UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Damjan Košćak

Varovanje informacij v skladu s standardom ISO/IEC 27000

DIPLOMSKO DELO

NA VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

Mentor: viš. pred. dr. Damjan Vavpotič

Ljubljana, 2011

Univerza
v Ljubljani
Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00062/2011

Datum: 01.02.2011

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **DAMJAN KOŠĆAK**

Naslov: **VAROVANJE INFORMACIJ V SKLADU S STANDARDOM ISO/IEC 27000**

INFORMATION SECURITY IN ACCORDANCE WITH ISO/IEC 27000

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

V okviru diplomskega dela predstavite področje varovanja informacij v podjetjih in se v sklopu tega še posebno posvetite družini standardov ISO/IEC 27000. Naloga naj vključuje teoretični in praktični del. V teoretičnem delu okvirno predstavite vsebino standardov ter temeljne pojme na področju varovanja informacij. Nato pa se v drugem delu posvetite prikazu uporabe standardov v praksi. V okviru tega na primeru manjšega izbranega podjetja analizirajte skladnost obstoječih varnostnih postopkov z omenjenimi standardi in na podlagi zaznanih odstopanj izdelajte predlog za izboljšanje stanja.

Mentor:

viš. pred. dr. Damjan Vavpotič

Dekan:

prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko
UNIVERZA V LJUBLJANI
2

I Z J A V A   O   A V T O R S T V U

diplomskega dela

Spodaj podpisani/-a Damjan Košćak,

z vpisno številko 63070431,

sem avtor/-ica diplomskega dela z naslovom:

Varovanje informacij v skladu s standardom ISO/IEC 27000

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom (naziv, ime in priimek)

  viš. pred. dr. Damjan Vavpotič

  in somentorstvom (naziv, ime in priimek)

  /

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela

- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne maj, 2011 Podpis avtorja/-ice:

Zahvala

Za vsestransko podporo, strokovno pomoč in nasvete pri izdelavi diplomske naloge bi se rad zahvalil mentorju, viš. pred. dr. Damjanu Vavpotiču. Prav tako hvala vsem domačim za dolgoletno podporo in spodbudo pri študiju. Najlepša hvala tudi direktorju podjetja ter vsem iz podjetja, ki so mi pomagali pri diplomski nalogi. Za strokovno lektoriranje naloge se zahvaljujem mag. prof. Nataši Koražiji.

Kazalo vsebine

Kazalo grafov

Kazalo slik

Kazalo prilog

Seznam uporabljenih kratic in simbolov

AAA – Authentication, authorization, and accounting

BS – British Standard

COBIT – Control Objectives for Information and related Technology

CVS – Concurrent Versions System

DNS – Domain Name System

GIS – Geographic information system

IDS – Intrusion Detection Systems

IEC - International Electrotechnical Commission

IS – Information systems

ISACA – Information Systems Audit and Control Association

ISO – International Organization of Standardization

IT – Information technology

ITIL – Information Technology Infrastructure Library

NAT – Network address translation

OIS – Občinski informacijski sistem

P2P – Peer-to-peer

SMS – Short Message Service

SUVI – Sistem za upravljanje varovanja informacij

SQL – Structured Query Language

SSH – Secure Shell

SSL – Secure Sockets Layer

UPS – Uninterruptible power supply

URL – Uniform Resource Locators

VPN – Virtual private network

ZIL – Zaščita intelektualne lastnine

Povzetek

Diplomska naloga obravnava varnost informacijskih sistemov z vidika standarda ISO/IEC 27001 in ISO/IEC 27002.

Diplomsko nalogo sestavljata dva dela. Prvi del predstavlja teoretične osnove varovanja informacij. Drugi del pa predstavlja vpeljavo varnostnega standarda ISO/IEC 27001 v podjetju »X«, v katerem sem opravljal praktično izobraževanje. V zaključku nadgradim nalogo tako, da se soočim s pridobljenimi rezultati raziskovalne naloge in z opravljeno analizo predlagam izboljšave in ukrepe.

Ključne besede

ISO/IEC 27000, informacijska varnost, varnostna politika, standardi varovanja informacij, vdori.

Abstract

The diploma assignment discusses Information Technology Security according to standards ISO/IEC 27001 and ISO/IEC 27002.

Diploma consists of two parts. In the first part of the diploma a theoretical bases of information security are presented. The second part presents the introduction of ISO/IEC 27001 security standard in the company »X« in wich I performed a practical training. In the closure my diploma work is upgraded with results of my research work and their analysis as well as with my proposals for improvements.

Keywords

ISO/IEC 27000, information security, security policy, security standards, intrusions.

1. Uvod

Informacije so postale del našega vsakdanjika na vseh področjih, tako v zasebni sferi kot tudi v poslovnem svetu. Ker predstavljajo zelo pomemben dejavnik delovanja združbe, je potrebno dodeliti posebno pozornost njihovemu varovanju.

Z informacijsko tehnologijo (IT) se srečujemo v osebnem življenju, kot tudi v podjetju, v katerem delamo. Informacijska tehnologija je tisti ključni dejavnik, za katerega bi lahko rekli, da narekuje način in tempo delovanja, bodočega razvoja ter obstoja združbe. Vodilni v podjetju se problemov informacijske varnosti največkrat sploh ne zavedajo in tako se z informacijsko varnostjo v glavnem ukvarjajo tehniki. Varnost, ki jo lahko dosežemo s tehničnimi sredstvi, je omejena in jo je zato potrebno ustrezno upravljati.

Cilj diplomske naloge je predstaviti grožnje informacijske varnosti, ukrepe zoper grožnjam informacijske varnosti, varnostne informacijske standarde, kot so ITIL, COBIT ter serija standardov ISO/IEC 27000, ter analizirati stanje informacijske varnosti v organizaciji in navesti predloge za izboljšanje stanja.

