih procesa u okviru vremenskih okvira navedenih u Analizi utjecaja na poslovanje i/ili uputama danim na bazi svakog pojedinačnog slučaja od strane regulatornih tijela;
e) utvrditi procese i postupke za uspostavu svih potrebnih usluga na sekundarnoj lokaciji;
f) odrediti i implementirati uobičajena testiranja plana za obnovu nakon katastrofe.

9. KLASIFIKACIJA INFORMACIJA I INVENTURA

Klasificiranje informacija znači pridruživanje određenih zahtjeva za povjerljivost, integritet i dostupnost toj informaciji.

Klasifikacija informacija osigurava temelj za određivanje sigurnosnih uvjeta za informacijsku imovinu i predstavlja osnovni element u procjenjivanju rizika vezanih za informacijsku imovinu Tvrtke od nepravilna korištenja ili postupanja s informacijama.

Postupak klasificiranja mora obuhvatiti sve vrste informacija, dokumenata koji sadrže informacije i programe (osnovni softver, aplikacijski softver i pojedinačno proizveden softver) koji koriste ili obrađuju informacije, bez obzira na to na koji su način informacije, dokumenti ili programi pohranjeni.

9.1. Klasifikacija informacija

Informacije, bez obzira na vrstu, format, metodu pohrane ili alate koji su korišteni za njihovu obradu ili razmjenu, moraju biti klasificirane s obzirom na zahtjeve za povjerljivost, integritet i dostupnost korištenjem posebnih metoda u svrhu određivanja odgovarajućih razina zaštite.

9.1.1. Model klasifikacije informacija

Mora se usvojiti jedinstven model klasifikacije informacija na razini cijele Tvrtke, koji omogućava usvajanje mjera koje su prikladne za klasifikacijsku razinu koja je pridružena informaciji.

Smjernice:

a) razviti i dokumentirati model klasifikacije informacijske imovine koji se temelji na zahtjevima za povjerljivost, integritet i dostupnost informacija;
b) odrediti i dokumentirati odgovornosti, postupke, metode i alate za upravljanje klasifikacijskim razinama koje su pridružene informacijskoj imovini;
c) razviti i dokumentirati kriterije za određivanje primjerenih metoda zaštite informacijske imovine na osnovu klasifikacijske razine;
d) definirati i formalizirati uloge za upravljanje informacijama u ovisnosti o njihovoj klasifikacijskoj razini, u skladu s trenutnim regulatornim zahtjevima.

9.1.2. Određivanje klasifikacijske razine

Informacijska imovina mora biti označena, točno navodeći klasifikacijsku razinu za svaku informaciju kako bi se osiguralo da se s njima ispravno upravlja.

Smjernice:

a) nedvosmisleno označiti informacijsku imovinu (fizički ili logički) s pridruženom klasifikacijskom razinom na osnovu standardiziranih kriterija;
b) propisati prikladne metodologije za upravljanje elektroničkim i ispisanim dokumentima u skladu s klasifikacijskom razinom informacija koje se u njima nalaze, osiguravajući povjerljivost, integritet i dostupnost informacija.

9.2. Popisivanje imovine

Potrebno je dodijeliti odgovornosti za zaštitu informacijske imovine, te je potrebno razviti metode za pripremu, upravljanje i održavanje popisa informacijske imovine.

9.2.1. Upravljanje popisom

Moraju se razviti metode za razvoj i upravljanje inventurom informacijske imovine, i s time u skladu trebaju se dodijeliti odgovornosti.

Smjernice:

a) odrediti i dokumentirati koju je informacijsku imovinu potrebno popisati;
b) dodijeliti i dokumentirati odgovornosti za zaštitu informacijske imovine koja je određena u točki a), u skladu s trenutnim regulatornim zahtjevima;
c) pripremiti i upravljati popisivanjem informacijske imovine iz točke a), dodjeljujući odgovornosti za prvu procjenu i kasnije ažuriranje, te uzimajući u obzir cjelokupan životni ciklus imovine;
d) prekontrolirati popis barem jednom godišnje kako bi se utvrdila njegova točnosti i potpunost, bilježeći svaku anomaliju i podnositi izvještaje o njima odgovarajućoj službi u Tvrtki

10. UPRAVLJANJE SIGURNOSNIM INCIDENTIMA

Upravljanje informacijskom sigurnošću zahtijeva učinkovit sustav za praćenje i kontrolu sumnjivih situacija i sigurnosnih incidenata. U ovome je slučaju potrebna stalna pozornost i potrebno je razviti model upravljanja koji će na učinkovit način prepoznati, reagirati i riješiti situacije koje za sobom povlače rizik od narušavanja povjerljivosti, integriteta i dostupnosti informacija.

10.1. Izvještavanje o događajima

Potrebno je uspostaviti odgovarajuće metode i kanale za komunikaciju u svrhu hitne prijave incidenata i sumnjivih situacija, minimiziranja štete i sprječavanja ponavljanja neprimjerenih radnji.

10.1.1 Prijavljivanje incidenta koji ugrožavaju informacijsku sigurnost

Potrebno je odrediti postupke za prijavljivanje sigurnosnih incidenata i sumnjivih situacija.

Smjernice:

a) uspostaviti metode i alate za prijavljivanje sigurnosnih incidenata i sumnjivih situacija te donošenje odluke o tome koji će organizacijski dijelovi biti uključeni;
b) izrada obrazaca za prijavu sigurnosnih incidenata i sumnjivih situacija i određivanje neophodnih informacija za rješavanje incidenata ili situacija;
c) utvrđivanje smjernica i programa izobrazbe za djelatnike, koji se odnose na sigurnosne događaje i mjere reagiranja.

10.2. Upravljanje incidentima

Potrebno je odrediti odgovarajuće odgovornosti i postupke za upravljanje sigurnosnim incidentima.

10.2.1. Upravljanje incidentima

Postupci i odgovornosti moraju se odrediti u svrhu osiguranja brze, učinkovite i organizirane reakcije na sigurnosne incidente. Ovisno o ozbiljnosti nastalog prekida usluge, postupci upravljanja moraju u obzir uzeti različite stupnjeve eskalacije u skladu s planom za upravljanje u izvanrednim situacijama i krizama.

