те критерији за одређивање прихватљивости, односно неприхватљивости нивоа ризика.

ЗАКЉУЧАК

Усвајањем Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине, створиће се правни основ за усвајање међународних стандарда из серије ISO/IEC 27000, закона и подзаконских аката о мјерама у овој области, стандарда за поједине области, те програма информационе безбједности у Босни и Херцеговини. Такође, у циљу потпуног уређења ове области потребно је измијенити законе којим је уређена: електронска трговина, електронски потпис, електронски документ и архивско пословање. Поштујући препоруке и најбољу праксу, засновану на међународним стандардима приликом израде наведених прописа, ствара се информационо-комуникациона платформа неопходна за сарадњу са свим релевантним факторима из окружења, у првом реду са ЕУ и НАТО. Сарадња базирана на повјерењу које је нормирано и реализовано у свим сегментима информационог друштва има перспективу континуираног развоја и добробити и за грађане и за државу. Чињеница да управљање информационом безбједношћу, као дио укупне националне безбједности, све више добија на значају намеће потребу њеног даљег развоја, како у теоријском, тако и у практичном смислу. У Босни и Херцеговини не постоји довољно развијена свијест о управљању информационом безбједношћу, као ни организована редовна едукација било којег нивоа. Подизање свијести о потреби и неопходности увођења система управљања информационом безбједношћу, као и њено изучавање кроз систем редовног високошколског образовања има важну улогу у даљем развоју информационог друштва. С обзиром на комплексност, вишеслојност и интердисциплинарност, обученост у сфери управљања информационом безбједношћу подразумијева одређени фонд техничких, управљачких и специјалистичких знања. Са сваким новим достигнућем у области информационих технологија јављају се нови аспекти информационе безбједности, што мора бити пропраћено научно истраживачким радом.

Ова политика управљања информационом безбједношћу у себи садржи и едукативну компоненту. На тај начин се хтјело указати да свака институција мора схватити неопходност и потребу реализовања сопствене политике и увођењем система за управљање информационом безбједношћу. Да би се те политике могле реализовати, неопходно је, паралелно са нормативним уређивањем ове области, радити на програмима који ће у наредном периоду подићи укупну свијест и креирати неопходну кадровску и научну инфраструктуру. Планирањем мјера и активности, организовањем стручних дебата, системском промоцијом нових технологија и метода информационе безбједности, као и ажурирањем прописа, обезбиједиће се услови за брзо и квалитетно прикључење БиХ развијеном свијету, а тиме и услови за побољшање укупног квалитета живота.

Na osnovu člana 10. Zakona o ministarstvima i drugim organima uprave Bosne i Hercegovine ("Službeni glasnik BiH", br. 5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09, 103/09, 87/12 i 61/13) i člana 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08), Vijeće ministara Bosne i Hercegovine, na 95. sjednici, održanoj 22. marta 2017. godine, donijelo je

ODLUKU
O USVAJANJU POLITIKE UPRAVLJANJA INFORMACIONOM SIGURNOŠĆU U INSTITUCIJAMA BOSNE I HERCEGOVINE, ZA PERIOD 2017 - 2022. GODINE

Član 1.
(Predmet Odluke)

Ovom Odlukom usvaja se Politika upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017-2022. godine (u daljem tekstu: Politika) koja je u prilogu ove Odluke i čini njen sastavni dio.

Član 2.
(Podnošenje izvještaja)

Zadužuje se Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine da Vijeću ministara Bosne i Hercegovine podnose godišnji izvještaj o realiziranju Politike.

Član 3.
(Stupanje na snagu)

Ova Odluka stupa na snagu narednog dana od dana objavljivanja u "Službenom glasniku BiH".

VM broj 83/17
22. marta 2017. godine
Sarajevo

Predsjedavajući
Vijeća ministara BiH
Dr. **Denis Zvizdić**, s. r.

Prilog

POLITIKA UPRAVLJANJA INFORMACIONOM SIGURNOŠĆU U INSTITUCIJAMA BOSNE I HERCEGOVINE, ZA PERIOD 2017 - 2022. GODINE

UVOD

Uspostavljanje i razvoj sistema informacione sigurnosti u svim segmentima jedne države predstavlja važnu pretpostavku za stvaranje informacionog društva. Stvaranje informacionog društva, posmatrano u širem smislu, predstavlja ne samo uvjet za uključivanje određene države u međunarodne integracione procese, već i način za opstanak te države u društvu razvijenih. Osnovni subjekti informacionog društva su državna uprava, privredni subjekti i stanovništvo, dok osnovu njegovog razvoja predstavlja povjerenje tih subjekata u elektronske usluge i elektronsko poslovanje.

Kroz uspostavljanje sistema informacione sigurnosti i upravljanje tim sistemom, javna uprava izvršava svoju ulogu u izgradnji informacionog društva. Razvojem sistema informacione sigurnosti javna uprava uspostavlja preventivne mjere i stvara organizaciono-tehničke preduvjete za sistemski razvoj zaštitnih i represivnih mjera u okviru informacionog društva. Ti procesi ne mogu se uspješno sprovoditi bez uspostavljanja konzistentnog sistema informacione sigurnosti u institucijama Bosne i Hercegovine (u daljem tekstu: Institucije).

Pod politikom upravljanja informacionom sigurnošću podrazumijeva se hijerarhijski uređen skup dokumenta koji predstavlja osnovu za implementaciju sistema upravljanja informacionom sigurnošću u Institucijama. Uopće, dokumenti politike mogu se podijeliti na krovne, sprovedbene i izvršne, kao i na standarde i preporuke. Politika tretira oblast upravljanja informacionom sigurnošću u skladu sa ISO/IEC 27001 standardom.

Također, politika se ne odnosi na oblast tajnih podataka, budući da je ista u Bosni i Hercegovini uređena odgovarajućim zakonskim i podzakonskim propisima.

1. OPĆE O INFORMACIONOJ SIGURNOSTI

1.1. Pojam informacione sigurnosti

Pojam informacione sigurnosti obrađuje se na način koji je danas prihvaćen u razvijenim zemljama svijeta i koji osigurava kompatibilnost sa konceptom informacione sigurnosti NATO-a (*North Atlantic Treaty Organisation*) i EU (*The European Union*). Pri tome treba imati u vidu da informaciona sigurnost nije isto što i informatička sigurnost. Naime, informaciona sigurnost se odnosi na zaštitu informacija bez obzira na medij na kome se čuva i prijenosi. Sistemom informacione sigurnosti obuhvataju se fizička lica, procesi, organizacija i tehnologija. Taj sistem se sastoji od uravnoteženog skupa sigurnosnih mjera, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacionih sistema, koordiniranog uvođenja formalnih procedura, kao što su procjene rizika, certificiranje uređaja i akreditacije tehničkih sistema za primjenu u određenim segmentima poslovnih procesa u Institucijama. Uravnoteženost i koordinacija mjera i postupaka treba da se postiže organizacijom i upravljanjem sistemom informacione sigurnosti.

1.2. Definicija i uloga politike upravljanja informacionom sigurnošću

Uspješna realizacija namjere da se ovlada obimnim i složenim problemom kakav je upravljanje informacionom sigurnošću, pretpostavlja postojanje polazne osnove koja će to omogućiti, a takvu osnovu predstavlja **politika**. Dakle, politika je neophodan temelj na kojem se može razviti jedan efikasan i sveobuhvatan sigurnosni program.

Donošenje politike upravljanja informacionom sigurnošću jedan je od najboljih načina kako savremene državne institucije mogu postepeno i sistemski riješiti probleme vezane za sigurnost informacija. Primjena informaciono - komunikacionih tehnologija danas predstavlja jedan od osnovnih preduvjeta za povećanje efikasnosti u poslovanju, kako u privatnom sektoru, tako i u organima javne uprave. Međutim, tehnologija nije i ne može biti sama sebi svrha. Informacione tehnologije treba, prije svega, da budu osnova i stimulans za restrukturiranje poslovnih procesa u organima javne uprave i međusobnu koordinaciju tih organa.

Svaki informacioni sistem treba da se postepeno i sistemski nadograđuje i kvalitetno održava kroz cijeli životni ciklus, u svakoj svojoj fazi od inicijalizacije i idejnog projekta, preko razvoja, implementacije, korištenja pa sve do rashodovanja. Sigurnosna procjena mora biti dio svih tih faza životnog ciklusa. Izgradnja računarsko-komunikacione mreže institucije javne uprave neophodna je za ostvarivanje elektronskih usluga za stanovništvo i poslovne subjekte, kao i za međusobno povezivanje institucija javne uprave.

Sigurnosna procjena projekta računarsko-komunikacione mreže organa javne uprave nije moguća sve do potpunog uspostavljanja sistema informacione sigurnosti u Bosni i Hercegovini, što predstavlja dodatni razlog za ubrzano uspostavljanje tog sistema.

1.2.1. Definicija politike upravljanja informacionom sigurnošću

Informacioni sistemi sadrže podatke kojima se služe ovlašteni korisnici na osnovu kojih im je omogućen pristup i korištenje sistema (identifikacija, lozinka, itd.). Obzirom da takvi podaci ne smiju biti javno dostupni, ne smiju biti mijenjani bez odobrenja i ne smiju biti nedostupni vlasnicima, važno je sprovesti određene mjere sigurnosti kako bi navedeni uvjeti uvijek bili zadovoljeni.