Zaradi varovanja informacij sem se pri pisanju praktičnega dela diplomske naloge moral omejiti na podjetje »X«, ki pa v resnici obstaja in posluje, v njem sem tudi opravljal praktično izobraževanje. Poskušal se bom izogibati kakršnih koli podatkov, na podlagi katerih bi se lahko ugotovila identiteta združbe.

2. Splošno o varovanju informacij

2.1 Uvod

Poglavje opredeljuje splošne pojme, pomembne za varovanje informacij, kot so razlike med informacijo in sporočilom, prikazuje značilnosti informacijskega sistema, pojem ranljivosti in varnosti. Prikazana je tudi kratka zgodovina interneta in vpliva njegove rasti na informacijsko varnost. Kot osnovo za opredelitev pojmov smo vzeli različne standarde s tega področja [12, 14] in drugo razpoložljivo literaturo [3, 6, 7, 9, 11], za opis samega interneta pa ustrezno literaturo [8, 10].

2.2 Informacija in lastnosti informacije

Informacija je rezultat procesa interpretacije podatkov. Je obratno sorazmerna verjetnosti pojava določenega dogodka oziroma podatka – manjša ko je verjetnost pojava, tem večja je informacija ob določenem dogodku – podatku.

Informacija je rezultat procesiranja, upravljanja in organiziranja podatkov na način, ki prejemniku informacije omogoča boljše razumevanje in poznavanje določene tematike.

Informacije imajo lahko različne oblike. Lahko so natisnjene ali napisane na papir, lahko so v elektronski obliki, lahko se pošiljajo po pošti ali preko elektronskih kanalov, prikazane na filmu, lahko pa je oblika govorne narave.

Če naj sporočila postanejo informacije, morajo biti predvsem:

- pravočasna,
- zanesljiva,
- natančna,
- jedrnata,
- pomembna,
- celovita.

2.3 Informacijski sistem

Sistem pomeni urejeno celoto elementov, v kateri vladajo določene zakonitosti.

Komunikacijski sistem je namenjen za pravočasno dostavljanje ustreznih sporočil nosilcem nalog v svoji in drugih organizacijskih enotah, ki ga zaradi uresničevanja smotra in izvedenih ciljev vzpostavljamo v združbi. Tako naravnan komunikacijski sistem, ki vključuje tudi zbiranje, obdelavo in hranjenje sporočil, v združbi imenujemo informacijski sistem združbe, saj med sporočili, ki jih posreduje, prevladujejo informacije.

Sam informacijski sistem združbe lahko opredelimo kot z oddajniki, prejemniki in potmi sporočil vgrajeno namensko pridobivanje, oblikovanje, oddajanje in sprejemanje sporočil na delovnih mestih ravnateljev ter izvajalcev in na drugih mestih odločanja v združbi v skladu z vlogo posameznikov in skupin, določeno s predpisi, ter hranjenje podatkov.

Sodobno zasnovan informacijski sistem omogoča:

- hitrejše in bolj kakovostno delo,
- boljše odločanje, ker poišče, generira, predstavi podatke, ki tvorijo informacijsko podlago za odločanje in boljšo uporabo znanja pri tem,
- boljšo komunikacijo znotraj organizacije, med organizacijami in njenim okoljem.

Računalniški informacijski sistem ima dva dela. Prvi del je sistem za obravnavanje podatkov, s katerim opravljajo rutinske, centralizirane naloge. Drugi del je sistem za podporo odločanju, ki ravnateljem omogoča dostop do različnih virov informacij in njihovo ustvarjalno uporabo.

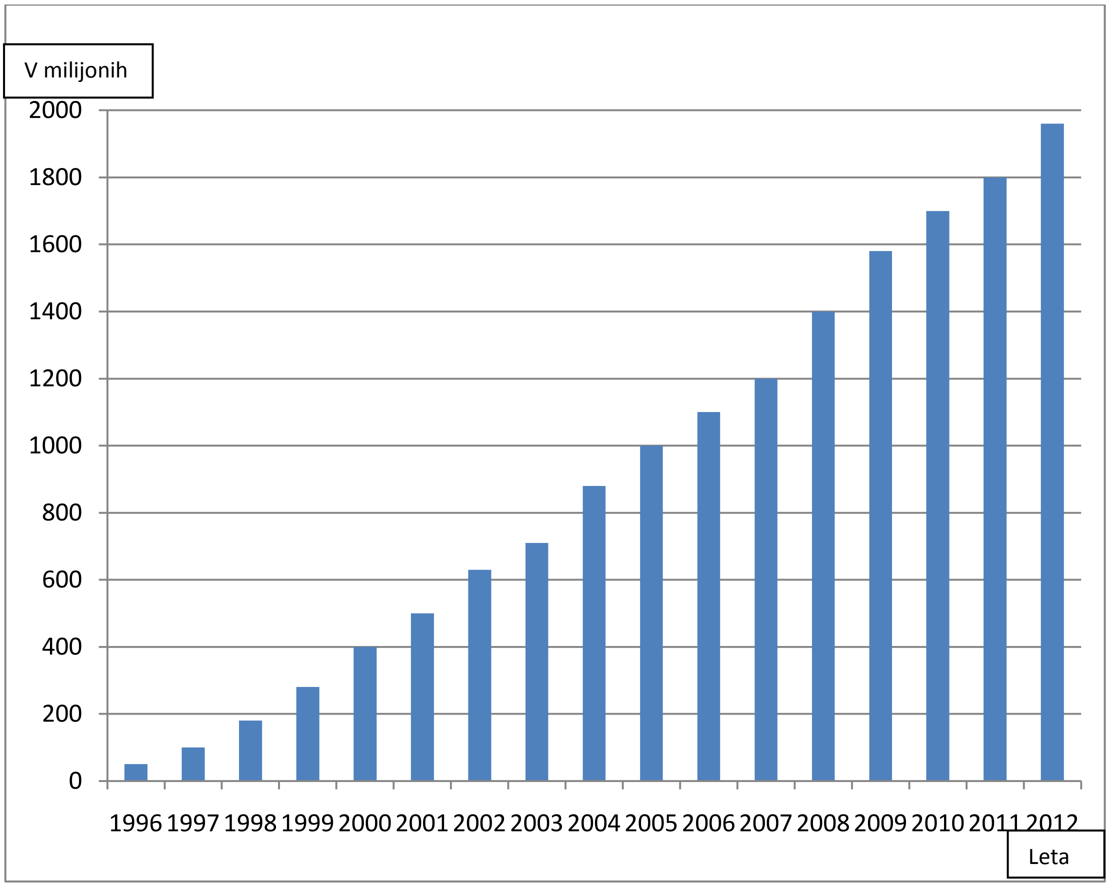
Elemente informacijskega sistema lahko razdelimo na 7 vsebinskih sklopov:

- vhodni del, ki predstavlja množico vnosnih obrazcev, prek katerih poteka vnos podatkov;
- metode, ki predstavljajo sklop proceduralnih, logičnih ali matematičnih metod, s katerimi se obdelujejo podatki, da bi prišli do želenih rezultatov;
- tehnična sredstva, ki omogočajo dejansko transformacijo podatkov;
- podatkovna baza, ki hrani podatke v določeni podatkovni strukturi;
- izhodni del, ki mora prikazovati izhodne informacije;
- kontrolni mehanizmi informacijskega sistema, ki morajo zagotavljati preverjanje vhodnih podatkov in izločati tiste nepravilne vnosne podatke, ki so nepotrebni ali napačni;
- ljudje, ki skrbijo in upravljajo z informacijskim sistemom ter uporabljajo izhode informacijskega sistema. Ločimo dve vrsti: uporabniki in informatiki. Informatiki skrbijo za razvoj, izvedbo in vzdrževanje informacijskega sistema, medtem ko so uporabniki tisti, ki jim je sistem namenjen in ga uporabljajo.

2.4 Kratka zgodovina interneta in izziv varovanja informacij

Internet je globalno omrežje, ki ga sestavljajo različna računalniška omrežja, v katerem milijonom računalnikom omogoča vsakodnevno medsebojno komunikacijo.

Sprva je bil internet namenjen uporabnikom, kateri se med seboj poznajo in zaupajo. Z naglim večanjem priljubljenosti interneta se je povečalo tudi število uporabnikov, kar je zrušilo model zaupanja. Uporabniki so postali žrtve posameznikov z naprednejšim znanjem (imenujemo jih hekerji), s katerim so izkoriščali sistem. Z razvojem spletnih brskalnikov v začetku 90. let se pojavilo ogromno novosti. Spletne strani so poleg besedila vsebovale tudi slike, zvoke, animacije in video posnetke. Priljubljenost interneta je zaradi brskalnikov še bolj naraščala. Graf 1 prikazuje skupno število uporabnikov interneta.



Graf 1: Rast števila uporabnikov interneta skozi čas.

Podjetja so kmalu začela uporabljati internet kot nov medij za komuniciranje s strankami. Tako je internet prerasel svoj prvotni namen, ki je bil samo posredovanje informacij med akademskimi in vladnimi organizacijami. Odprtost interneta je podjetjem veliko pomagala pri uporabi internetne tehnologije, hkrati pa je bila ravno ta odprtost, gledano z vidika varovanja informacij, največja slabost.

Prvi pomembnejši napad je bil črv[1] Morris, ki je leta 1988 za nekaj ur onesposobil približno 5000 strežnikov. Od takrat pa se je zvršilo že veliko varnostnih incidentov, ki so jih povzročili virusi, črvi in druga zlonamerna programska oprema. Danes podobni napadi povzročajo na milijone dolarjev škode, saj je njihov glavni cilj onemogočiti internetno povezavo določenega spletnega mesta.

Danes je pomemben elektronski način za poslovanje s sedanjimi in prihodnjimi strankami. Čeprav ima glede tega internet velike prednosti, so zanj značilne tudi velike varnostne slabosti, ki jih podjetja prezirajo ali podcenjujejo v lastno škodo.

---

[1] Zlonamerna programska koda.

2.5 Varnost

Eden izmed razlogov za skrb je, da so vse sodobne organizacije odvisne od podatkov, ki jih hranijo informacijski sistemi. Zbirke podatkov so v ozadju informacijskih sistemov, od katerih je odvisno naše vsakdanje življenje.

Ravno zaradi tega je varovanje informacij zelo pomembno, saj zaščita informacij pred raznimi vrstami groženj, da se zagotovi neprekinjeno poslovanje, zmanjša poslovno tveganje ter se doseže kar največji dohodek iz naložb in poslovnih možnosti.

Varnost informacij dosežemo z vpeljavo ustreznih kontrol, vključno s politikami, procesi, postopki, organizacijskimi strukturami ter funkcijami programske in strojne opreme. Te kontrole je treba vzpostaviti, vpeljati, spremljati, pregledovati in, kjer je potrebno, izboljšati za zagotovitev, da so izpolnjeni specifični varnostni in poslovni cilji organizacije.

Varnost je v bistvu izključevanje nevarnosti. Govoriti o varnosti je zelo težko, če ne celo nesmiselno, če ne znamo ali ne moremo opredeliti nevarnosti.

Dejstvo je, da absolutno varnega sistema ni. Stopnja varnosti je odvisna od tega, koliko se ukvarjamo s tistimi nevarnostmi, ki nam objektivno grozijo, in ne kar na splošno z nekim imaginarnim notranjim, zunanjim ali kakršnimkoli sovražnikom. Ne smemo pa pozabiti, da je napadalec v končni fazi vedno človek.