Smjernice:

a) odrediti koji su organizacijski dijelovi zaduženi za reagiranje na napade i sigurnosne incidente te dodijeliti odgovarajuće odgovornosti za koordinaciju, reagiranje, ograničavanje štete i prikupljanje podataka;

b) odrediti i klasificirati potencijalne incidente prema vrsti, težini i proizašlom utjecaju, odrediti prijelazne kriterije između različitih stupnjeva i odrediti najdulje vrijeme za reagiranje;

c) planirati različite stupnjeve eskalacije ovisno o težini incidenta;

d) utvrditi aktivnosti za uočavanje, aktiviranje funkcija za upravljanje odgovora na sigurnosne incidente, ograničavanje utjecaja i interakcija između subjekata unutar Tvrtke koji su pogođeni te nadležnih tijela, osiguravanje brzu reakciju nadležnih instanci Tvrtke i onemogućavanje promjene dokaza;

e) utvrditi metode i alate za prijavljivanje incidenata ili sumnjivih situacija, obavještavanje odgovornih osoba i nadležnog rukovodstva, te arhiviranje i predočavanje dokumentacije o incidentu;

f) izrada formulara za prijavu za upravljanje incidentima;

g) utvrditi postupke, pravila i standarde za korisnike u pogledu koraka koje treba slijediti prije, za vrijeme i nakon uočavanja sigurnosnog incidenta, formalizirati sve neophodne procedure oporavka;

h) odrediti, za svaku vrstu incidenta, koje je informacije potrebno evidentirati, vremenski okvir za podnošenje izvještaja, te izvještavanje o uvjetima zaštite, u skladu sa zahtjevima nadležnih tijela i zakonskih odredaba, kako bi se osiguralo da je informacija pogodna za korištenje u parničnom ili kaznenom postupku;

i) analizirati i reorganizirati prikupljene informacije u svrhu sastavljanja periodičnih izvještaja koji omogućavaju pregled stanja vezanog za incidente;

j) formalizirati, testirati i periodički pregledati plan upravljanja kriznim situacijama, u skladu s trenutnim regulatornim zahtjevima;

k) usvojiti odgovarajuće sigurnosne mjere koje jamče dostupnost podataka u slučaju njihova oštećenja ili kvara elektroničke opreme na kojoj se nalaze.

10.2.2. Učenje iz sigurnosnih incidenata

Sigurnosni incidenti moraju se analizirati kako bi se omogućilo prepoznavanje ponavljajućih ili relativno ozbiljnih incidenata i da bi se osigurala osnova za razvoj učinkovitih protumjera, koje se mogu sastojati i od organizacijskih i obrazovnih komponenata.

Smjernice:

a) analizirati i preispitati incidente koji se najčešće ponavljaju, kvantificirati ih prema vrsti, obujmu i utjecaju u svrhu planiranja odgovarajućih korektivnih mjera za poboljšanje preventivnih sposobnosti;
b) dopuniti programe izobrazbe s elementima rizika koji se najčešće ponavljaju i odgovarajućim radnjama koje trebaju poduzeti zaposlenici u svrhu sprečavanja i upravljanja sigurnosnim incidentima.

10.2.3. Prikupljanje dokaza

Dokazi se moraju prikupiti na način koji omogućava njihovo priznavanje na sudu i/ili u arbitražnom postupku.

Smjernice:

a) dodijeliti odgovornosti i propisati odgovarajuće aktivnosti kako bi se osiguralo prikupljanje i očuvanje dokaza, počevši od početne faze istrage i/ili parničenja;
b) korištenje računalne forenzike i ostalih tehnika, prikupljanje potpunih dokaza u prihvatljivom obliku koji se može predočiti na sudu i/ili arbitražnom postupku.

11. SIGURNOST U ODNOSU S UGOVORNIM PARTNERIMA

Upravljanje informacijskom sigurnošću zahtijeva jamstva za pravilno postupanje s informacijskom imovinom Tvrtke u odnosima s ugovornim partnerima u pogledu informacijske sigurnosti i poštivanja zakonskih odredaba.

Ugovorne odredbe koje se odnose na sigurnosna pitanja moraju se navesti u svakom uspostavljanju odnosa s ugovornim partnerima, a koji omogućavaju dotičnim ugovornim partnerima pristup informacijskom sustavu Tvrtke za potrebe izvršavanja ugovornih obveza.

11.1. Sigurnosni uvjeti u odnosima s ugovornim partnerima

U odnosima s ugovornim partnerima moraju se definirati i procijeniti rizici povezani s pristupom partnera informacijskom sustavu i imovini Tvrtke. Potrebno je sastaviti odgovarajuće odredbe ugovora koje se odnose na sigurnost, a nadležne službe u Tvrtki moraju ih ažurirati na osnovu potreba za pristupom ugovornih partnera i svih povezanih rizika.

11.1.1. Rizici povezani s informacijskim sustavom Tvrtke

Pristupanje ugovornih partnera bilo kojem dijelu informacijskog sustava Tvrtke mora se pomno procijeniti i isplanirati kako bi se osigurala povjerljivost, integritet i dostupnost.

Smjernice:

a) analiziranje potrebe ugovornog partnera za pristup informacijskom sustavu Tvrtke, odrediti razloga i utvrditi potrebne vrste pristupa (fizički, logički, mrežno povezivanje, ispisana dokumentacija, itd.), navedeno dokumentirati u procedurama;
b) provedba primjerenih analiza procjene rizika koji proizlaze iz pristupanja ugovornog partnera informacijskom sustavu Tvrtke kako bi se osigurala adekvatna razina sigurnosti kroz provedbu adekvatnih protumjera;
c) propisivanje posebnih sigurnosnih zahtjeva u odgovarajućim odredbama ugovora.

11.1.2. Sigurnosni zahtjevi u ugovorima s vanjskim izvršiteljima i ostalim trećim stranama

Pristup treće strane (dobavljača ili vanjskog izvršitelja) informacijskom sustavu i imovini bit će dozvoljen isključivo nakon što stranke izvrše i potpišu ugovor o uslugama ili sporazum o čuvanju tajni te nakon provedbe sigurnosnih mjera koje su propisane u ugovoru. Ugovore s vremena na vrijeme treba preispitati i ažurirati.

Smjernice:

a) sastaviti odgovarajuće ugovorne odredbe i zahtijevati poštivanje određenih tehničkih dodataka koji će osigurati da dobavljači i/ili vanjski izvršitelji provode propisane mjere za zaštitu informacijskog sustava Tvrtke;
b) osigurati da se u ugovore s trećim stranama uključe odgovarajuće odredbe te da ih s vremena na vrijeme preispita nadležni organizacijski dio, te da ih dostavljaju isključivo nadležni rukovoditelji tvrtki koji su zaduženi za takvu funkciju, i da su iste na pravilan način stavljene na raspolaganje . Nadalje, upućivati organizacijske dijelove koje rutinski sklapaju ugovore o uslugama s trećim stranama da koriste isključivo odredbe koje su sastavljene u Tvrtki i ažurirane, da među njima odaberu i prilagode ih potrebama u svakom pojedinom slučaju;
c) s vremena na vrijeme prekontrolirati izvršenje ugovornih obveza dobavljača i/ili vanjskih izvršitelja kao i poštivanje tehničkih specifikacija iz dodatka;
d) uspostava i usvajanje postupaka i procedura za povremenu kontrolu i reviziju ugovora s trećim stranama kako bi se osiguralo da su ogledni ugovori u svakom trenutku u skladu s vrhunskom razinom usluge.