Politika upravljanja informacionom sigurnošću u osnovi definira odnos organizacije prema informacionim dobrima i u tom kontekstu njena primarna svrha jeste da informira rukovodioce, tehnička lica i korisnike o bitnim zahtjevima za zaštitu informacione imovine, uključujući ljude, hardverske i softverske resurse i podatke. Dakle, politika upravljanja informacionom sigurnošću pribavlja okvir za najbolju praksu koju mogu razumjeti i ispratiti svi zaposleni, čime presudno pomaže da se osigura minimiziran rizik i da se na bilo koji sigurnosni incident efikasno odgovori. Politikom korisniku se nameću obavezna pravila ponašanja i odgovornosti kako bi se zaštitio informacioni sistem, tj. informacije smještene u informacionom sistemu, od vanjskih i unutrašnjih neprimjerenih utjecaja.

Politikom su definirana pravila koja se odnose na svu informatičku opremu organizacije (hardver i softver), osobe odgovorne za administraciju informacionog sistema, sve zaposlene i korisnike sistema, odnosno osobe koje imaju pravo pristupa i vanjske saradnike.

Nakon definiranja politike važno je osigurati da se pravila koja su definirana istom sprovode i poštuju. Da bi se to postiglo bitno je svakom korisniku sistema dati na znanje da je politika uvedena i upoznati ga sa njegovim dužnostima. Postoji više načina kako korisnike upoznati sa politikom, npr. dijeljenjem dokumenta politike ili objavljivanjem sigurnosne politike na web stranicama institucije itd.

1.2.2. Uloga politike upravljanja informacionom sigurnošću

Uvođenjem i sprovođenjem politike institucija smanjuje mogućnost gubitka podataka što u velikoj mjeri utječe na efikasno poslovanje.

Sigurnosti informacionih sistema doprinosi ispravna upotreba svih dijelova informacionog sistema i poštovanje pravila propisanih sigurnosnom politikom institucije. Politikom se propisuju dozvoljene i nedozvoljene radnje kako bi se osigurala postojanost informacionog sistema i podataka koje on sadrži. Kreiranjem politike upravljanja informacionom sigurnošću, korisnicima se nameću obavezujuća pravila ponašanja koja ograničavaju slobodu prilikom pregledanja informacija, kao i pravila za ispravno korištenje računarske opreme koja su korisniku data na korištenje. Mehanizmi zaštite i sprječavanja dijele se na tri osnovna nivoa:

- **fizička sigurnost**, pod kojom se smatra sigurnost računarske opreme i podataka,
- **lična sigurnost**, koja podrazumijeva zaštitu korisnika i povjerljivih informacija o korisniku,
- **sigurnost institucije**, koja proizilazi iz prva dva nivoa.

Termin **informaciona sigurnost** podrazumijeva stanje u kojem je osiguran **integritet** hardvera, procesa i podataka, njihova **raspoloživost** i **povjerljivost** podataka i informacija.

Integritet u razmatranom kontekstu podrazumijeva tačnost i kompletnost podataka i informacija koji se nalaze na sistemu i samog sistema u njegovoj cijelosti, uključujući i procese koji se na njemu odvijaju.

Da bi se smatrali **raspoloživim**, podaci, informacije i sistem moraju biti na svom mjestu, dostupni i upotrebljivi za obavljanje funkcija koje su im namijenjene. U tom kontekstu termin *raspoloživost* povezan je i sa *kontinuitetom* usluga.

Povjerljivost se koristi u kontekstu osjetljivosti na otkrivanje (objelodanjivanje) podataka i informacija.

1.3. Definiranje sigurnosnih zahtjeva

Tri su glavne kategorije za definiranje sigurnosnih zahtjeva:

- Procjena rizika, uzimajući u obzir poslovnu strategiju institucije i njezine ciljeve. Na ovaj način se identificiraju prijetnje imovini institucije, njezina ranjivost i određuje vjerovatnost pojave prijetnji, kao i njihov utjecaj na instituciju ukoliko se te prijetnje realiziraju;

- Ustavne, zakonske i ugovorne obaveze koje institucija mora zadovoljiti;
- Skup ciljeva, načela i poslovnih zahtjeva institucije.

1.3.1. Procjena rizika

Metodičkom procjenom sigurnosnih rizika identificiraju se sigurnosni zahtjevi. Proširenje sigurnosnih kontrola mora biti proporcionalno šteti koju sigurnosni propusti nanose instituciji. Rezultati procjene rizika pomažu u određivanju prioriteta i adekvatnih akcija kod upravljanja sigurnosnim rizicima. Kako bi se u procjenu uključile bilo kakve promjene koje bi mogle utjecati na rizik, procjena rizika se mora provoditi periodički.

1.3.2. Izbor odgovarajućih kontrola

Kako bi se rizik sveo na prihvatljiv nivo, nakon identificiranja sigurnosnih zahtjeva i izrade procjene rizika, potrebno je izabrati i implementirati adekvatne kontrole. Izbor kontrola zavisi o instituciji, odnosno prihvatljivosti rizika i načinu upravljanja rizikom, ali i o državnim i međunarodnim zakonskim pravima i obavezama.

1.3.3. Početna tačka u postizanju informacione sigurnosti

Sa zakonske tačke gledišta kontrole presudne za instituciju odnose se na zaštitu tajnosti ličnih podataka i informacija, čuvanje institucijskih izvještaja i poštovanje prava intelektualnog vlasništva.

Prilikom implementacije sistema upravljanja informacionom sigurnošću, kontrole koje u praksi postižu dobre rezultate su:

- sigurnosna politika;
- podjela odgovornosti informacione sigurnosti;
- svijest o informacionoj sigurnosti, edukacija i trening;
- ispravno procesiranje podataka u aplikacijama;
- upravljanje ranjivostima;
- upravljanje poslovnim kontinuitetom;
- upravljanje sigurnosnim incidentima i poboljšanjima sistema.

1.4. Važnost uspostave sistema upravljanja informacionom sigurnošću

Informacije i pripadajući procesi, sistemi i mreže u Institucijama su od izuzetne važnosti. Kako bi se zadovoljile zakonske norme i osigurao ugled, od presudne važnosti može biti definiranje, implementacija, održavanje i poboljšavanje upravljanja informacionom sigurnošću. Računarske prevare, špijunaže, sabotaže, vandalizam, požar, poplave i sl. su sigurnosne prijetnje sa kojima se Institucije često suočavaju. Šteta nanesena instituciji u obliku zlođudnog koda, računarskog hakiranja i uskraćivanja usluge je sve prisutnija pojava. Upravljanje informacionom sigurnošću zahtjeva učestvovanje svih zaposlenih u Institucijama.

2. UPRAVLJANJE INFORMACIONOM SIGURNOŠĆU INSTITUCIJE

Cilj: Uspostava sistema za upravljanje sigurnošću informacija (ISMS) institucije kako bi se osigurala podrška rukovodiocima institucije i njihovoj usmjerenosti ka informacionoj sigurnosti, a u skladu sa poslovnim zahtjevima i odgovarajućim zakonima.

Standardi informacione sigurnosti

Uspostavljanje upravljanja informacionom sigurnošću u instituciji zahtijeva primjenu standarda za sigurnost informacionih sistema, što prema raspoloživim standardima osigurava sve aspekte zaštite nekog informacionog sistema. Na taj način se osigurava i kvalitet uspostavljenih mjera informacione sigurnosti.

Standardi iz serije ISO/IEC 27000 ISO/IEC (*Information Security Management Systems (ISMS) - Information technology - Security techniques - Information security management systems)* **institucijama pružaju smjernice za izradu, primjenu i provjeru sigurnosti informacionih sistema čime se osigurava povjerljivost, integritet i raspoloživost informacionog sadržaja, sistema i procesa unutar institucije.**

Ovi standardi su proizvod ISO/IEC JTC1 (Joint Technical Committee 1) SC27 (Sub Committee 27), ISO tehničkog tijela, koje preuzima najbolju praksu i standarde iz oblasti informacione sigurnosti i donosi ih kao međunarodne standarde. Za područje upravljanja sigurnosti informacionih sistema najčešće se koriste slijedeći ISO standardi:

- **ISO/IEC 27001 -** Sigurnosne tehnike - Sistemi za upravljanje sigurnošću informacija - Zahtjevi
- **ISO/IEC 27002 -** Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija
- **ISO/IEC 27003** - Sigurnosne tehnike - Smjernice za implementaciju sistema za upravljanje sigurnošću informacija
- **ISO/IEC 27004** - Sigurnosne tehnike - Upravljanje sigurnošću informacija - Mjerenje
- **ISO/IEC 27005 -** Sigurnosne tehnike - Upravljanje rizicima sigurnosti informacija
- **ISO/IEC 27006 -** Sigurnosne tehnike - Zahtjevi za tijela koja vrše audit i certificiranje sistema za upravljanje sigurnošću informacija
- **ISO/IEC 27011 -** Sigurnosne tehnike - Smjernice za upravljanje sigurnošću informacija za telekomunikacione organizacije zasnovane na ISO/IEC 27002
- **ISO/IEC 27013** - Sigurnosne tehnike - Smjernice za integriranu implementaciju standarda ISO/IEC 27001 i ISO/IEC 20000-1
- **ISO/IEC 27031** - Sigurnosne tehnike - Smjernice za spremnost informacione i komunikacione tehnologije za kontinuitet poslovanja
- **ISO/IEC 27033-1** - Sigurnost mreža - Dio 1: Pregled i koncepti
- **ISO/IEC 27033-2** - Sigurnost mreža - Dio 2: Smjernice za dizajn i implementaciju sigurnosti mreže
- **ISO/IEC 27033-3** - Sigurnost mreža - Dio 3: Preporuke kod scenarija umrežavanja - Prijetnje, tehnike dizajna i pitanja upravljanja
- **ISO/IEC 27033-5** - Sigurnost mreža - Dio 5: Osiguravanje komunikacije kroz mreže korištenjem virtualnih privatnih mreža (VPN)
- **ISO/IEC 27035** - Sigurnosne tehnike - Upravljanje incidentima informacione sigurnosti
- **ISO/IEC 27007** - Sigurnosne tehnike - *Smjernice za audit sistema za upravljanje sigurnošću informacijama*
- **ISO/IEC 27008** - Sigurnosne tehnike - Smjernice za auditore o kontrolama informacione sigurnosti
- **ISO/IEC 27014** - Sigurnosne tehnike - Upravljanje sigurnošću informacijama
- **ISO/IEC 27015** - Sigurnosne tehnike - Smjernice za upravljanje sigurnošću informacija kod finansijskih usluga
- **ISO/IEC 27032** - *Sigurnosne tehnike - Smjernice za kibernetičku sigurnost*
- **ISO/IEC 27034-1** - *Sigurnosne tehnike - Dio 1: Pregled i koncepti*

Ostali standardi koje treba navesti iz oblasti informacione sigurnosti su:

- **NIST SP** *(National Institute of Standards and Technology - Special Publication)* **800-30** - *Risk management guide for information technology*

systems: Standard koji detaljno propisuje na koji način vršiti procjenu i ovladati informacionim rizicima, iako je pisan za primjenu u američkim državnim službama, primjenljiv je na sve vrste organizacija.

- **NIST SP 800-34** - *Contingency planning guide for IT systems*: Preporuke za izradu planova, procedura i tehničkih mjera za oporavak IT sistema.
- **BS** *(British Standards)* **25999-2** - *Specification for business continuity management*: Standard koji specificira kako postaviti osnove za upravljanje kontinuitetom poslovanja u organizaciji bilo koje vrste.
- **BS 25999-1:2006** *Business continuity management - Code of Practice*: Smjernice za sprovođenje upravljanja kontinuitetom poslovanja.
- **NIST SP 800-61** - *Computer security incident handling guide*: Standard koji opisuje na koji način se upravlja incidentima informacione sigurnosti.
- **NIST SP 800-100** - *Information security handbook: A guide for managers*: Standard koji opisuje na koji način se upravlja informacionom sigurnošću iz pozicije različitih uloga u organizaciji. Iako je pisan za primjenu u američkim državnim službama, primjenjiv je na sve vrste organizacija.

Za efikasnu uspostavu upravljanja informacionom sigurnošću institucije uglavnom se preporučuje upotreba standarda ISO/IEC 27001. Međutim, zavisno od obima poslova i nadležnosti pojedine institucije, kao i potreba za specifičnim zahtjevima uspostavu upravljanja informacionom sigurnošću mogu se koristiti i ostali standardi iz serije 27000, kao i ostali međunarodno priznati standardi koji se bave problematikom informacione sigurnosti.

Standard ISO/IEC 27001

ISO/IEC 27001 (*ISO/IEC 27001 Informacione tehnologije - Tehnike zaštite -Specifikacije za sistem upravljanja informacionim sistemom*) standard je izrađen 2005. godine, a nastao je na osnovu standarda BS 7799 (British Standards).

ISO/IEC 27001 je službena grupa specifikacija na osnovu kojih institucije mogu zatražiti postupak certifikacije, naravno pod uvjetom da su primijenile taj standard na sistem upravljanja sigurnošću informacija. Ovaj standard propisuje zahtjeve za ustanovljavanje, implementaciju, kontrolu i unaprjeđenje ISMS-a.

Standard se sastoji od 5 dijelova:

1. Sistem za zaštitu informacija,
2. Odgovornost menadžmenta,
3. Interna provjere sistema za zaštitu informacija,
4. Provjera ispravnosti sistema za zaštitu informacija,
5. Poboljšanja na sistemu za zaštitu informacija.

Takođe, u standardu su navedeni ciljevi provjere koje je potrebno ostvariti i provjere koje je potrebno sprovesti kako bi se ostvarili ti isti ciljevi. Postoje institucije akreditirane za certifikaciju prema ISO/IEC 27001 standardu.

Standard sadrži sigurnosne odredbi što ga čini vrlo detaljnim i temeljnim. Suštinski, standard sadrži polazno poglavlje "Procjena i upravljanje ICT rizikom" sa ostalim dijelovima u koji su grupisani prema sigurnosnim odredbama:

1) Organizacija informacione sigurnosti (2);
2) Upravljanje imovinom (2);
3) Sigurnost i ljudski resursi (3);
4) Fizička zaštita i zaštita od okoliša (2);
5) Upravljanje komunikacijama i operacijama (10);
6) Kontrola pristupa (7);
7) Nabavka, razvoj i održavanje informacionog sistema (6);
8) Upravljanje incidentima informacionog sistema (2);
9) Upravljanje poslovnim kontinuitetom (1);
10) Usklađivanje (3).

Svaka sigurnosna odredba sadrži:

a) kontrolni cilj koji je potrebno ostvariti;
b) jednu ili više kontrola koje se mogu primijeniti da bi se ostvario kontrolni cilj.

Opisi kontrola su definirani na slijedeći način:

Kontrola: Definira određenu kontrolu koja treba zadovoljiti kontrolni cilj.

Implementacijske smjernice: Pruža detaljnije informacije za implementiranje kontrole.

Dodatne informacije: Pruža dodatne informacije koje je potrebno razmotriti pri uvođenju neke kontrole, npr. legalne aspekte kontrole i reference na neke druge standarde. Ovaj kodeks postupaka treba biti početna tačka razvoja informacione sigurnosti specifične za svaku pojedinu instituciju. Sve kontrole i smjernice ne mogu se primijeniti na svaku instituciju. Ponekad je potrebno uključiti kontrole i smjernice koje nisu dio ovog standarda ukoliko to zahtijeva poslovanje institucije.

Sistem upravljanja informacionom sigurnošću (engl. ISMS Information Security Management System)

Sve institucije, svih vrsta i veličina, sakupljaju, obrađuju, pohranjuju i prijenose velike količine informacija, te prepoznaju da su informacije i njima dodijeljeni procesi, sistemi, mreže i ljudi vrlo važna imovina za postizanje poslovnih ciljeva institucije. Takođe, institucije se suočavaju se sa širokim područjem rizika koji utječu na funkcioniranje njihove imovine, te modificiraju rizike kroz implementaciju sigurnosnih kontrola.

Budući da se rizici informacione sigurnosti, te efikasnost kontrola mijenjaju zavisno o promjenama okoliša, svaka institucija treba nadgledati i vrjednovati efikasnost primijenjenih kontrola i procedura, identificirati pojavu rizika koji se moraju obraditi i odabrati, primijeniti i poboljšavati kontrole kada je to potrebno.

Sistem upravljanja informacionom sigurnošću - osigurava model za uspostavu, implementaciju, rad, nadzor, preglede, održavanje i poboljšanje zaštite informacione imovine u cilju postizanja poslovnih ciljeva koji su zasnovani na procjeni rizika te na prihvatljivom nivou rizika za instituciju na kojima se zasniva efikasna obrada i upravljanje rizika.

Principi koji takođe doprinose uspješnoj implementaciji ISMS-a su:

- Podizanje svijesti o razumijevanju i potrebi za informacionom sigurnošću;
- Pridruživanje odgovornosti za informacionu sigurnost;
- Uključivanje podrške menadžmenta institucije i interesa zainteresiranih strana;
- Procjena rizika određuje odgovarajuće kontrole kako bi se dostigao prihvatljiv nivo rizika;
- Sigurnost uključiti kao važan element informacionih sistema i mreža;
- Aktivna prevencija i detekcija incidenata informacione sigurnosti;
- Osiguravnje sveobuhvatnog rješenja za upravljanje informacionom sigurnošću;
- Kontinuirana procjena informacione sigurnosti, te provođenje izmjena kada je to potrebno.

Procesni pristup

Procesno rješenje za ISMS koje se koristi u ISMS familiji standarda je uopćeno poznat kao **Plan-Do-Check-Act** (PDCA) proces (*Deming-ov ciklus*):

- **Plan**: Uspostavljanje ISMS politike, ciljeva, procesa i procedura važnih za upravljanje rizikom i povećanje

informacione sigurnosti kako bi dali rezultate u skladu sa ukupnom politikom i ciljevima institucije;
- **Do**: Implementacija i pokretanje ISMS politike, kontrola i procedura;
- **Check**: Procjena, i gdje je primjenjivo, mjerenje performansi procesa u odnosu na ISMS politiku, ciljeve i praktično iskustvo te izvještavanje menadžmenta o rezultatima;
- **Act**: Izvođenje korektivnih i preventivnih akcija zasnovanih na rezultatima ISMS procjene (audita) i procjene menadžmenta ili ostalim bitnim informacijama, kako bi se ISMS kontinuirano usavršavao.