Varovanje mora biti usmerjeno v preprečevanje potencialno možnih nevarnosti. Veliko teh nevarnosti lahko predvidimo in identificiramo s kakovostnim in zanesljivim nadzorom sistema.

Podjetja se morajo zavedati šestih pomembnih nevarnosti in jih upoštevati. Te pomembne nevarnosti so:

- Zahteve pri e-poslovanju – internet je omogočil pomembno poslovno pot, ki ji pravimo elektronsko poslovanje. To je podjetjem omogočilo veliko novih načinov ponujanja izdelkov in storitev svojim strankam preko interneta.
  Zaradi povečanja obsega poslovanja pa so podjetja pod velikim pritiskom, ker morejo nove sisteme izdelati čim prej. Podjetja morajo tudi hraniti zaupne podatke, kot so domači naslovi in številke kreditnih kartic strank, kar lahko predstavlja tarčo napada za napadalca.
- Napadi na varovane informacije – varnostni incidenti, ki jih povzroča zlonamerna koda, so zrasli iz rahlo nadležnih v zelo škodljive za poslovanje.
  Zgodnji računalniški virusi[2] so bili pogosto omejeni na sisteme z enim uporabnikom. Danes pa obstajajo tudi mešane grožnje, ki pomeni več groženj hkrati in povzročajo

[2] Zlonamerna programska koda.

velike motnje v poslovanju ter škodo v milijardah dolarjev. Mešane grožnje združujejo različne vrste zlonamerne kode in tako izkoriščajo znane varnostne luknje.

- Nezrelost trga varovanja informacij – dejstvo je, da so ustvarjalci zlonamerne programske kode vedno korak pred industrijo varovanja informacij. Še dodaten izziv pa je razmeroma nizka stopnja pomembnosti, ki jo industrija programske opreme namenja varnosti.
- Pomanjkanje strokovno usposobljenega osebja za varovanje informacij – zaposlitev strokovnjakov za varovanje informacij je težka naloga, ki bo po vsej verjetnosti ostala taka tudi v prihodnje. Podjetja bodo morala v to področje vlagati več, če bodo želela rešiti omenjeno težavo.
- Vladna zakonodaja in industrijski pravilniki – podjetja morajo upoštevati, da so zakoni pogosto napisani za točno določeni dve državi in da se elektronsko poslovanje izvaja globalno. Takoj ko začne podjetje za poslovanje uporabljati internet, začne poslovati globalno. Zaradi tega je lahko podjetje ob upoštevanju predpisov ene države v konfliktu s predpisi druge države, če ti predpisi niso poenoteni.
- Mobilna delovna sila in brezžična omrežja – z brezžičnimi napravami sta se razpoložljivost informacij in komuniciranje še bolj razširila. Take naprave so zelo praktične, pri tem pa je treba še bolj poskrbeti za varnost zaupnih informacij, ki so shranjene v njih.

2.6 Ranljivost

Ranljivost informacijskega sistema je vsaka pomankljivost informacijskega sistema, ki jo lahko določena grožnja izrabi. Je posledica slabe zaščite informacijskega sistema zoper določeno grožnjo ali aktivnosti napadalca. Ranljivost sama po sebi ne povzroča škode, je zgolj stanje ali serija stanj, ki dopušča, da grožnja vpliva na informacijski sistem.

3. Grožnja varnosti informacijskemu sistemu

3.1 Uvod

Poglavje zajema obsežen pregled nad možnimi grožnjami, ki ogrožajo informacijski sistem. Izvor teh groženj so lahko izredni dogodki, naključni dogodki in dejavnosti človeka. Opisane so tudi varnostne tehnologije zoper grožnjam informacijske varnosti. Kot osnovo za opredelitev izrednih dogodkov, naključnih dogodkov, dejavnosti človeka in varnostne tehnologije je uporabljen standard s tega področja [12], razpoložljiva literatura [1, 5, 7, 8,10] in internetni viri [18, 19, 21].

3.2 Splošno o grožnji varnosti

Grožnja varnosti informacijskemu sistemu je neželen dogodek ali dejavnost, ki privede do izgube celovitosti, zaupnosti ali razpoložljivosti informacij in onemogoča zadovoljivo delovanje informacijskega sistema.

Posledica takega dogodka je lahko velika finančna izguba v organizaciji. Intenzivnost posledic groženj pa se razteza od nizke, to je na primer izguba kakega manj pomembnega dokumenta, do katastrofalnih posledic, kar bi bilo uničenje informacijskega sistema.

Vse grožnje je potrebno čim bolje predvideti in napisati spisek ukrepov, ki jih je potrebno izvesti v primeru, če se katera izmed groženj uresniči. Če pa se kljub ukrepom uresničijo, moramo v najkrajšem možnem času grožnjo odstraniti.

Grožnje glede na njihov izvor lahko delimo na izredne dogodke, naključne dogodke in dejavnosti človeka.

3.3 Izredni dogodki

Izrednih dogodkov, kot so požari, poplave, potresi, strele, izpadi ali nihanja električne energije, vnaprej ne moremo napovedati niti nanje ne moremo bistveno vplivati. Večina naštetih lahko popolnoma uniči informacijski sistem organizacije.

3.3.1 Požar

Požar predstavlja zelo veliko grožnjo informacijskemu sistemu, saj so posledice lahko katastrofalne. Lahko povzroči uničenje cele organizacije ali njenega dela. Požar lahko nastane kot posledica človekove namerne ali nenamerne dejavnosti, pa tudi kot posledica naravne katastrofe.