11.2. Poštivanje zakona, propisa i sigurnosne politike Tvrtke

U slučajevima kada su razvoj, upravljanje ili nadzor cijelog ili dijela informacijskog sustava ili mreže Tvrtke povjereni ugovornim partnerima, potrebno je osigurati sukladnost sa zakonskim odredbama koje se odnose na sigurnost informacijskog sustava Tvrtke koja je povjerena ugovornim partnerima.

11.2.1. Poštivanje sigurnosnih propisa

Potrebno je osigurati da su usluge koje pružaju ugovorni partneri u skladu s važećim propisima o sigurnosti.

Potrebno je razviti postupke kontrole za provjeru poštivanja navedenih propisa.

Smjernice:

a) sastaviti i izvršiti ogledne ugovore koji od vanjskog izvršitelja zahtijevaju da usvoje i provode mjere za zaštitu i sigurnost informacija u skladu sa zakonskim odredbama, sigurnosnim propisima i sigurnosnom politikom Tvrtke, te osigurati ostvarivanje prava Tvrtke ili Nadzornog odbora da prekontrolira pridržava li se vanjski izvršitelj ugovornih odredaba o sigurnosti;
b) obavljanje posebnih kontrola u svrhu provjere poštivanja sigurnosnih propisa Tvrtke.

11.3. Razmjena informacija s trećim stranama

Potrebno je formalizirati odgovornosti, procese, alate i metode razmjene informacija s trećim stranama. Potrebno je provesti analizu i ocijeniti mogućnost korištenja mehanizama za prenošenje informacija koji garantiraju neporecivost.

11.3.1. Standardi i metodologija razmjene informacija

U oglednim ugovorima potrebno je odrediti parametre za razmjenu informacija i softvera s trećim stranama i pritom odrediti odgovornosti, procese i tehnike slanja, prijenosa i primanja informacija i softvera.

Smjernice:

a) sastaviti posebne ugovorne odredbe za postupanje s informacijama koje je objavila Tvrtka kako bi se osigurala povjerljivost, zaštita i uništenje informacija;
b) ugovor treba točno odrediti odgovornost u slučaju gubitka integriteta, povjerljivosti ili dostupnosti informacija ili softvera;
c) usuglasiti se o metodama prijenosa informacija i softvera;
d) ocijeniti u kojim je okolnostima i/ili slučajevima potrebno prenijeti informaciju izvan Tvrtke te odrediti primjerene mjere, koje se moraju ugraditi u ogledni ugovor, u svrhu zaštite povjerljivosti, integriteta i dostupnosti takvih informacija;
e) osigurati da se razmjenjivanje informacija i softvera odvija u skladu sa zakonskim, regulatornim i ugovornim odredbama o sigurnosti;
f) odrediti pravila za zaštitu imovine, softvera, datoteka ili dokumentacije Tvrtke ili treće strane koji su razmijenjeni s trećim stranama;

g) razmotriti mogućnost korištenja mehanizama za prenošenje informacija koji garantiraju neporecivost.

12. KONTROLE SIGURNOSTI I USKLAĐENOSTI

Za potrebe dugoročne učinkovitosti provedenih protumjera, treba ih redovito provjeravati kako bi se unaprijedile zaštitne mjere i utvrdili novi rizici ili kršenja pravila i postupaka.

Sve aktivnosti koje su povezane sa zaštitom informacija trebaju biti u skladu sa zakonskim i regulatornim odredbama o informacijskoj sigurnosti te s direktivama koje objave regulatorna tijela.

12.1. Sigurnosni pregledi

Potrebno je planirati nadzor u svrhu provjere sukladnosti dijelova informacijskog sustava s internom sigurnosnom politikom, a bilo kakvi slučajevi nesukladnosti moraju se utvrditi i zabilježiti. Alati korišteni za kontrolu sustava i aplikacija moraju biti zaštićeni i ne smiju ometati aktivnosti sustava i aplikacija koji se kontroliraju. Primjerenost provedenih zaštitnih mjera treba kontinuirano provjeravati.

12.1.1. Kontrole sukladnosti sigurnosnih pravila

Svi organizacijski dijelovi Tvrtke trebaju provesti povremene kontrole u svrhu osiguranja ili ponovne ocjene njihove sukladnosti s internim sigurnosnim pravilima.

Smjernice:

a) dodijeliti odgovornosti za različite faze unutarnjih kontrola;
b) vremenski isplanirati i izvršiti unutarnje kontrole o kojima se unaprijed treba usuglasiti sa svakim organizacijskim dijelom koji podliježe kontroli;
c) evidentirati rezultate kontrole i preispitati ih s rukovodstvom organizacijskih dijelova koji su prekontrolirani u svrhu određivanja primjerenih korektivnih radnji za ispravljanje svih slučajeva nesukladnosti;
d) povremeno vremenski isplanirati i izvršiti unutarnje kontrole u svrhu sprečavanja sigurnosnih rizika;
e) vremenski isplanirati i provesti, u dogovorenom roku, provjere korektivnih radnji koje su provedene u svrhu ispravljanja svih slučajeva nesukladnosti koji su navedeni u točki c).

12.1.2. Tehničke kontrole

S vremena na vrijeme moraju se prekontrolirati sustavi i aplikacije kako bi se provjerila primjerenost objavljenih sigurnosnih pravila i otkrile bilo kakve ranjivosti.

Smjernice:

a) odrediti i dodijeliti odgovornosti za provedbu sustava sigurnosnih kontrola u skladu s organizacijskim modelom Tvrtke, a u svrhu očuvanja pouzdanosti sustava;
b) provjeriti pravilnu primjenu pravila koja se odnose na ispravno korištenje informacijskog sustava Tvrtke od strane korisnika i ugovornih partnera;
c) osigurati da kontrole provode stručne osobe koristeći pritom standardizirane metode na unaprijed utvrđenoj povremenoj osnovi i pod nadzorom ovlaštenih zaposlenika.

12.1.3. Kontrole sustava, aplikacija i mreža

Kontrole sustava, aplikacija i mreža moraju se planirati u cilju smanjenja utjecaja na poslovanje.

Smjernice:

a) osigurati da su pristupna prava zaposlenika koje je nadležno za kontrolu sustava ograničena samo na ono što je izričito potrebno za obavljanje njihovih zadataka;
b) odrediti i osigurati dostupnost zaposlenika koje je potrebno za provedbu kontrola;
c) dokumentirati sve postupke provjere i zahtjeve prije provedbe kontrola;
d) pratiti i zabilježiti sva pristupanja sustavu za vrijeme kontrola;
e) osigurati da se kontrole provode na takav način da se minimizira utjecaj uobičajeno poslovanje Tvrtke;
f) odrediti posebne opsege analize koje će s vremena na vrijeme provjeriti i potvrditi neovisne treće strane.

12.2. Provjera sukladnosti

Potrebno je utvrditi, provjeriti i tijekom vremena osigurati sukladnost protumjera sa zakonskim i regulatornim odredbama. Sukladnost protumjera također treba odražavati

presude i/ili propise regulatornih tijela, te ostale izvore primjenjivih pravila koja se odnose na sigurnost informacija.