Važnost uspostave ISMS-a

- Postiže veću garanciju sigurnosti u zaštiti informacione imovine od informacionih rizika na kontinuiranoj osnovi;
- Održava radni okvir za identificiranje i procjeni rizika informacione sigurnosti, odabir i primjenu odgovarajućih sigurnosnih mjera (kontrola) te mjerenje i poboljšanje njihove efikasnosti;
- Kontinuirano poboljšava kontrolirani okoliš;
- Efikasno postiže zakonsku i regulatornu usklađenost.

Kritični faktori uspjeha ISMS-a

Primjeri kritičnih faktora uspjeha su:
- Politika informacione sigurnosti institucije, ciljevi i aktivnosti koje su podešene ciljevima;
- Rješenje i radni okvir za projektiranje, implementaciju, nadzor i unapređenje informacione sigurnosti koje je konzistentno sa kulturom institucije;
- Vidljiva podrška i predanost na svim nivoima upravljanja, posebno na nivo visokog menedžmenta;
- Razumijevanje zahtjeva za zaštitu informacione imovine koja se postiže kroz primjenu upravljanja rizikom informacione sigurnosti;
- Efikasan program podizanja svijesti o informacionoj sigurnosti, treningu i edukaciji, informiranje svih zaposlenih i ostalih strana o njihovim obavezama;
- Efikasan proces upravljanja incidentima informacione sigurnosti;
- Efikasno rješenje za kontinuitet poslovanja;
- Sistem mjerenja koji se koristi za vrjednovanje performansi u upravljanju informacionom sigurnošću.

Način uspostave ISMS-a

- Primjena kontrola definiranih Politikom informacione sigurnosti institucija Bosne i Hercegovine;
- Oformiti vlastiti tim eksperata za informacionu sigurnost ili angažirati vanjske konsultante;
- Rukovoditi se najboljom praksom;
- Implementacija **standarda ISO/IEC 27001**, *Information security management systems –Requirements.*

2.1. PROCES IMPLEMENTACIJE POLITIKE

Preporuka je da institucija implementaciju politike upravljanja informacionom sigurnošću bazira na unaprijed izrađenim standardima, čime se uveliko smanjuju operativni troškovi i vrijeme potrebno za sprovođenje iste. Implementaciju ove politike institucija može izraditi samostalno, procjenom mogućih prijetnji informacionom sistemu, te procjenom i zaštitom slabih tačaka sistema. Ovaj proces je dugotrajniji i skuplji, ali osigurava način zaštite koji potpuno odgovara potrebama institucije. Iako se na prvi pogled samostalna implementacija sigurnosne politike čini kao bolje rješenje, preporučuje se implementacija sigurnosne politike institucije na bazi standarda kako bi se obratila pažnja na sve moguće prijetnje koje mogu ugroziti informacioni sistem. Kako je prethodno naglašeno, implementacija sigurnosne politike institucije treba se zasnivati na ISO/IEC 27001 standardu. Međutim, potrebno je pomenuti da ISO/IEC 27001 standard opisuje sve **šta** je potrebno napraviti, ali ne i **kako**. Da bi se odgovorilo na pitanje **kako**, koristi se standard ISO/IEC 27002 kroz potrebne smjernice. Upravo na bazi ovog standarda opisan je proces uspostavljanja sigurnosne politike, tj. koraci i postupci koje je potrebno napraviti.

2.1.1. Upravljanje i procjena rizika

Upravljanje rizikom je proces kojim se potvrđuje poslovna opravdanost odabira sigurnosnih rješenja i kontrola koje će osigurati dovoljan nivo sigurnosti. Također, proces upravljanja rizikom omogućuje razvoj strategije i postavljanje ciljeva u području informacione sigurnosti. Upravljanje rizikom uključuje tri procesa: **procjenu rizika, umanjivanje rizika i evaluaciju rizika**.

Proces upravljanja rizika omogućuje stvaranje ravnoteže između operativnog i ekonomskog troška zaštitnih mjera, te dobiti koja se ostvaruje zaštitom informacionih sistema i podataka. Dobro strukturirana metodologija upravljanja rizikom jedan je od ključnih faktora pri odabiru odgovarajućih sigurnosnih kontrola koje osiguravaju kontinuirano odvijanje poslovnih procesa.

Standard ISO/IEC 27005 nudi propisanu metodu za analizu i procjenu rizika, za razliku od ISO 27001 standarda koji je fleksibilan i nudi mogućnost da institucija primjenjuje čak i nekoliko metoda za procjenu rizika.

2.1.2. Identifikacija resursa

Jedan od uvjeta za uspješno upravljanje sigurnošću informacionog sistema jeste identificiranje resursa koji su dio tog sistema. Bez precizne identifikacije resursa nije moguće sprovesti njegovu kvalitetnu zaštitu. Kroz proces identificiranja resursa potrebno je evidentirati sve resurse unutar informacionog sistema te procijeniti njihovu relativnu vrijednost za instituciju. Kako bi se mogla odrediti vrijednost resursa za instituciju, potrebno je poznavanje poslovnih procesa koji se odvijaju u instituciji. Na osnovu toga je kasnije u procesu upravljanja rizikom, odnosno prilikom analize rizika, moguće ocijeniti potreban nivo zaštite za svaki pojedini resurs bitan za funkcioniranje poslovnih procesa unutar institucije. Kvalitetnim identificiranjem resursa nužno je postići slijedeće zahtjeve:
- ustanoviti vlasnike poslovnih procesa, odnosno odgovorne osobe,
- identificirati pojedine resurse bitne za funkcioniranje poslovnih procesa,
- procijeniti vrijednost resursa,
- ustanoviti njihovo fizičko ili logičko mjesto u sistemu,
- napraviti odgovarajuću dokumentaciju.

Podjelu resursa moguće je napraviti prema raznim pravilima. U informacionim sistemima resurse je moguće podijeliti u slijedeće kategorije:
- informacije (baze podataka, dokumentacija, autorska djela itd.),
- programska podrška (aplikacije, operativni sistemi, razvojni alati itd.),
- oprema (računarska oprema, mrežno-komunikaciona oprema, mediji za čuvanje podataka i ostala oprema potrebna za rad informacionog sistema),
- servisi (računarski i komunikacioni i uopćeno servisi kao što su klimatizacija, osvjetljenje itd.).

Za svaki od identificiranih resursa potrebno je napraviti procjenu njegove relativne vrijednosti unutar sistema bez obzira kojoj kategoriji pripada. Cilj podjele informacija je osiguranje njihove odgovarajuće zaštite. Uz procjenu rizika potrebno je odrediti kako postupati sa rizicima. Mogući postupci uključuju:

- ugrađivanje odgovarajućih kontrola koje smanjuju rizik,
- svjesno i objektivno prihvatanje rizika, udovoljavajući sigurnosnoj politici institucije i kriterijumima prihvatljivog rizika,
- izbjegavanje rizika zabranama, tj. onemogućavanjem akcija koje prouzrokuju rizik.

Za rizike čiji postupci uključuju implementaciju odgovarajućih kontrola, te kontrole moraju biti odabrane i implementirane na način da zadovoljavaju zahtjeve definirane procjenom rizika.

2.1.3. Analiza rizika

Analiza rizika je postupak kojem je cilj da se ustanove ranjivosti sistema, uoče potencijalne prijetnje (rizici), te na odgovarajući način kvantificirati moguće posljedice kako bi se mogao odabrati najprimjereniji način zaštite, odnosno procijeniti opravdanost uvođenja dodatnih protivmjera. Postoje dva osnovna pristupa analizi rizika: kvantitativna i kvalitativna analiza.

Kvantitativna analiza podrazumijeva iskazivanje rizika u očekivanim novčanim troškovima na godišnjem nivou, dok rezultat kvalitativne analize iskazuje samo relativan odnos vrijednosti šteta nastalih djelovanjem neke prijetnje i uvođenja protivmjera.

2.1.4. Tumačenje rezultata

Analizom rizika moraju se utvrditi slijedeće činjenice:

- kritični resursi i prijetnje i vjerovatnost njihove pojave,
- potencijalni gubici koje uzrokuje ostvarenje prijetnje,
- preporučene protivmjere i njihova vrijednost (relativna ili novčana),
- nadzor i zaštita.

Na osnovu dobijenih rezultata potrebno je odlučiti kakve protivmjere treba preduzeti. Postoje tri mogućnosti djelovanja koje ne moraju biti međusobno isključive, a to su: smanjenje rizika, prijenos rizika i prihvatanje rizika.

Jedini važan parametar prilikom izbora načina djelovanja je isplativost za instituciju. Smanjenje rizika predstavlja proces u kojem se na osnovu provedene analize rizika nastoje sprovesti odgovarajuće protivmjere i uvesti sigurnosni nadzor da bi se zaštitili resursi institucije. Ukoliko se pokaže isplativijim, rizik je moguće prenijeti na treću stranu (na primjer, osiguravajuće društvo). Isto tako moguće je da implementacija protivmjera ili prijenos rizika nisu isplativi. U tom slučaju institucija može odlučiti da prihvati rizik, odnosno troškove koji iz toga proizlaze. Jedini pristup koji u upravljanju rizikom nije prihvatljiv je ignoriranje ili zanemarivanje rizika.