Zato so varovalni ukrepi za preprečitev požara nujni, da se zavaruje pred katastrofo. Taki ukrepi so:

- nevarni in gorljivi materiali morajo biti shranjeni na varni razdalji, stran od varovanih območij, in s protipožarnim zidom. Preseženi materiali, kot so pisarniški pripomočki, naj se ne shranjujejo na varovanem območju,
- v prostoru mora biti nameščen avtomatiziran protipožarni sistem,
- organizacija mora imeti ustrezno gasilsko opremo, ki naj bo primerno nameščena,
- v prostoru je prepovedano kajenje,
- zaposleni so seznanjeni s protipožarnimi ukrepi in usposobljeni za uporabo gasilnih aparatov.

3.3.2 Poplave

Možnost izliva vode upoštevajo le redki. Dragocene informacijske vire, kateri niso dvignjeni od tal, lahko počena vodovodna cev dokaj hitro zalije. Še posebej je to nevarno v nočnem času, ko nihče ne more ukrepati. Poleg vode škodijo informacijskim tehnologijam tudi druge tekočine. Neredki so primeri, ko uporabnik po tipkovnici ali prenosniku polije kavo ali kakšno drugo tekočino.

Voda lahko na strojni opremi, programski opremi in podatkih naredi ogromno škode, med katerim je potrebno poudariti delno in popolno nerazpoložljivost sistema, uničenje ali poškodbo. Možni varovalni ukrepi zoper poplavam so:

- naprave za obdelavo informacij niso na tleh,
- strop je brez vodnih instalacij,
- predvidena je možnost hitrega odstranjevanja vode iz prostora,
- strop je brez odprtin, kjer bi voda lahko prodrla v prostor.

3.3.3 Prekinitve električnega toka

Posledice izpada električne energije so lahko izguba ali uničenje podatkov, poškodbe strojne opreme ali škoda, ki nastane zaradi nerazpoložljivosti sistema. Varovalni ukrepi za zaščito so:

- opremljenost s sistemom za brezprekinitveno napajanje UPS,
- rezervni generator, če je treba nadaljevati z delom tudi v primeru daljše prekinitve v oskrbi z električno energijo,
- varnostna stikala, da se v primeru sile omogoči hitra prekinitev električnega toka.

3.4 Naključni dogodki

Naključni dogodki so predvsem odpovedi, kot so odpoved strojne opreme, programske opreme ali človeka.

3.4.1 Odpoved strojne opreme

Grožnje odpovedi strojne opreme so predvsem računalniški sistemi, kot so strežniki, namizni in prenosni računalniki, ostali gradniki ter posledično podatki in informacije. Možne posledice ob tej grožnji so izguba ali popačenje podatkov in informacij, poškodba strojne opreme ter delna ali popolna nerazpoložljivost sistema. Vzroki za takšne odpovedi so največkrat komponente, izdelane iz slabših materialov, staranje materialov, napačna raba, nepravilno vzdrževanje, nezdružljivost opreme, pregretja, tresljaji, vlage in udarci. Delna odpoved strojne opreme je redka, a zelo kritična. Takrat naprava deluje, a rezultati obdelav so lahko napačni. Možni ukrepi zavarovanja pred tovrstno grožnjo so lahko:

- pazljivo ravnanje s strojno opremo,
- učinkovito preventivno in korektivno vzdrževanje,
- uvedba redundančnih delov za kritične gradnike,
- vzdrževanje naj izvaja pooblaščeno osebje,
- uporaba klimatskih naprav v prostorih.

3.4.2 Odpoved programske opreme

Programsko opremo sestavlja vrsta različnih programov, med katerimi vsak opravlja določeno funkcijo. Sem spada tudi operacijski sistem, brez katerega računalnik sploh ne bi deloval. Nerazpoložljivost programske opreme, izguba ali popačenje podatkov in informacij ter delna ali popolna nerazpoložljivost sistema je pogosto posledica te varnostne grožnje. Varnostni ukrepi, ki jih lahko uvedemo zoper te vrste grožnje, so:

- testiranje prepustimo najboljšim programerjem,
- avtor programa se izogiba testiranju lastnega programa,
- redno nadgrajevanje in posodabljanje,
- izobraževanje zaposlenih.

3.4.3 Napake človeka

Napake človeka, ki so posledica neusposobljenosti, neizkušenosti ali psihičnih in fizičnih preobremenitev, so vzrok odpovedi sistema. Pri tem se lahko povzroči materialna škoda, škoda na zdravju posameznika ali celo smrt. Varnostni ukrepi, ki pripomorejo oblažiti tovrstno varnostno grožnjo, so:

- zagotoviti normalo delovno obremenitev zaposlenih,
- redno usposabljanje zaposlenih,
- čas za prehrano, počitek.

3.5 Namerne dejavnosti človeka

Varnost organizacije je v mnogih primerih ogrožena s strani zaposlenih in ljudi, ki sodelujejo z organizacijo kot pogodbeni sodelavci ali stranke. Kazniva dejanja, storjena s pomočjo računalniške, informacijske in komunikacijske tehnologije, so v velikem razmahu. Zato preverjanje preteklosti ne bi smeli omejiti samo na zaposlene v tem podjetju, ampak bi jo morali izvajati tudi na zunanjih izvajalcih.

V primeru prekinitve sodelovanja z zaposlenim morajo biti natančno določeni postopki, po katerih se ravnamo, saj lahko zaposleni, ki odhaja iz organizacije, povzroči veliko škodo.

V nadaljevanju so opisane najpomembnejše tovrstne grožnje.