12.2.1 Važeći zakoni

Potrebno je utvrditi i dokumentirati zakonske i ugovorne uvjete i povezane obveze. Ti zahtjevi također trebaju biti u skladu sa zakonodavstvom u zemljama gdje Tvrtka namjerava poslovati ili gdje trenutačno posluje, kao i s međunarodnim propisima.

Smjernice:

a) osigurati da se sa svim informacijama i informacijskim sustavima Tvrtke postupa i da ih se koristi u skladu sa zakonskim, regulatornim i ugovornim odredbama koje se odnose na obradu i sigurnost informacija, te odrediti povezane kriterije upravljanja i odgovornosti;
b) redovito kontrolirati i ažurirati zakonske odredbe, prilagođavajući ih zakonodavnim okvirima države u kojoj ih treba primjenjivati.

12.2.2 Prava intelektualnog vlasništva

Potrebno je usvojiti neophodne mjere kako bi se osiguralo nekršenje prava intelektualnog vlasništva.

Smjernice:

a) razviti postupak kako bi se osiguralo da su softver i povezana korisnička dokumentacija nabavljeni izvan Tvrtke pokriveni valjanim dozvolama;

b) razviti standardna pravila koja reguliraju stvaranje intelektualnog vlasništva Tvrtke;
c) odrediti pravila za korisnike koja se odnose na zaštitu intelektualnog vlasništva i korištenje softvera;
d) utvrditi postupak kako bi se osiguralo da eksternalizacija softvera, savjetodavnih usluga ili ostalih usluga koje su zaštićene kao intelektualno vlasništvo ne može narušiti prava intelektualnog ili industrijskog vlasništva treće strane.

12.2.3 Zaštita i povjerljivost osobnih podataka

Potrebno je usvojiti adekvatne mjere za zaštitu osobnih podataka koji Tvrtka koristi.

Smjernice:

a) razviti specifične procese kako bi se osiguralo da se s informacijama i osobito s osobnih podacima postupa u skladu sa važećim zakonima i propisima;

b) provođenje, upravljanje i ažuriranje formalnih i strukturnih mjera u skladu sa zakonodavstvom koje se odnosi na zaštitu osobnih podataka, razvijanje namjenske organizacijske strukture kojoj će se povjeriti povezane odgovornosti;
c) sastavljanje popisa osobnih podataka, svrstanih prema vrsti (osjetljivi podaci, sudski podaci, itd.), neovisno o njihovu formatu ili uređajima za njihovu pohranu ili prijenos koji su korišteni za njihovu obradu;
d) obrada osobnih podataka na zakonit i pravilan način, njihovo prikupljanje i bilježenje isključivo za navedene potrebe, te sa se ne koriste u bilo koju drugu svrhu osim one, ili da ne premašuju onu svrhu, zbog koje su izvorno prikupljeni;
e) obavijestiti subjekt podataka (pojedinca ili korporaciju) o metodologijama i svrsi obrade osobnih podataka;
f) pribaviti, kada je to propisano zakonom, pristanak subjekta podataka za obradu njegovih osobnih podataka;
g) pohrana i upravljanje osobnim podacima koje koristi Tvrtka na način da se na najmanju moguću mjeru svedu rizici namjernog ili slučajnog gubitka, promjene ili uništavanja, ili neovlaštena pristupa;
h) razvoj programa izobrazbe, za zaposlenike, koji osiguravaju specifične upute za obradu osobnih podataka u skladu s primjenjivim zakonima i propisima;
i) organizirati i pohranjivati datoteke s osobnim podacima na način koji omogućava subjektu podataka da dobije informacije o tome koji su podaci prikupljeni i zabilježeni, da prekontrolira podatke i zatraži ispravak, dodavanje, brisanje, ili da odbije dati dozvolu za korištenje osobnih podataka;
j) upravljati osobnim podacima na način da njihova obrada od strane Tvrtke bude u skladu sa zakonskim aktima vezanim za čuvanje osobnih podataka;
k) u slučaju bilo kakvog saznanja o neovlaštenom pristupu osobnim podacima, o navedenome je potrebno obavijestiti organizacijski dio / službu zaduženu za zaštitu osobnih podataka;
l) organizacijski dio / služba zadužena za zaštitu osobnih podataka, u slučajevima povrede zaštite osobnih podataka koja je rezultirala uništenjem, gubitkom, promjenom ili neovlaštenim razotkrivanjem osobnih podataka, nadzire komunikaciju s državnom agencijom zaduženom za zaštitu osobnih podataka, Nadzor u ovom smislu

podrazumijeva provjeru kvalitete i kvantitete poslanih podataka te broja klijenata zahvaćenih povredom zaštite osobnih podataka.

12.2.4 Regulacija kriptografskih kontrola

Moraju se usvojiti potrebne mjere u svrhu postizanja sukladnosti sa važećim zakonima i/ili propisima.

Smjernice:

a) provjeriti sve zakonske odredbe, ako postoje, koje reguliraju korištenje enkripcije podataka;

b) osigurati sukladnost sa svim zakonima ili propisima koji se odnose na korištenje kriptografskih tehnika.

13. SIGURNOSNE SMJERNICE ZA DJELATNIKE

Učinkovitost sigurnosnih mjera ovisi o stvaranju „kulture sigurnosti“. To je moguće postići razvijanjem odgovarajuće svijesti i programa izobrazbe, kao i razvijanjem adekvatnih pravila koja će usmjeravati djelatnike da na pravilan način upravljaju informacijama u obavljanju svakodnevnih poslovnih aktivnosti.

13.1. Pravila za djelatnike

Treba razvijati pravila koja djelatnicima nameću odgovorno korištenje prava pristupa, bez obzira na to radi li se o djelatnicima Tvrtke ili djelatnicima ugovornih partnera. Informacijska oprema i pomoćni uređaji (faks uređaji, fotokopirni aparati, telefoni, oprema za videokonferencije, itd.) koji su na raspolaganju djelatnicima također trebaju biti zaštićeni kroz adekvatnu skupinu pravila koja reguliraju njihovo korištenje, čuvanje i zaštitu, posebice kada su bez nadzora.

13.1.1. Korištenje korisničkih računa

Kod korisnika treba razviti svijest i osigurati im izobrazbu o utvrđivanju, korištenju i upravljanju korisničkih računa.

Smjernice:

a) utvrditi pravila za djelatnike kako bi se osiguralo da su djelatnici, nakon što dobiju svoje korisničke račune, upoznati s time da je korisnički račun izričito osoban te da se ne smije otkrivati bilo kome drugome, čak ni za izdvojene aktivnosti ili na kraće vremensko razdoblje;
b) utvrditi pravila za djelatnike za potrebe stvaranja, korištenja i upravljanja povjerljivom komponentom korisničkog računa (npr. zaporka, PIN itd.) ;
c) utvrditi pravila za djelatnike za korištenje i upravljanje uređajima za autentikaciju koje posjeduje i koristi isključivo pojedini djelatnik.(npr. token, pametna kartica itd.)