Na osnovu ove Politike upravljanja informacionom sigurnošću u Institucijama uspostavlja se niz pravila i smjernica koje je potrebno izraditi kroz interne dokumente institucije, u cilju uspostave "Sistema upravljanja informacionom sigurnošću - ISMS" u svim institucijama u skladu sa uočenim zahtjevima i potrebama svake institucije pojedinačno.

Da bi implementacija sigurnosne politike bila efikasna potrebno je politiku primijeniti na svaki dio institucije. Dokumente za uspostavu ISMS-a je potrebno službeno objaviti i upoznati sve zaposlene i korisnike o njihovom sadržaju, a koji trebaju sadržavati kontrole i ciljeve definirane standardom ISO 27001, a u skladu sa zahtjevima, potrebama, zakonskom legislativom i internim pravilima svake institucije.

2.1.5. Važnost usvajanja politike upravljanja informacionom sigurnošću u institucijama BiH

Usvajanjem Politike upravljanja informacionom sigurnošću, Vijeće ministara Bosne i Hercegovine izražava odlučnost u podršci naporima koji za svoj cilj imaju poboljšanje informacione sigurnosti. Također, stvara se pravni osnov za donošenje zakona i podzakonskih akata kojim će se bliže urediti način postupanja Institucija sa ciljem uvođenja minimalnih sigurnosnih kriterijuma i uspostava sistema za upravljanje sigurnošću informacija.

2. 2. ORGANIZACIJA INFORMACIONE SIGURNOSTI

2.2.1. Unutrašnja organizacija

CILJ	AKTIVNOSTI
Upravljanje informacionom sigurnošću unutar institucije.	- uraditi procjenu nivoa sigurnosti nekog dijela opreme (npr. laptop-a). - popisati vrijednosti koje organizacija posjeduje na način da se svako korištenje dokumentuje sa ciljem zaštite vrijednosti od kopiranja, uništavanja i zamjene od strane zaposlenih, partnera ili treće strane.

2.2.2. Vanjski saradnici

CILJ	AKTIVNOSTI
Održavanje sigurnosti informacija i opreme za obradu informacija institucije kojima pristupaju, koje obrađuju, prijenose ili kojima upravljaju vanjski saradnici.	- savjetovati se sa organizacijama koje se - bave računarskom sigurnošću kako bi se u slučaju sigurnosnih incidenata dobili primjereni savjeti i smjernice koje upućuju kako djelovati. - održavanje kontakta sa drugim organizacijama zbog unapređenja znanja o sigurnosti informacionih sistema ili brzih obavještenja u slučaju sigurnosnog incidenta. - redovno provjeravati sigurnost informacionog sistema zbog osiguravanja u smislu ispravnog funkcioniranja sistema zaštite. - održati jednak nivo sigurnosti i kod informacija kojima treća strana ima pristup. - provjeriti moguće rizike prije dodjele prava pristupa trećoj strani kako bi se informacioni sistem primjereno zaštitio. - formalnim dokumentom odrediti pravila zaštite koja su u skladu sa sigurnosnom politikom organizacije ukoliko postoji dogovor sa trećom stranom koja ima pristup informacionom sistemu.

2.3. UPRAVLJANJE IMOVINOM

2.3.1. Odgovornost za imovinu

CILJ	AKTIVNOSTI
Postizanje i održavanje odgovarajuće zaštite imovine institucije.	- identificirati (popisati) imovinu institucije u svrhu procjene vrijednosti i važnosti, i shodno tome primjerenog nivoa zaštite. - odrediti vlasnika, tj. osobu odgovornu za sigurnost i zaštitu imovine kako ne bi došlo do mijenjanja ili otuđivanja imovine, - definirati jasna pravila ispravnog korištenja imovine kako ne bi došlo do gubitka informacija ili sigurnosnog incidenta.

2.3.2. Klasifikacija informacija

CILJ	AKTIVNOSTI
Osigurati da informacione vrijednosti dobiju odgovarajući nivo zaštite.	- Informacije trebaju biti klasificirane kako bi se iskazala potreba, prioritet i nivo zaštite. -klasifikaciju informacija izvoditi na osnovu vrijednosti, osjetljivosti, važnosti za instituciju i zakonodavnih okvira. - definirati procedure za označavanje i rukovanje informacijama, npr. procedure za kopiranje, snimanje, prijenos, itd.

2.4. ZAŠTITA OD ZAPOSLENIH

2.4.1. Prije zaposlenja

CILJ	AKTIVNOST
Osigurati zaposlenima, ugovornim saradnicima i trećoj strani razumijevanje njihovih odgovornosti, provjeriti njihovu podobnost za posao koji im je namijenjen i smanjiti rizik od krađe, prevare ili zloupotrebe opreme.	-prije zaposlenja ili ugovaranja posla sa ulagačima ili trećom stranom potrebno je u ugovor uključiti dio koji sve strane obavezuje na poštovanje sigurnosne politike institucije. -definirati uloge i odgovornosti zaposlenih, zaposlenih po osnovu ugovora i treće strane. -provjeravaju se potencijalni zaposleni, ili poslovni partneri kako bi se povećala sigurnost informacionog sistema.

2.4.2. Tokom zaposlenja

CILJ	AKTIVNOST
Osigurati zaposlenima, ugovornim saradnicima i trećoj strani razumijevanje prijetnji informacionoj sigurnosti, njihovih odgovornosti i obaveza kao i opremiti ih za podršku sigurnosnoj politici institucije tokom njihovog normalnog rada i smanjiti rizik ljudske greške.	-informiranje zaposlenih o ulogama i odgovornostima u sprovođenju sigurnosti od strane rukovodstva institucije. - provesti edukacija o informacionoj sigurnosti zaposlenih ili treće strane kako bi se postigli zadovoljavajući rezultati, tj. kako bi svi bili svjesni važnosti zaštite informacionog sistema.

2.4.3. Prekid ili promjena zaposlenja

CILJ	AKTIVNOST
Osigurati zaposlenima, ugovornim saradnicima i korisnicima treće strane uredno napuštanje institucije ili promjenu zaposlenja.	- jasno definirati procedure koje je potrebno izvršiti po raskidu radnog odnosa, ili ugovora, tj. odrediti pravila o vraćanju imovine instituciji koja je zaposlenom data na korištenje, ukidanje prava pristupa informacionom sistemu, itd.

2.5. FIZIČKA ZAŠTITA I ZAŠTITA OD OKOLIŠA

2.5.1. Osigurana područja

CILJ	AKTIVNOSTI
Sprječavanje neovlaštenog fizičkog pristupa, oštećenja i ometanje prostora i informacija institucije.	- osigurati da moraju biti zaštićeni nekom vrstom fizičke prepreke, npr. zidovima, vratima, autentifikacijskim uređajima, itd. - postaviti odgovarajuće metode provjere ulaska u dijelove institucije koji sadrže povjerljive informacije kako bi se osiguralo da pravo pristupa prostorijama za te namjene unutar institucije imaju samo ovlaštene osobe.

2.5.2. Sigurnost opreme

CILJ	AKTIVNOSTI
Sprječavanje gubitka, oštećenja, krađe ili ugrožavanja imovine i prekida aktivnosti institucije.	- osigurati zaštitu primjerenu vrijednostima institucije kako ne bi došlo do gubitaka, štete ili prekida poslovnih aktivnosti, - opremu smjestiti u skladu sa uputstvima proizvođača opreme, - voditi računa o ispravnosti instalacija u prostorijama institucije kako ne bi došlo do oštećenja informacionog sistema, - zaštitit kablove za napajanje električnom energijom ili telekomunikacione kablove u skladu s propisima, - redovno održavati opremu prema uputstvima proizvođača, a održavanje smiju raditi samo ovlaštene osobe.

2.6. UPRAVLJANJE KOMUNIKACIJAMA I OPERACIJAMA

2.6.1. Operativne procedure i odgovornosti

CILJ	AKTIVNOSTI
Osigurati ispravan i siguran rad opreme za obradu informacija.	- nadzor promjena u operativnim sistemima i objektima, - provesti postupak razdvajanja obaveza i odgovornosti zaposlenih kako bi se mogućnosti obavljanja neovlaštenih i neželjenih radnji svele na minimum, - odvojiti razvojne i aktivnosti vezane za ispitivanje, isto kao i aktivnosti vezane uz operativni rad (npr. program koji se provjerava ili razvija može biti opasan za ispravno funkcioniranje informacionog sistema, pa je potrebno odvojiti sisteme na kojima se obavlja razvoj i ispitivanje od onih na kojima se radi).

2.6.2. Planiranje i prihvatanje sistema

CILJ	AKTIVNOSTI
Smanjenje rizika od zastoja u radu sistema.	- osigurati dostupnosti potrebnih kapaciteta računarskih i drugih resursa

2.6.3. Zaštita od zlođudnog i prenosivog koda

CILJ	AKTIVNOSTI
Zaštititi cjelovitost softvera i informacija.	- uvesti zaštitu koja će odgovorne osobe u instituciji upozoriti da je informacioni sistem ugrožen zlonamjernim programom kako bi se zaštitio integritet podataka, - ugraditi određene alate i mjere koji će redovno pratiti da li u sistemu postoje zlonamjerni programi.