3.5.1 Kraja, vlom

Kraja je resna varnostna grožnja vsem sredstvom podjetja. S krajo si lahko nepooblaščena oseba pridobi občutljive podatke in informacije ter organizaciji povzroči gmotno materialno škodo. Možna preventivna dejanja, ki pomagajo onemogočiti to grožnjo, so:

- prostor je lociran tako, da je normalen dostop omogočen samo pooblaščenim osebam,
- potrebne so fizične pregrade, kjer je to mogoče, da se prepreči nepooblaščen fizični dostop,
- organizacija mora imeti recepcijo ali drug način fizične kontrole dostopa v prostor ali zgradbo; dostop v prostor ali zgradbo mora biti omejen le na pooblaščeno osebje,
- zmogljivosti za obdelavo informacij, ki jih upravlja organizacija, morajo biti fizično ločene od zmogljivosti, ki jih upravlja tretja stranka,
- varovano območje, kot je zaklenljiva pisarna ali več sob, obdanih z neprekinjeno notranjo fizično pregrado,
- nameščen alarmni sistem,
- vhod v pomembnejše prostore naj bo zaščiten z dodatno avtentikacijo (gesla, kartice, biometrija ...).

3.5.2 Destruktivno dejanje

Je vrsta grožnje, pri kateri želi nekdo znotraj organizacije namerno povzročiti škodo. S povzročeno škodo se lahko okoristi ali pa tudi ne. Nekateri ljudje so nagnjeni k temu, da povzročajo škodo, pa naj bo to namerno ali nenamerno. Posledice teh vrst groženj so uničenje ali popačenje sredstev, delna ali popolna nerazpoložljivost sistema, nepooblaščeno razkritje podatkov. Varovalni ukrepi so lahko:

- beleženje prihoda in odhoda obiskovalcev, vse obiskovalce je treba nadzorovati, če nimajo predhodno odobrenega dostopa,
- pravice do dostopa na varovana območja je treba redno pregledovati in dopolnjevati ter jih preklicati, kadar je to potrebno,
- pomembne prostore zaščitimo z video nadzorom.

3.5.3 Logični vdori

Nepooblaščen dostop do sistema in podatkov v sistemu je možen preko programskih vsiljivcev in programov bodisi z neposredno aktivnostjo napadalca. Ta dejanja lahko napadalcem predstavljajo izziv, lahko samo kot dokazovanje v »hekerski druščini«, nekateri pa hočejo dobiti razne podatke iz sistema. Posledice teh groženj so lahko nepooblaščeno razkritje podatkov in informacij, njihova nepooblaščena sprememba ali uničenje.

Ker je tak vdor v računalniški sistem običajno povezan z veliko znanja in vloženega truda, napadalci po uspešnem vdoru naredijo vse, da bi do takega sistema lahko imeli prikrit dostop tudi v prihodnje. Možni varovalni ukrepi so:

- uvedba varnostnih gesel,
- sistemi za zaznavanje logičnih vdorov – IDS,
- omejitve dostopov uporabnikom ob določenih urah izven rednega delovnega časa,
- vodenje in analiziranje dnevniških zapisov varnostne tehnologije o vseh uporabnikih, ki so uporabljali sistem, in o vseh spremembah podatkov in programov, ki so jih naredili,
- strojne in programske požarne prepreke,
- redno posodabljanje programske opreme.

3.5.4 Virusi

Računalniški virusi so najbolj znana skupina zlonamerne kode, ki se lahko razmnožujejo in širijo podobno kot biološki virusi.
Računalniški virus se pripne ali okuži izvršne programske datoteke. V primerjavi s črvi mora z virusom okužene datoteke zagnati uporabnik, ki s tem povzroči razmnoževanje virusa ali aktiviranje njegovega tovora. Tovor, ki ga nosi virus, lahko zbriše podatke ali poškoduje

sistemske datoteke. Glede na nevarnost za računalniške sisteme ločimo več vrst virusov: od takih, ki zaigrajo glasbo, do takih, ki prikažejo spremenjeno sliko na ekranu, do upočasnitve delovanja sistema in do takih, ki spreminjajo podatke ali jih celo zbrišejo.

Zgodnji računalniški virusi so bili pogosto omejeni na sisteme z enim uporabnikom. Posledica je bila samo rahlo zmanjšana produktivnost osebja za kak dan ali dva. Današnji računalniški virusi pa povzročajo velike motnje v poslovanju ter škodo v milijardah dolarjev.

3.5.5 Črvi

Računalniški črvi za razliko od virusov za svoje delovanje ne rabijo gostiteljskega programa. Znajo se širiti kar sami, brez potrebne ročne pomoči. Črvi izdelajo svoje kopije in za širjenje izkoriščajo obstoječe povezave med računalniki. Črvi se hitro razmnožujejo, porabljajo sredstva, upočasnijo delovanje računalnikov in omrežij, da se skoraj ustavijo, ali pa povzročijo celo popolno sesutje omrežja.

3.5.6 Trojanski konji

Trojanski konj (poimenovan po trojanskem konju iz grške mitologije) je neavtorizirana koda, priključena legalnemu programu, ki izvaja neznane in za uporabnika neželene operacije. Trojanski konji potrebujejo za zagon program, h kateremu so pripeti. Posledice trojanskega konja so kraja ali brisanje podatkov, namestitev stranskih vrat, preko katerih hekerjem omogočijo prevzem nadzora nad sistemom. V primerjavi z virusom se trojanski konji ne razmnožujejo.

3.5.7 Vohuni

Vohun (spyware) je vsaka programska oprema, ki je običajno pripeta kot skrita komponenta shareware[3] ali freeware[4] aplikacijam, ki so prenesene z interneta. Vohun je lahko tudi na spletnih straneh. Ob obisku teh strani se lahko namesti na računalnik. Najpogosteje se naselijo kar preko priponk. Vohun poskuša pridobiti informacije iz žrtvinega računalnika brez uporabnikovega dovoljenja, običajno v oglaševalske namene. Ko je vohun enkrat nameščen v žrtvinem računalniku, spremlja internetne aktivnosti uporabnika in nato sporoča te informacije napadalcu. Posledice te vrste grožnje so v najboljšem primeru le upočasnitev delovanja računalnikov v podjetju in internetne povezave. V najslabšem primeru pa lahko tretjim osebam odkrije zaupne podatke, kot so gesla, številke kreditnih kartic, naslovi elektronske pošte.