13.1.2 Korištenje informacijskog sustava i imovine Tvrtke

Potrebno je definirati pravila za djelatnike u svrhu ispravna korištenja informacijskog sustava i informacijske imovine kako bi se osigurala zaštita informacija koje su u njima sadržane kao i informacijske imovine Tvrtke općenito.

Smjernice:

a) propisati pravila za djelatnike za upravljanje elektroničkim i ispisanim dokumentima u skladu s razinom klasifikacije informacija koje su u njima sadržane, izbjegavajući pritom nepotrebno umnožavanje predmetnih dokumenata;
b) propisati pravila za korisnike u svrhu pravilna korištenja informacijske imovine Tvrtke kako bi se zaštitile informacije koje su u njoj sadržane;
c) propisati pravila za korisnike koja zabranjuju korištenje bilo koje opreme za postupanje ili obradu informacija Tvrtke osim one koju je Tvrtka dodijelila djelatniku, osim ako nije posebno odobreno drukčije, te koja zabranjuju svaki drugi način povezivanja s informacijskim sustavom Tvrtke osim onoga koji je izričito odobren;
d) propisati pravila za fizičku i logičku zaštitu i čuvanje alata, opreme i informacijske imovine kada se isti koriste izvan prostorija Tvrtke. Ta bi pravila u pogledu ograničenja trebala biti barem jednaka onima koja se primjenjuju na interno korištenje i moraju uzeti u obzir specifične rizike koji su povezani s korištenjem izvan Tvrtke;
e) propisati pravila za djelatnike koja se odnose na upravljanje pokretnim medijima za pohranu podataka koji su na raspolaganju djelatniku;
f) propisati odgovarajuća pravila za djelatnike koja se odnose na sprečavanje malicioznih kodova i zaštitne mjere;
g) propisati pravila za djelatnike koja se odnose na korištenje elektroničke pošte i interneta. Ta pravila moraju izričito navesti povezane rizike;
h) propisati pravila za djelatnike za provjeru pouzdanosti, vjerodostojnosti i integriteta informacija koje dolaze izvan Tvrtke, a zaprimaju se telefonom, pomoću faks uređaja ili elektroničke pošte, ili u ispisanom obliku;
i) propisati pravila za djelatnike u svrhu zaštite integriteta i povjerljivosti verbalno razmijenjenih informacija (razgovor licem u lice, telefonom, za vrijeme videokonferencije, itd.);
j) propisati pravila za korištenje i plasman dijeljenih vizualnih ili verbalnih komunikacijskih sustava (npr. videokonferencijski sustav) u svrhu zaštite integriteta i povjerljivosti razmijenjenih informacija;
k) propisati pravila za djelatnike za upravljanje dijeljenim (razmijenjenim) softverom, datotekama i dokumentacijom kako bi se osigurala pravilna briga i pravilno čuvanje vlasništva Tvrtke ili ugovornog partnera;
l) obavijestiti djelatnike Tvrtke i ugovorne partnere o utvrđenim pravilima i postupcima za njihovu provedbu.

13.1.3 Pravila za upravljanje dokumentacijom ("politika čistog stola") i osobnim računalima ("politika praznog zaslona")

Potrebno je objaviti pravila za korisnike u cilju promicanja svijesti o važnosti informacija s kojima se postupa te o povezanim rizicima.

Smjernice:

a) utvrditi pravila za upravljanje dokumentacijom na radnim mjestima („politika čistog stola“);

b) utvrditi metode upravljanja osobnim računalima koja nisu pod nadzorom korištenjem logičkih („politika praznog zaslona“) i fizičkih mehanizama.

14. DODATAK

14.1. Objašnjenje pojmova

Ovaj rječnik objašnjava osnovne pojmove koji su korišteni u ovom dokumentu, a koji zahtijevaju nedvosmislenu definiciju. Navedene definicije temelje se na sljedećim izvorima:

- hrvatskom zakonodavstvu
- ISO/IEC (Međunarodna organizacija za normizaciju)
- ENISA (Europska organizacija za sigurnost mreža i podataka)
- NIST (Nacionalni institut za norme i tehnologiju)

POJAM	DEFINICIJA
Analiza rizika	Aktivnosti u svrhu utvrđivanja prirode i izvora rizika, s njime povezanih ranjivih točaka i posljedica, te usvojenih protumjera, a u cilju objektivne procjene razine rizika.
Analiza utjecaja na poslovanje	Element upravljanja kontinuitetom poslovanja. Proces utvrđivanja i analiziranja ekonomskih, regulatornih i reputacijskih i operativnih posljedica prekida poslovnih procesa.
Anti virus	Softver čija je namjena traženje, utvrđivanje i uklanjanje malicioznog programskog koda unutar informacijskog sustava.
Aplikacije	Softverski programi koji podržavaju funkcionalnosti koje su neophodne korisniku ili drugom softverskom programu za obavljanje aktivnosti s informacijama.
Autorizacija	Postupak dodjele, ili automatske provjere, dozvole nekog subjekta (računala, aplikacije ili osobe) da pristupi zatraženoj informaciji nakon što je subjekt potvrđen.
Autentikacija	Vidi "Potvrđivanje"
Digitalni certifikat	Elektronički dokument koji u sebi sadržava digitalni potpis i povezuje javni ključ s identitetom osobe ili organizacije. Može se koristiti za provjeru da javni ključ doista pripada osobi. Izdaje ga davatelj usluga certificiranja, tijelo koje je priznato u skladu s međunarodnim normama (X.509), a potpisuje se privatnim ključem davatelja usluga certificiranja.

Digitalni potpis	Sustav asimetrične kriptografije koji imitira sigurnosne značajke rukom pisanog potpisa, a koristi se kao sustav potvrđivanja digitalnih dokumenta.
Djelatnici	Vidi "Zaposlenici"
Dostupnost	Stanje dostupnosti i iskoristivosti na zahtjev autorizirana subjekta.
Dostupnost informacija	Uvjet informacijske sigurnosti temeljem kojega informacija mora biti dostupna i upotrebljiva samo ovlaštenim subjektima u skladu s pravilima o vremenskim okvirima i metodama.
Elektronička trgovina	Transakcije koje se obavljaju elektronički (na primjer, Internet bankarstvo).
Elektronička pošta	Usluga slanja elektroničkih poruka i sadržaja u različitim formatima.
Evidencija	Kronološka evidencija događaja koju generiraju sustavi, aplikacije i mreže, i operacija koje su u sustavima, aplikacijama i mrežama obavili korisnici.
Filtriranje datoteka	Korištenje softverskih filtara za praćenje i/ili blokiranje slanja datoteka.
Filtriranje sadržaja	Operacija koju izvodi softver (proxy agent) u svrhu uklanjanja ili stavljanja u karantenu virusa ili neželjenog sadržaja općenito tijekom korištenja interneta te slanja i primanja elektroničke pošte.
Forenzička analiza	Analitičke i istražne tehnike koje se koriste za sustavnu kontrolu računalnih sustava i njihovih sadržaja u svrhu određivanja, prikupljanja, ispitivanja i očuvanja dokaza o kaznenom djelu ili drugom nepropisnom korištenju sustava.
Identifikacija	Proces prepoznavanja subjekta (računala, aplikacije ili osobe) putem provjere predočenog korisničkog imena.
Imovina	Sve što ima vrijednost za organizaciju.
Informacija	Skup podataka koji su ustrojeni u posebnom obliku i imaju određeno značenje.
Informacijska imovina	Sastavni element informacijske imovine Tvrtke. Informacijska imovina uključuje podatke, informacije, instrumente, infrastrukturu, medije za pohranu podataka i sve procese koji su uključeni u obradu informacija.
Informacijska imovina Tvrtke	Ukupnost podataka, informacija i ostale informacijske imovine koji pripadaju ili njima upravlja Tvrtka. Ovi podaci, informacije i ostala informacijska imovina mogu biti materijalni ili nematerijalni, organizirani ili neorganizirani, i obrađeni pomoću ili bez pomoći elektroničkih instrumenata.