2.6.4. Sigurnosne kopije

CILJ	AKTIVNOSTI
Očuvanje integriteta i dostupnosti podataka redovnom izradom sigurnosnih kopija neophodnih poslovnih informacija.	Redovno izrađivati sigurnosne kopije podataka radi očuvanja integriteta i raspoloživosti istih, pri čemu treba uzeti u obzir slijedeće: - na udaljenoj lokaciji potrebno je spremati minimalni broj sigurnosnih kopija informacija, zajedno sa tačnim i potpunim zapisima o sigurnosnim kopijama i dokumentiranim procedurama za osnovno osposobljavanje sistema. Lokacija treba biti na dovoljnoj udaljenosti od glavne lokacije kako bi se izbjegla šteta koja može nastati od posljedica katastrofe na glavnoj lokaciji, - sigurnosnim kopijama mora se osigurati odgovarajući nivo fizičke zaštite i zaštite okoliša u skladu sa standardima koji se primjenjuju na glavnoj lokaciji, - mediji sigurnosnih kopija, gdje je primjenjivo, moraju se redovno testirati kako bi se osiguralo da se na njih može računati u slučaju potrebe, - procedure za ponovno uspostavljanje sistema moraju se redovno provjeravati i testirati kako bi se osigurala njihova efikasnost i mogućnost izvršavanja u predviđenom vremenu, - vrijeme čuvanja sigurnosnih kopija mora biti vremenski tačno određeno.

2.6.5. Upravljanje sigurnošću mreže

CILJ	AKTIVNOSTI
Osiguranje zaštite informacija u mrežama i zaštite prateće infrastrukture.	- osigurati zaštitu informacija koje mrežni sistem sadrži, te zaštititi sam mrežni sistem - operativne odgovornosti za mreže trebaju biti odvojene od računarske operative gdje je to moguće, - uspostaviti postupke i odgovornosti za upravljanje udaljenom opremom, - uspostaviti kontrole kako bi se sačuvala povjerljivost i integritet podataka koji prolaze nezaštićenim mrežama.

2.6.6. Rukovanje izmjenjivim i trajnim medijima za pohranu podataka

CILJ	AKTIVNOSTI
Uspostava postupaka za upravljanje izmjenjivim i tajnim računarskim medijima (hard diskovi, trake, kasete, CD, DVD, štampani izvještaji drugo).	- ako više nisu potrebni, treba obrisati prijašnje sadržaje svakog ponovno iskoristivog medija koji će biti uklonjen iz institucije, - tražiti ovlaštenje za uklanjanje medija iz organizacije, te voditi zapis o takvim aktivnostima, - svi mediji trebaju biti pohranjeni na sigurnom i zaštićenom mjestu, u skladu sa specifikacijama proizvođača, - svi postupci i nivo ovlaštenja trebaju biti jasno određeni i dokumentirani. - ako su tvrdi diskovi neispravni, bilo da se neispravnost očituje u neispravnosti kontrolora ili magnetnih ploča/glava za zapis, treba izvršiti fizičko uništenje tvrdog diska tako da se nijednom od poznatih metoda za povratak podataka nemoguće isto ostvariti - ukoliko tvrdi diskovi više nisu potrebni, a šalju se na daljnje korištenje unutar institucije, sadržaj tvrdog diska treba "sigurno obrisati" prema propisanim procedurama - o svakom uništenom/"sigurno obrisanom" tvrdom disku treba voditi zapisnik/dnevnik o svim izvršenim aktivnostima - svi uništeni tvrdi diskovi trebaju biti pohranjeni na sigurnom i zaštićenom mjestu, u skladu sa internim procedurama institucije - svi postupci i nivo ovlaštenja trebaju biti jasno određeni i dokumentirani

2.6.7. Razmjena informacija

CILJ	AKTIVNOSTI
Osigurati sigurnost pri razmjeni informacija i softvera unutar institucije ili izvan nje.	- osigurati zaštitu pri razmjeni podataka i programa unutar institucije ili izvan nje. - kako bi se zaštitila razmjena podataka potrebno je definirati smjernice razmjene, uspostaviti i vršiti kontrolu, te sankcionirati prekršioce u skladu sa važećim zakonima.

2.6.8. Nadzor

CILJ	AKTIVNOSTI
Blagovremeno uočavanje neovlaštenih aktivnosti.	- Informacioni sistem potrebno je konstantno nadgledati (eng. monitoring), te bilježiti svaku aktivnost. Nadgledanje mora zadovoljavati sve važeće zakone, korisnike treba obavijestiti o nadgledanju i dati im do znanja da su im prava privatnosti minimalna.

	- Kako bi bili uočeni eventualni propusti u implementaciji sigurnosnih kontrola potrebno je voditi dnevnik svih aktivnosti i događaja unutar sistema u cilju moguće otkrivanja nepravilnosti i njihovog uklanjanja na vrijeme.

2.7. KONTROLA PRISTUPA

2.7.1. Poslovni zahtjevi za kontrolu pristupa

CILJ	AKTIVNOSTI
Kontrola pristupa informacijama.	- provjera pristupa u skladu sa poslovnim zahtjevima (pristup informacijama treba odgovarati zahtjevima poslovnih dužnosti kako bi se spriječio neovlašteni pristup podacima), - uspostaviti niz pravila kojima će se odrediti nivo pristupa zaposlenih, - uspostaviti sistem upravljanje pristupom korisnika kako bi se spriječio neovlašteni pristup informacijama, - uspostaviti postupak registracije korisnika radi dobijanja prava pristupa višenamjenskim informacionim sistemima, - odrediti nivoe privilegija u informacionom sistemu koje je potrebno osigurati zaposlenim, - dokumentirati i provjeriti pristup sistemu kako bi se pravovremeno uočili pokušaji nedozvoljenih radnji, - bilježiti prethodne aktivnosti u sistemu u slučaju pojave sigurnosnog incidenta kako bi se moglo odrediti šta se zapravo dogodilo, - pratiti koliko i kako korisnici koriste sistem kako bi se osiguralo da korisnici sistema izvode samo one aktivnosti za koje su ovlašteni.

2.7.2. Upravljanje korisničkim pristupom

CILJ	AKTIVNOSTI
Osigurati pristup ovlaštenih korisnika i spriječiti neovlašteno pristupanje informacionim sistemima.	- uspostaviti procedure za kontrolu dodjele prava pristupa informacionim sistemima koje trebaju obuhvatiti sve stadije u životnom ciklusu korisničkog pristupa - od početne registracije novog korisnika do konačnog odjavljivanja korisnika kojem više nije potreban pristup sistemu i uslugama.

2.7.3. Odgovornosti korisnika

CILJ	AKTIVNOSTI
Sprječavanje pristupa neovlaštenih korisnika i ugrožavanja ili krađe informacija i opreme za obradu informacija. Za efikasnu sigurnost bitna je saradnja ovlaštenih korisnika.	- podstaći svijest korisnika o odgovornosti vezanoj uz lozinke i opremu koja im je data na korištenje radi smanjenja mogućnosti neovlaštenog pristupa,

2.7.4. Kontrola pristupa mreži

CILJ	AKTIVNOSTI
Zaštita mrežnih servisa.	- uspostaviti provjeru mrežnih servisa i usluga kako bi se zaštitio mrežni sistem od nedozvoljenih radnji,

2.7.5. Kontrola pristupa operativnom sistemu, aplikacijama i informacijama

CILJ	AKTIVNOSTI
Sprječavanje neovlaštenog pristupa operativnim sistemima.	- uspostaviti sigurnosne mehanizme unutar operativnog sistema u cilju sprječavanja neovlaštenog pristupa računarskim resursima, - spriječiti neovlašteni pristup informacijama prisutnim u aplikativnim sistemima.

2.7.6. Upotreba mobilnih računara i rad na daljinu

CILJ	AKTIVNOSTI
Ostvariti informacionu sigurnost pri upotrebi mobilnih računara i opreme za rad na daljinu.	- dodatnim sigurnosnim kontrolama treba spriječiti (otežati) sve napade koji mogu biti počinjeni zbog ostvarivanja prava pristupa s mobilnih računara, a koje prvenstveno treba da obuhvate: - načini zaštite od malicioznih programa, - načini i prava pristupa, - postavke sigurnosnih uređaja za pristup (engl. firewall). - zaštitom od malicioznih programa treba osigurati da mobilni računar ne može ugroziti informacioni sistem zato što se na njemu nalazi maliciozni program. - definirati načine pristupa treće strane resursima institucije.

2.8. NABAVKA, RAZVOJ I ODRŽAVANJE INFORMACIONIH SISTEMA

2.8.1. Sigurnosni zahtjevi informacionih sistema

CILJ	AKTIVNOSTI
Sigurnost kao sastavni dio informacionih sistema.	- Informacioni sistemi uključuju operativne sisteme, infrastrukturu, poslovne aplikacije, standardne proizvode, usluge i korisničke aplikacije. Projektiranje i primjena informacionog sistema koji podržava poslovni proces može biti od presudnog značaja za sigurnost. Prije projektiranja i/ili primjene informacionih sistema potrebno je odrediti i uskladiti sigurnosne zahtjeve. Sve sigurnosne zahtjeve potrebno je odrediti u fazi postavljanja zahtjeva projekta, te ih opravdati, uskladiti i dokumentirati kao dio ukupnog poslovnog slučaja za informacioni sistem.