---

[3] Preizkusni program.
[4] Zastonj program.

Piškotki so ena vrsta vohunov. So majhne datoteke, ki jih spletna stran namesti na uporabnikov računalnik, tako da lahko ob naslednjem obisku prikaže personalizirano vsebino.

3.5.8 Spam (neželena e-pošta)

Spam je pošiljanje enakih ali podobnih sporočil na veliko število naslovov. Takšna sporočila pošiljajo spamerji, ki naslove prejemnika pridobivajo s forumov, spletnih strani, podatkovnih baz, P2P[5] omrežjih ali pa jih preprosto uganejo s kombiniranjem pogostih uporabniških imen in domen.

3.5.9 Socialni inženiring (manipulacija)

Podjetja se premalokrat zavedajo, da je človek in človeški faktor odločilnega pomena v varnem poslovanju podjetja.

Podjetja zapravijo ogromno časa in denarja za zaščito svojega poslovanja, svoje informacijske infrastrukture, omrežij z raznimi nadgradnjami, popravki, varnostnimi paketi in enkripcijskimi algoritmi. V resnici pa je najšibkejši člen prav človek.

Gre za metodo, s katero napadalec prodre v varovano omrežje. V tej zvrsti napada igra glavno vlogo človek, ki zaradi pomanjkanja računalniškega znanja in zaupanja napadalcu omogoči vstop v omrežje.

Najbolj razširjene tehnike socialnega inženiringa so pregledovanje smeti, gledanje čez ramo, internet, ribarjenje, pharming, elektronska pošta, prepričevanje. Večina takih napadov izkorišča prirojeno človekovo pripravljenost pomagati osebi v nesreči, neizobraženost in naivnost.

Najboljša obramba pred takimi napadi je redno osveščanje in usposabljanje zaposlenih.

Kot komunikacijsko sredstvo uporablja socialni inženir v večini primerov telefon, SMS, elektronsko pošto, faks, internet ter spletne klepetalnice.

V nadaljevanju sledi podrobnejši opis tehnik socialnega inženiringa, saj menim, da je tej vrsti grožnje potrebno nameniti več pozornosti.

[5] Medsebojna neposredna komunikacija med vozlišči.

a) Pregledovanje smeti

Veliko informacij lahko socialni inženirji pridobijo z brskanjem po smeteh. V smeteh podjetij se lahko najde naslove zaposlenih, dokumenti, telefonski imeniki, organizacijske sheme, navodila, pravilniki, diskovne naprave, arhivske kasete, zgoščenke in uporabniška gesla. Vse naštete stvari lahko predstavljajo vire socialnemu inženirju.

b) Gledanje čez ramo

Socialni inženir opazuje čez žrtvino ramo podatke, ko se žrtev prijavlja v poslovni sistem. Podatke, ki pomenijo koristno informacijo, na primer uporabniško ime in geslo, si socialni inženir zapomni in se z njim okoristi.

c) Internet

Internet predstavlja glavno komunikacijsko središče moderne dobe. Na spletu se puščajo osebni podatki, poštni naslovi, gesla itd. Napaka, katero uporabniki pogosto delajo, je uporaba preprostih gesel in enakih uporabniških imen. Ko napadalec pridobi geslo uporabnika, lahko z njim zlorablja več storitev uporabnika.

d) Ribarjenje (phishing)

Ribarjenje je nezakonit način zavajanja uporabnikov, pri katerem poskuša prevarant s pomočjo lažnih spletnih strani in elektronskih sporočil od uporabnikov izvabiti njihove osebne podatke. Napadalec v tem primeru izdela natančno kopijo spletne strani in jo namesti v strežnik, ki ga nadzoruje. V naslednjem koraku napadalec pošlje večjo količino elektronskih sporočil svojim žrtvam, pri čemer sporočila ponaredi v obliko, ki je podobna sporočilom originalne spletne strani. Ko žrtev vnese pristopne podatke, jih napadalec zajame in zlorabi.

Tudi socialna omrežja so največkrat izvor ribarjenja za osebnimi podatki.

e) Pharming napadi

Napadi pharming so za uporabnika zelo nevarni, saj jih je težko prepoznati. Glavna razlika med phishingom in pharmingom je v tem, da gre pri pharmingu bolj za tehnični napad kot za tehniko socialnega inženiringa, na katerem temelji ribarjenje podatkov. Praviloma gre pri pharming napadih bodisi za neposreden napad na DNS strežnik bodisi za napad na določeno datoteko, ki se nahaja na računalniku uporabnika. Uporabnik je v teh primerih prepričan, da se nahaja na pravi strani, saj je vtipkal pravi URL naslov strani, v resnici pa je na lažni strani. Uporabnik vnese svoje osebne podatke v obrazce, ki se nahajajo na takšnih straneh. Te podatke lahko napadalec zlorablja.

f) Elektronska pošta

Priponke v spletni pošti lahko vsebujejo oziroma nosijo viruse, črve, trojanske konje, izvajalne skripte itd. Vsa ta internetna zalega je pomoč socialnim inženirjem.
Spletna pošta lahko nosi okuženo pripeto datoteko, nevaren JavaScript[6], zlonamerni spletni naslov itd.

g) Prepričevanje

Osrednji del je prepričati osebo, da je socialni inženir v resnici oseba, ki ji lahko zaupa vse občutljive podatke. Osnovna metoda prepričevanja vsebuje laganje, dvorjenje, skladnost, razpršitev odgovornosti in vzpostavitev enostranskih prijateljskih vezi.