Informacijska sigurnost	Disciplina koja se bavi očuvanjem temeljnih značajki informacijske imovine – povjerljivosti, integriteta i dostupnosti. Također može obuhvaćati i druge značajke kao što su autentičnost, odgovornost, nemogućnost nijekanja i pouzdanost.
Informacijski sustav	Skup informacijskih izvora (procesa, sustava, tehnološke infrastrukture, podataka) ustrojen tako da omogućava prikupljanje, rukovanje, pohranjivanje i korištenje informacija (ili, općenito, obradu informacija).
Informatička oprema	Tehnološka oprema (hardver, mediji za pohranu podataka, mrežna oprema itd.) koji se koriste za upravljanje informacijskom imovinom Tvrtke.
Integritet	Značajka očuvanja točnosti i potpunosti informacijske imovine i metoda obrade.
Integritet informacija	Element informacijske sigurnosti koji osigurava da je informacija u svakom trenutku potpuna, točna i vjerodostojna.
ISO 17799:2005	Pravilnik o postupanju za sustave upravljanja informacijskom sigurnošću.
ISO 27001:2005	Međunarodni standard koji propisuje zahtjeve za sustav upravljanja informacijskom sigurnošću (Information Security Management System - ISMS).
ISO 27002:2005	Ažurirana norma ISO 17799:2005, na snagu stupila 1. srpnja 2007.
Izmjenjivi mediji za pohranu podataka	Sustavi za pohranu podataka koji se s lakoćom mogu odstraniti iz računala (disketa, CD, DVD, flash kartice, USB diskovi, dlanovnici (PDA), itd.).
Izrada sigurnosnih kopija	Operacija izrade kopija informacija, programa ili operativnih sustava kako bi se osiguravala mogućnost njihova oporavka.
Izvorni kod	Niz naredaba koje su zapisane na bilo kojem programskom jeziku koji je razumljiv ljudima i koristi se za stvaranje računalnih programa.
Izvršni kod	Slijed računalnih naredaba koje su spremne za izvršenje u stvarnim (npr. strojni kod) ili virtualnim (npr. prevedeni kodovi) sustavima.
Javni ključ / privatni ključ	Matematičko korelirane numeričke komponente asimetričnog sustava šifriranja.
Klijent	Računalni sustavi koji pristupaju udaljenim uslugama u drugom računalu (koji se uobičajeno naziva server – poslužitelj) kroz bilo koju vrstu mreže. Klijenti i serveri mogu biti softverske ili hardverske komponente.

Ključ	Dio informacije koji kontrolira operaciju algoritma za enkripciju. U kriptiranju, ključ određuje pretvaranje običnog teksta u kriptirani tekst, ili obrnuto u slučaju dekripcije.
Kontinuitet poslovanja	Značajka poslovanja društva koja je osigurana kroz skup preventivnih i korektivnih tehnoloških i organizacijskih mjera kojima je cilj smanjiti rizike od prekida u poslovanju na prihvatljivu razinu.
Korektivne preinake	Preinaka u svrhu uklanjanja grešaka koje su uočene u funkcioniranju usluge.
Korisničko ime	Element korisničkog računa za pristup informacijama u informacijskom sustavu. Omogućava nedvojbenu identifikaciju subjekta (računala, aplikacije ili osobe).
Korisnički račun	Korisnička identifikacija s povezanim profilom za pristup informacijama. Podaci i uređaji koje posjeduje, s kojima je upoznata i koji su nedvojbeno povezani s osobom i koriste se za informatičko potvrđivanje. Mogu se sastojati od korisničkog imena i povjerljive komponente koja može biti kombinacija jedne ili više značajki u obliku: • nečega što je poznato korisniku (npr. zaporka); • nečega što korisnik posjeduje (npr. pametna kartica, token); • nekog obilježja korisnika (npr. otisak prsta, uzorak šarenice oka).
Korisnik	Osoblje, treće strane ili subjekti (uključujući računala i aplikacije) koji koriste bilo koji dio informacijske imovine Tvrtke, osim aktivnih ili potencijalnih klijenata.
Kriptiranje	Proces u kojemu se informacije pomoću algoritama i ključeva pretvaraju na način da su nečitljive neovlaštenim osobama.
Kriptografija	Dolazi od grčke riječi kryptós (tajna, skriven) i graphéin (pisati): znanost o metodama „zamagljivanja“ sadržaja neke poruke kako bi isti bio nerazumljiv svima koji nisu ovlašteni da pročitaju njezin sadržaj.
Kritični podaci	Podaci se smatraju kritičnima ako njihov gubitak ili narušavanje njihove povjerljivosti, integriteta ili dostupnosti može nanijeti: • štetu ugledu; • gospodarske ili financijske gubitke; • dovesti u konkurentski nepovoljan položaj (gubitak posla ili poslovnih prilika);