2.8.2. Ispravna obrada u aplikacijama

CILJ	AKTIVNOST
Sprječavanje grešaka, gubitka, neovlaštene promjene ili zloupotrebe informacija u aplikacijama.	- U aplikacije, uključujući korisničke aplikacije, potrebno je ugraditi odgovarajuće kontrole radi osiguranja ispravne obrade. Ove kontrole trebaju sadržavati provjeru ispravnosti ulaznih podataka, interne obrade i izlaznih podataka. Dodatne kontrole mogu biti potrebne za sisteme koji obrađuju ili imaju utjecaja na osjetljive, vrijedne ili ključne informacije. Takve kontrole treba odrediti na osnovu sigurnosnih zahtjeva i procjene rizika.

2.8.3. Kriptografske kontrole

CILJ	AKTIVNOSTI
Zaštita povjerljivosti, vjerodostojnosti ili cjelovitosti informacija uz upotrebu kriptografskih tehnika.	- razviti politiku za upotrebu kriptografskih kontrola.

2.8.4. Sigurnost sistemskih datoteka

CILJ	AKTIVNOSTI
Ostvariti sigurnost sistemskih datoteka.	- kontrolirati pristup sistemskim datotekama i izvornom kodu programa, a IT projekte i prateće aktivnosti izvoditi na siguran način.

2.8.5. Sigurnost u procesima razvoja i podrške

CILJ	AKTIVNOSTI
Održavanje sigurnosti softvera i informacija aplikativnog sistema.	- strogo kontrolirati projektno okruženje i okruženje za podršku. - rukovodioci odgovorni za aplikativne sisteme trebaju također biti odgovorni za sigurnost projektnog okruženja ili okruženja za podršku. Oni trebaju osigurati provjeru svih promjena sistema kako bi se utvrdilo da ne ugrožavaju sigurnost bilo sistema ili radnog okruženja.
Sprječavanje kršenja svih pravnih, zakonskih, regulativnih ili ugovornih obaveza i sigurnosnih zahtjeva.	- Projektiranje, funkcija, upotreba i upravljanje informacionim sistemima mogu biti podvrgnuti zakonskim, regulativnim i ugovornim sigurnosnim zahtjevima. - Od pravnih savjetnika organizacije ili podobnih pravnih stručnjaka zatražiti savjet o posebnim pravnim zahtjevima. Zakonodavni zahtjevi razlikuju se od države do države i mogu se razlikovati za informacije stvorene u jednoj zemlji koje se prijenose u drugu zemlju.

2.8.6. Upravljanje tehničkom ranjivošću

CILJ	AKTIVNOSTI
Smanjenje rizika od iskorištavanja objavljenih tehničkih ranjivosti.	- Upravljanje tehničkom ranjivošću treba primijeniti na efikasan, sistematski i ponovljiv način uz mjere koje će potvrditi njegovu efikasnost. Ova razmatranja trebaju uključivati operativne sisteme i sve ostale korištene aplikacije.

2.9. UPRAVLJANJE INCIDENTIMA U INFORMACIONOM SISTEMU

2.9.1. Izvještavanje o sigurnosnim događajima i slabostima

CILJ	AKTIVNOSTI
Osiguranje izvještavanja o sigurnosnim događajima i slabostima vezanim uz informacione sisteme na način koji omogućava pravovremeno izvođenje korektivnih akcija.	- prijaviti sigurnosni incident prema unaprijed određenoj proceduri u što kraćem vremenskom roku, - prijaviti ranjivost po otkrivanju sigurnosnog propusta u informacionom sistemu u što kraćem vremenskom roku.

2.9.2. Upravljanje sigurnosnim incidentima i poboljšanjima

CILJ	AKTIVNOSTI
Osiguranje primjene dosljednog i efikasnog pristupa upravljanju sigurnosnim incidentima.	- unaprijed definirati procedure u slučaju sigurnosnih incidenata ili ranjivosti kako bi se u što kraćem vremenskom roku iste mogle riješiti, - definirati procedure koje će obuhvatiti različite vrste učestalih sigurnosnih incidenata, postupke koji će sistem zaštititi od ponavljanja istog sigurnosnog incidenta, i sačuvati i zaštititi dokumentaciju o incidentu kako bi se upotrijebila kao dokaz u sudskom postupku.

2.10. UPRAVLJANJE POSLOVNIM KONTINUITETOM
2.10.1. Stanovišta informacijske sigurnosti pri upravljanju kontinuitetom poslovanja

CILJ	AKTIVNOSTI
Ostvariti protivmjere u slučaju prekida poslovnih aktivnosti te zaštititi ključne poslovne procese od utjecaja velikih zastoja informacionih sistema ili katastrofa i osigurati pravovremen nastavak rada.	- institucija se mora suočiti s rizicima poslovanja i biti spremna primjereno reagirati ukoliko se dogodi incident koji može prouzrokovati zastoj u poslovanju, - identificirati i analizirati događaje, tj. incidentne situacije, koji mogu prekinuti poslovni proces te definirati plan za kontinuirano poslovanje institucije, - kontinuirano sprovoditi ispitivanja kako bi se pravovremeno otkrili propusti uslijed promjena u sistemu, - odrediti potencijalne prijetnje informacionom sistemu institucije, - odrediti koje je mjere moguće primijeniti kako bi se smanjili rizici kojima je izložen informacioni sistem, - primjena provjera za minimiziranje štete nastale prirodnim katastrofama (zemljotresi, poplave, požari, itd.) i - preduzeti sve mjere zaštite i opreza kako korisnici sistema ne bi mogli prouzrokovati prestanak ispravnog rada informacionog sistema.

2.11. USKLAĐIVANJE
2.11.1. Usklađenost sa zakonskim propisima

CILJ	AKTIVNOSTI
Sprječavanje kršenja svih pravnih, zakonskih, regulativnih ili ugovornih obaveza i sigurnosnih zahtjeva.	- definirati odgovarajuća pravila koja će biti u skladu sa zakonskim odredbama koje su vezane uz ugovore o intelektualnom vlasništvu i autorskim pravima,

2.11.2. Usklađenost sa sigurnosnim politikama i standardima i tehnička usklađenost

CILJ	AKTIVNOSTI
Osigurati usklađenost sistema sa organizacionim sigurnosnim politikama i standardima.	- dokumentirati korištenje računarskih resursa u neposlovne ili neovlaštene svrhe kao neprimjereno, - dokumentaciju primjereno zaštititi od gubitka, oštećenja i krivotvorenja.

2.11.3. Razmatranja revizije informacionih sistema

CILJ	AKTIVNOSTI
Povećati efikasnost i smanjiti ometanja od ili prema procesu revizije informacionih sistema.	- korisnike obavijestiti o pravilima o nadgledanju ukoliko zakon tako nalaže.

3. ZAKON I PODZAKONSKI AKTI ZA REALIZIRANJE POLITIKE

Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine će izraditi i dostaviti Vijeću ministara Bosne i Hercegovine na razmatranje i usvajanje slijedeće prijedloge, koji će se odnositi na Institucije:

- Zakon o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema

SVRHA: Ovim Zakonom se utvrđuje pojam informacione sigurnosti, mjere i standardi informacione sigurnosti, područja informacione sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacione sigurnosti.

- Smjernice o informatičkoj sigurnosti radnog mjesta

SVRHA: Smjernice o informatičkoj sigurnosti radnog mjesta namijenjene su korisnicima informacionog sistema institucije s ciljem podizanja svijesti o IT sigurnosti kroz obavljanje svakodnevnih zadataka na računaru, korištenju Interneta, upotrebi elektronske pošte, postupanja sa osjetljivim podacima, korištenjem aplikacija. Korisnici također moraju biti svjesni da upravo oni imaju kritičnu ulogu u održavanju uspješne informacione sigurnosti.

- Smjernice o klasificiranju informacionih resursa

SVRHA: Smjernice o klasificiranju informacionih resursa upućuje korisnike na koji način rukovati pojedinim resursom. Budući da nije moguće za svaki resurs definirati na koji način se prema njemu odnositi u smislu zaštite, nastao je pojam klasificiranje. Cilj klasificiranja je svrstati svaki resurs u pojedinu klasu u zavisnosti o kriterijima klasificiranja. Klasa resursa određuje na koji način je korisnik dužan koristiti resurs, sa kolikom pažnjom i odgovornošću.

- Smjernice o korištenju prijenosnih uređaja

SVRHA: Prijenosni uređaji su sve popularniji. Cjenovno gotovo identični, a praktično dosta ispred desktop računara, postali su česti izbor pri kupovini računarske i elektronske opreme, bilo da se radi o poslovnim ili privatnim korisnicima. Ali, upotreba prijenosnih uređaja od strane zaposlenih, partnera ili drugih korisnika donosi potrebu za implementacijom dodatnih sigurnosnih kontrola. One moraju spriječiti svaku neovlaštenu radnju koja može ugroziti sigurnost informacionog sistema.

- Smjernice o fizičkoj zaštiti informacija

SVRHA: Preventivnim metodama sigurnosti zaštitu sistema institucije od namjernih ili slučajnih destruktivnih radnji. Smjernicama o fizičkoj zaštiti informacija potrebno je:

- spriječiti neovlašteni pristup,
- spriječiti ometanje poslovnih prostorija,
- spriječiti nepotreban pristup korisnika osjetljivoj opremi,
- osigurati zaštitu opreme od prirodnih utjecaja,
- osigurati sigurnost instalacija,
- osigurati održavanje opreme.