	• uzrokovati pravne posljedice; • cjelokupan ili djelomičan prekid poslovnih procesa.
Kriza	Situacija u kojoj se, slijedom izvješća o sigurnosnom incidentu, poduzimaju radnje u svrhu zaštite imovine i usluga kroz analizu i ograničavanje štete, uklanjanje uzroka i obnavljanje svih ugroženih sustava ili podataka.
Maliciozni kod	Bilo koji softver koji je stvoren s namjerom nanošenja izravne ili neizravne štete sustavima u kojima se pokrene (virusi, crvi, „trojanski konji“, špijunski programi, dialeri, keyloggeri, rootkit programi, itd.).
Mediji za pohranu podataka	Promjenjivi ili ugrađeni uređaji na kojim se mogu pohranjivati informacije.
Mjera	Zaštitna ili sigurnosna mjera. Vidi „Protumjera“.
Mreža	Računalna mreža je sustav koji omogućava razmjenu informacija i izvora (hardver i softver) između različitih računala. Sustav pruža uslugu prijenosa informacija korisnicima koji mogu biti na jednom ili više mjesta.
Mrežna oprema	Oprema koja služi za upravljanje slanja i primanja (prenošenja) podataka (npr. preklopnici, usmjernici (ruteri), vatrozidi).
Načela sigurnosti	Načela koja opisuju sigurnosno okruženje, ciljeve i opća načela koja Tvrtka usvaja u svrhu zaštite informacijske imovine Tvrtke.
Najmanje pravo	Načelo prema kojemu je svakom subjektu u sustavu odobren najrestriktivniji mogući skup pristupnih prava koji subjektu omogućava ispunjavanje legitimne zadaće.
Neporecivost	Jamstvo da subjekti koji su uključeni u proces komunikacije ne mogu zanijekati da su sudjelovali u razmjeni. Konkretno, može garantirati nemogućnost pošiljatelja da porekne da je poslao poruku, a primatelj ne može zanijekati da je poruku primio.
Obrada podatka	Svaka operacija ili skup operacija koje se obavljaju uz podršku ili bez podrške elektroničkih uređaja a uključuju prikupljanje, evidentiranje, organiziranje, pohranjivanje, konzultiranje, obradu, preinake, odabir, izlučivanje, uspoređivanje, korištenje, međusobno povezivanje, sprečavanje, prenošenje, širenje ili distribuiranje podataka, čak i ako isti nisu zabilježeni u bazi podataka.
Oporavak nakon katastrofe	Organizacijsko i tehnološko rješenje u svrhu oporavka IT i poslovnih usluga te poslovanja na alternativnoj lokaciji, a nakon događaja koji su doveli do duljih prekida.

Osjetljivi podaci	Osobni podaci koji otkrivaju rasnu ili etničku pripadnost, vjerska, filozofska i druga uvjerenja, političko opredjeljenje, članstvo u političkoj stranci, sindikatu, udruzi ili vjerskoj, filozofskoj, političkoj ili sindikalnoj organizaciji, kao i osobni podaci koji otkrivaju zdravstveno stanje ili seksualni život.
Osobni podaci	Svaka informacija o fizičkoj osobi, pravnoj osobi, subjektu ili udruženju koje je identificirano ili može biti identificirano, čak i neizravno, putem reference na bilo koju drugu informaciju, uključujući osobni identifikacijski broj.
Planiranje kapaciteta	Proces u kojem se izračunavaju kapaciteti sustava te se planiraju neophodne promjene kako bi se ispunili zahtjevi koji se mijenjanju ili su predviđeni, te kako bi se osigurao dostatan kapacitet sustava u svrhu izbjegavanja kvarova zbog preopterećenja.
Podaci suda	Osobni podaci koji mogu otkriti kaznenu evidenciju, upravne sankcije za kaznena djela i povezane neriješene optužbe, ili status osumnjičenika ili okrivljenika prema kaznenom zakonu.
Podatak	Svaka činjenica ili stanje koje se može evidentirati, prenijeti ili obraditi, čak i ako samo po sebi nema nikakvo značenje.
Politika čistog stola	Politika organizacije koja upućuje sve zaposlenike da na kraju svakog radnog dana urede svoje radne stolove.
Politika praznog zaslona	Politika organizacije koja upućuje sve korisnike zaslona/terminala da osiguraju da je sadržaj na ekranu zaštićen od radoznalih pogleda i oportunističkog kršenja povjerljivosti. Najlakši je način pridržavanja aktivacija zaštitnika zaslona koji se aktivira ili na zahtjev ili nakon unaprijed određena vremena.
Pomoćna oprema	Oprema čija je svrha osigurati pravilno funkcioniranje i visoku pouzdanost informacijskih sustava.
Pomoćni sustavi	Uslužni sustavi koji su podrška informacijskim sustavima: struja, klimatizacija, itd.
Posebne privilegije	Privilegije za pristup sustavima i informacijama dodijeljene tehničkim ili administrativnim profilima, a koje se ne vezuju uz običnu radnu ulogu djelatnika.
Poslovanje	Skup aktivnosti i procesa čija je svrha osigurati pravilno pružanje planiranih usluga.
Potvrđivanje	Postupak u kojem se podaci koje pruži identificirani subjekt (računalo, aplikacija ili osoba) uspoređuju s oni podacima koji su memorirani u

	sustavu kako bi se osiguralo da je navedeni subjekt u stvarnosti taj ili to za koga ili za što se predstavlja.
Povjerljiva komponenta	Vidi "Korisnički račun".
Povjerljivost informacija	Značajka na temelju koje informacijska imovina nije dostupna ili se ne daje na uvid osobama, subjektima ili procesima koji nisu autorizirani za pristup navedenoj imovini.
Prava pristupa	Autorizacija za obavljanje radnji na informacijskoj imovini kao što su čitanje, pisanje, izvršenje, uređivanje, brisanje ili stvaranje.
Pravila	Dovoljno uopćene upute i formalizirana pravila koja propisuju relativno stabilna ponašanja i discipliniraju tehničke aspekte određena područja. To mogu biti zakonske norme, pravilnici poduzeća i norme koje se odnose na domaće i međunarodne standarde.
Pravila rada	Dokumenti koji uključuju operativne upute za primjenu protumjera koje se navode u sigurnosnim smjernicama.
Promjena u sklopu održavanja	Promjena koja služi unaprjeđenju pružanja ili kvalitete usluga.
Promjena u svrhu prilagodbe	Promjena u svrhu prilagodbe usluge kako bi se ispunile nove interne ili zakonske norme ili novi zahtjevi klijenata.
Prihvatljiv rizik	Rizik koji Tvrtka smatra prihvatljivim.
Prijava (Log-in / Logon)	Postupak za pristupanje sustavu ili aplikaciji.
Prijetnja	Svaka okolnost ili događaj koji potencijalno može nanijeti štetu organizaciji, poslovanju, informacijskoj imovini ili osobama.
Pristupanje	Operacija koja omogućava korisniku da pregledava ili izmijeni informacijsku imovinu.
Pristupni korisnički profil	Pristupna prava korisnika da pristupi izvorima Tvrtke.
Privatnost	Pravo na povjerljivost nečijih osobnih informacija i privatnog života.
Procedura	Slijed radnji u svrhu postizanja određenog cilja.
Produkcijska okolina	Infrastruktura, hardver, softver i procesi koji osiguravaju okruženje za produkcijske aktivnosti.
Protumjera	Metoda upravljanja rizikom. Može uključivati politike, procedure, smjernice, prakse i organizacijske strukture koje mogu biti administrativne, tehničke, upravljačke ili pravne prirode.
Provjera	Skup aktivnosti i postupaka kojima je svrha osigurati da razvijene aplikacije, sustavi ili infrastruktura udovoljavaju zahtjevima za koje su