- Smjernice o kontroli pristupa i bilježenju događaja

SVRHA: Zasigurno jedan od važnijih uzroka problema sigurnosti predstavljaju ovlašteni korisnici. Oni svojim postupcima, bilo slučajnim ili namjernim, ugrožavaju sigurnost sistema u velikoj mjeri. Neki od uzroka sigurnosnih incidenata od strane ovlaštenih korisnika:

- znatiželja,
- dokazivanje,
- krađa identiteta od strane zlonamjernog lica,
- slučajni postupci (needukovanost korisnika),
- prikupljanje podataka u zlonamjerne svrhe itd.

Navedene prijetnje sigurnosti informacionim sistemima razlog su zbog kojih postoji potreba za kontrolom pristupa, tj. zabranom pristupa onim resursima sistema kojima korisnik nema potrebe pristupati.

Osim kontrola pristupa, u svrhu pravovremenog uočavanja odstupanja od politike pristupa i radi pružanja dokaza u slučaju sigurnosnog incidenta, u sistem je potrebno implementirati sigurnosnu kontrolu bilježenja događaja (nadgledanje).

- Smjernice o upravljanju sigurnosnim incidentima

SVRHA: Bez obzira na sve veća sredstva i napore koji se ulažu u postizanje i održavanje sigurnosti informacionih sistema, sigurnosni incidenti i dalje su česta pojava. Svaki sigurnosni incident bez obzira na veličinu i trajanje za instituciju predstavlja gubitak, zbog čega je vrlo važno da se adekvatna pažnja posveti razvoju strategije i planiranju aktivnosti u slučaju pojave sigurnosnih incidenata. Zbog toga je upravljanje sigurnosnim incidentima važan segment poslovanja svake institucije. Ukoliko

se unaprijed definiraju zaštitne mjere i koraci u slučaju pojave incidenta, znatno se mogu umanjiti gubici i utjecaj incidenta na poslovanje institucije. Kako bi upravljanje sigurnosnim incidentima bilo kvalitetno organizirano, potrebno je definirati:

- odgovornosti i uloge,
- potencijalno opasne radnje,
- procedure u slučaju incidenta,
- procedure za pravovremenu detekciju,
- procedure za analizu incidenta i uklanjanje posljedica,
- procedure za vraćanje sistema u početno stanje.

- Smjernice o upravljanju sigurnosnim zakrpama

SVRHA: Reguliranje procesa otklanjanja skrivenih pogrešaka operativnih sistema i programskih paketa. Pravovremeno otklanjanje postojećih pogrešaka operativnih sistema i programskih paketa sprječavaju moguću štetu zbog širenja virusa, crva, zlonamjernih kodova i ostalih napada na sigurnost, koji za posljedicu imaju smanjenje operativnosti, integriteta i povjerljivosti informacionih sistema.

- Smjernice o korisničkim računima i pravima pristupa

SVRHA: Osigurati kontrolu nad otvaranjem, izmjenom, zamrzavanjem i zatvaranjem korisničkih računa u informacionom sistemu institucije, u cilju sprječavanja zastarjelih, redundantnih i korisničkih računa otvorenih na neispravan način. Drugi dio dokumenta treba da se odnosi na dodjelu prava pristupa. Pravo pristupa vrijednostima informacionog sistema jedna je od najkritičnijih tačaka sigurnosti. Zbog naizgled kompliciranog procesa dodjeljivanja prava pristupa, korisnicima se često dodjeljuju "uobičajna" prava, koja su najčešće puno veća od potrebnih. Što veća prava pristupa korisnik posjeduje, veće su mogućnosti da slučajnim ili namjernim radnjama ugrozi sigurnost informacionog sistema. Iz tog razloga potrebno je ograničiti djelovanje korisnika na način da im se dopusti obavljanje samo onih radnji koje su potrebne za obavljanje njihova poslova.

- Smjernice o sigurnosnim kopijama

SVRHA: Sigurnosne kopije podataka, smještene na informacionim sistemima institucija, rade se u svrhu osiguranja podataka od vitalnog značaja za normalno funkcioniranje institucije. Zadatak sigurnosnih kopija je osigurati oporavak sistema na osnovi autentičnih, cjelovitih i raspoloživih prethodno pohranjenih podataka, u slučaju oštećenja nastalih povredom integriteta podataka uslijed vremenskih nepogoda, potresa, ratnih razaranja, požara, poplave ili havarije samih sistema.

- Smjernice o zaposlenju i prekidu zaposlenja

SVRHA: Definirati slijedeće procedure:

- koje je potrebno preduzeti u pogledu sigurnosti kod zaposlenja, sklapanja ugovora o zaposlenju ili saradnji,
- koje definiraju na koji način kvalitetno provesti prekid zaposlenja ili raskid ugovora.

Cilj navedenih procedura je smanjenje rizika od ljudske pogreške, krađa, prijevara i zloupotrebe resursa informacionih sistema institucije.

- Smjernice za izradu metodologije procjene rizika

SVRHA: Metodologija procjene rizika definira načine određivanja vrijednosti ulaznih veličina na kojima se zasniva procjena rizika. Ulazne veličine pri procjeni rizika su najčešće vjerovatnost (eng. probability) i utjecaj (eng. impact), a mogu biti i mnoge druge. Koje sve ulazne veličine će biti korištene definirano je u svakoj pojedinoj metodologiji. Osim ulaznih veličina metodologijom je određen način izračunavanja nivoa rizika, te kriteriji za određivanje prihvatljivosti, odnosno neprihvatljivosti nivoa rizika.

ZAKLJUČAK

Usvajanjem Politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, stvorit će se pravni osnov za usvajanje međunarodnih standarda iz serije ISO/IEC 27000, zakona i podzakonskih akata o mjerama u ovoj oblasti, standarda za pojedine oblasti, te programa informacione sigurnosti u Bosni i Hercegovini. Također, u cilju potpunog uređenja ove oblasti potrebno je izmijeniti zakone kojim je uređena: elektronska trgovina, elektronski potpis, elektronski dokument i arhivsko poslovanje. Poštujući preporuke i najbolju praksu, zasnovanu na međunarodnim standardima prilikom izrade navedenih propisa, stvara se informaciono-komunikaciona platforma neophodna za saradnju sa svim relevantnim faktorima iz okruženja, u prvom redu sa EU i NATO. Saradnja bazirana na povjerenju koje je normirano i realizirano u svim segmentima informacionog društva ima perspektivu kontinuiranog razvoja i dobrobiti i za građane i za državu. Činjenica da upravljanje informacionom sigurnošću, kao dio ukupne nacionalne sigurnosti, sve više dobija na značaju nameće potrebu njenog daljeg razvoja, kako u teorijskom, tako i u praktičnom smislu. U Bosni i Hercegovini ne postoji dovoljno razvijena svijest o upravljanju informacionom sigurnošću, kao ni organizirana redovna edukacija bilo kojeg nivoa. Podizanje svijesti o potrebi i neophodnosti uvođenja sistema upravljanja informacionom sigurnošću, kao i njeno izučavanje kroz sistem redovnog visokoškolskog obrazovanja ima važnu ulogu u daljem razvoju informacionog društva. S obzirom na kompleksnost, višeslojnost i interdisciplinarnost, obučenost u sferi upravljanja informacionom sigurnošću podrazumijeva određeni fond tehničkih, upravljačkih i specijalističkih znanja. Sa svakim novim dostignućem u oblasti informacionih tehnologija javljaju se novi aspekti informacione sigurnosti, što mora biti propraćeno naučno istraživačkim radom.

Ova politika upravljanja informacionom sigurnošću u sebi sadrži i edukativnu komponentu. Na taj način se htjelo ukazati da svaka institucija mora shvatiti neophodnost i potrebu realiziranja sopstvene politike i uvođenjem sistema za upravljanje informacionom sigurnošću. Da bi se te politike mogle realizirati, neophodno je, paralelno sa normativnim uređivanjem ove oblasti, raditi na programima koji će u narednom periodu podići ukupnu svijest i kreirati neophodnu kadrovsku i naučnu infrastrukturu. Planiranjem mjera i aktivnosti, organiziranjem stručnih debata, sistemskom promocijom novih tehnologija i metoda informacione sigurnosti, kao i ažuriranjem propisa, osigurat će se uvjeti za brzo i kvalitetno priključenje BiH razvijenom svijetu, a time i uvjeti za poboljšanje ukupnog kvaliteta života.

523

Na temelju članka 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08), Vijeće ministara Bosne i Hercegovine na 101. sjednici, održanoj 12.5.2017. godine, donijelo je

RJEŠENJE
O RAZRJEŠENJU ZAMJENIKA DIREKTORA SLUŽBE ZA POSLOVE SA STRANCIMA

1. **Izet Nizam**, razrješava se dužnosti zamjenika direktora Službe za poslove sa strancima, sa danom 15.5.2017. godine.
2. Ovo rješenje stupa na snagu danom donošenja i objavljuje se u "Službenom glasniku BiH".

VM broj 78/17
12. svibnja 2017. godine
Sarajevo

Predsjedatelj
Vijeća ministara BiH
Dr. **Denis Zvizdić**, v. r.