	izrađeni, da pravilno funkcioniraju te da mogu biti preneseni u radnu okolinu i pušteni u rad.
Radno okruženje	Infrastruktura, hardver, softver, i procesi koji osiguravaju okruženje za rad aplikacija, sustava i mreža u svrhu pružanja usluga.
Ranjivost	Svojstvena slabost koja se može iskoristiti za nanošenje štete informacijskoj imovini.
Razdvajanje odgovornosti	Osnovna kontrola koja sprečava ili detektira greške i nepravilnosti, i osigurava da se odgovornosti za aktivnosti instaliranja, rukovanja, praćenja događaja i čuvanja informacijske imovine razdvoje i dodijele različitim pojedincima.
Razvoj	Aktivnosti koje dovode do stvaranja ili izgradnje sustava, aplikacija ili infrastrukture.
Razvojne promjene	Promjene u svrhu dodavanja novih funkcionalnosti usluzi ili unaprjeđenja postojećih funkcionalnosti.
Razvojna okolina	Infrastruktura, hardver, softver i procesi koji osiguravaju okruženje za razvojne aktivnosti.
Regulatorno tijelo	Institucija koja ima ovlasti za praćenje i kontrolu aktivnosti Tvrtke.
Revizija	Neovisna kontrola aktivnosti i dokumentacije u svrhu provjere poštivanja pravila te davanje preporuka za postizanje navedena poštivanja u slučajevima gdje nedostaje.
Rizik	Kombinacija vjerojatnosti da će se neki događaj dogoditi i posljedice tog događaja.
Semantička provjera	Potvrda da podaci imaju ispravno značenje.
Server(poslužitelj)	Sastavni dio informacijske mreže koji pruža usluge ostalim komponentama (koji se obično nazivaju „klijentima“). Pojmovi „server“ i „klijent“ odnose se i na hardverske i softverske komponente.
Sesija	Aktivna veza između dvije logičke jedinice (u načelu mrežnih servera ili aplikacija) koja traje neko određeno vrijeme.
Sigurno područje	Određeno područje unutar sigurnosnog perimetra koje zahtijeva dodatne kontrole u svrhu zaštite subjekata, podataka ili izvora koji su u njemu sadržani.
Sigurnosna politika	Vidi „Načela sigurnosti“.
Sigurnosna provjera	Provjera pravilne primjene sigurnosnih pravila Tvrtke i učinkovitosti mjera.

Sigurnosne smjernice	Skup kontrola i mjera, u skladu s utvrđenim sigurnosnim standardima, za smanjenje rizika i pojašnjenje što je potrebno napraviti u području informacijske sigurnosti da bi se ostvarili ciljevi koji su navedeni u Načelima sigurnosti koje je Tvrtka usvojila.
Sigurnosni događaj	Utvrđen događaj u statusu sustava, usluge ili mreže koji upućuje na moguće kršenje politike informacijske sigurnosti, neuspjeh protumjera, ili u potpunosti nova situacija koja može utjecati na sigurnost.
Sigurnosni incident	Neželjeni i neočekivani događaji ili serija događaja za koje postoji velika vjerojatnost da će ugroziti institucionalne ili poslovne aktivnosti i koje prijete informacijskoj sigurnosti ugrožavajući povjerljivost, integritet ili dostupnost informacija.
Sigurnosni kod	Kod razvijen kroz primjenu pravila koja na najmanju mjeru svode ranjivost aplikacija ili operativnih sustava na poznate prijetnje.
Sigurnosni zahtjevi	Zaštitne mjere koje štite izvor od rizika informacijske sigurnosti.
Sintaktička provjera	Potvrđivanje ispravne strukture podataka.
Sistemska važnost	Za sve izrazito važne procese u informacijskom sustavu kaže da su od „sistemske važnosti“.
Standard	Dokumentirani sporazum koji sadrži tehničke specifikacije ili ostale kriterije koji se moraju dosljedno primjenjivati, kao što su pravila, smjernice ili definicije značajki, u svrhu osiguranja da su materijali, proizvodi, procesi ili usluge primjerene njihovoj svrsi i ciljevima. Standardi pomažu u pojednostavljenu problema i unaprjeđenju pouzdanosti i učinkovitost dobara i usluga koje koristimo. (Na osnovu definicije ISO-a)
Sustav	Integrirana skupina komponenti hardvera za obradu, pohranjivanje i razmjenu informacija.
Sustav upravljanja informacijskom sigurnošću	Skup procesa, odgovornosti i pravila koji predstavljaju sastavni dio cjelokupna sustava upravljanja i čiji je cilj osigurati sigurnost informacijske imovine i poslovanja Tvrtke, te pravnih i ugovornih obveza.
Testna okolina	Infrastruktura, hardver, softver i procesi koji osiguravaju okruženje za testne aktivnosti.
Treće strane	Druge osobe ili subjekti osim osoblja ili klijenata društva.
Udaljeni pristup	Pristup informacijskim sustavima putem udaljenih veza.

Udaljeno povezivanje	Povezivanje, u načelu preko računala, komunikacijske linije i namjenskog softvera na mrežu Tvrtke s lokacije koja je izvan mreže Tvrtke.
Udaljeni rad	Korištenje telekomunikacija za rad od kuće ili s drugog mjesta umjesto u prostorijama Tvrtke.
Ugovorni partner	Društvo s kojim se sklapa ugovor u svrhu obavljanja zadaće ili neke faze u proizvodnom procesu.
Unutarnje mreže	Mreže koje nužno podliježu zahtjevima sigurnosti u okviru sigurnosnih pravila Tvrtke.
Upravljanje rizikom	Proces osmišljavanja i provedbe potrebnih protumjera za suzbijanje rizika na temelju ciljeva Tvrtke.
Usluge mreže	Skup funkcija koje su na raspolaganju mreži Tvrtke, isključujući aplikacije, koje zaposlenicima omogućavaju pristup i upravljanje informacijama.
Vanjske mreže	Sve ne-unutarnje mreže (vidi „Unutarnje mreže“). Vanjske mreže ne podliježu sigurnosnim zahtjevima koji su sadržani u sigurnosnim pravilima Tvrtke.
Veza	Fizička ili logička veza između dvaju ili više elektroničkih uređaja.
Virus	Program koji ima mogućnost kopiranja samog sebe, općenito zlonamjeran. Virusi se šire preko nekog "domaćina", izvršnih datoteka, ovisno o vrsti mogu zaraziti svaki dio informacijskog sustava.
Wireless Access Point (bežična pristupna točka)	Uređaj koji omogućava korisnicima mobilnih uređaja da se spoje na bežičnu mrežu. Pristupna točka, koja je fizički spojena na žičnu mrežu (ili preko druge pristupne točke), odašilje radio signale od korisnika ili ih prima prema korisniku i na taj način uspostavlja vezu.
Zaporka	Slijed znakova koji se koristi za jedinstveno pristupanje informacijskom sustavu. To je jedna od mogućih povjerljivih komponenti pristupnih isprava.
Zaposlenici	Ljudi koji su u ugovornom odnosu s Tvrtkom.