3.6 Varnostna tehnologija

V tem razdelku je kratek opis varnostnih tehnologij, namenjenih tehnični zaščiti pred opisanimi grožnjami informacijskih sistemov. Potrebno pa je poudariti, da je osebje najpomembnejši del učinkovitega programa za varovanje informacij. Če osebje ne bo ustrezno usposobljeno in poučeno o varnosti informacij, tudi tako dobra varnostna tehnologija ne bo uspešna proti grožnjam varnosti.

3.6.1 AAA – preverjanje pristnosti, pooblaščanja in skrbništvo računov

AAA je pomemben element varnostnega programa, ker omogoča prepoznavanje posameznikov in preverjanje njihovih pooblastil za dostop do določenega sredstva ali dela omrežja. Tehnologija AAA omogoča tudi sledenje zaposlenim in sredstvom podjetja, ki jih uporabljajo. Tehnologija AAA je prav tako pomembna pri določanju pravic za dostop do določenih lokacij v podjetju.

Preverjanje pristnosti je postopek, ki določi identiteto uporabnika. Uporabniška imena in gesla so najosnovnejša oblika preverjanja pristnosti. Med te vrste tehnologije spada uporaba fizičnih naprav ali žetonov, kot so pametne kartice, ki hranijo dodatne informacije za identifikacijo uporabnika. Sem spada tudi biometrija, s katero se preverjajo edinstvene biološke značilnosti uporabnika, kot je skeniranje prstnih odtisov ali očesne mrežnice.

Pooblaščanje določi, do česa ima uporabnik dostop. Tako imajo lahko vsi zaposleni v podjetju svoj e-poštni račun, samo omejeno število zaposlenih pa ima privilegiran dostop za dodajanje in odstranjevanje e-poštnih računov.

[6] Skriptni jezik.

Skrbništvo računov je orodje, ki preverja vse te postopke. Lahko se vidi, kdo ima dostop do sistemov in kaj počne. Preveri se lahko, ali je kdo imel dostop do sistema brez veljavnega pooblastila.

3.6.2 Požarni zidovi

Požarni zidovi sestavljajo »elektronsko« ograjo okoli računalniškega okolja. Vsebujejo filtre, ki samo določenim vrstam omrežnega prometa dovolijo vstop v omrežje podjetja in zavrnejo vse podatke, ki ne izpolnjujejo določenih meril.

3.6.3 Zaznavanje vdorov (IDS)

Sistem IDS zaznava elemente splošno znanih napadov. Omogoča proaktivno zaščito pred napadi. IDS iščejo vzorce, ki bi lahko pomenili, da napad ravno poteka ali da je bil izveden v preteklosti.

3.6.4 Protivirusni programi

Podobno kot se ljudje cepimo proti določenim boleznim, nam protivirusni programi pomagajo preprečiti okužbe računalnikov z virusi, s črvi in trojanskimi konji.

3.6.5 Šifriranje

Šifriranje je postopek pretvorbe podatkov v obliko, ki jo nepooblaščena oseba težko prebere.

3.6.6 Filtriranje vsebine

Orodja za filtriranje vsebine filtrirajo neprimerne informacije, kot je pornografija, in tako zagotovijo, da zaposleni ne morejo imeti dostopa do takih vsebin. Orodje za filtriranje vsebine omogoča filtriranje spleta in filtriranje e-pošte.

4. Varnostna politika

4.1 Uvod

Poglavje opisuje pomembnost varnostne politike v podjetju, njene lastnosti, delitev varnostne politike na več nivojev, pomembnost stalnega vzdrževanja ter prednosti uvedbe varnostne politike. Uporabljena razpoložljiva literatura je [4, 7], uporabljeni standard za to področje [12] ter interna dokumentacija podjetja »X« [22].

4.2 Splošno o varnostni politiki

Dobra varnostna politika je osnova vsakega varnostnega načrta v podjetju. Napisana mora biti z mislijo na končne uporabnike. Pomembno je, da je napisana jasno in enostavno, da jo bodo tudi nevešči uporabniki razumeli. Lahko je napisana kot en dokument, lahko pa je razdeljena na več nivojev, od krovnega na najvišjem, taktičnega na srednjem in operativnega na najnižjem nivoju.

Varnostna politika je v pristojnosti vodstva. Vodstvo je odgovorno za potrditev varnostne politike in za seznanjanje zaposlenih o varnostni politiki. Določi se lastnika dokumenta in ta je zadolžen za njegovo vzdrževanje in preglede.

Varnostna politika je definirana z varnostnimi pravilniki po posameznih področjih, ki jih je potrebno ciklično pregledovati in obnavljati. V varnostni politiki so definirani cilji, pravila in odgovornosti v zvezi z varnostjo informacijskih virov podjetja, razni postopki in pravila.

Ko celotno varnostno politiko spravimo v okvir, jo zapišemo v obliki dokumenta. Podjetja jo lahko objavijo na intranetu, ki je notranje omrežje podjetja, preko katerega dostopajo vsi zaposleni, kateri imajo vpogled vanjo.

Vsako dejanje, pa naj gre za namerno ali nenamerno, ki ne upošteva pravil, določenih v varnostni politiki, se obravnava kot kršenje varnostnih pravil. Dobra varnostna politika ima dovolj informacij o tem, kaj je potrebno postoriti za zaščito informacij, virov in ljudi v podjetju.

Varnostna politika zajema širok krog varnostnih vprašanj, ki so za vsako podjetje drugačna. Zaradi tega in zaradi specifičnosti poslovanja vsakega podjetja pa pripravljenega dokumenta varnostne politike ni mogoče kar kupiti v trgovini.

4.3 Prednosti varnostne politike

Prednosti uvedbe varnostne politike so:

- večja varnost informacijskega sistema pred grožnjami,
- varovanje ključnih poslovnih procesov,
- urejeno delo uporabnikov,
- poznavanje trenutnega stanja IT sistema in napotki za izboljšave.

5. Standardi na področju varovanja informacij

5.1 Uvod

Poglavje opredeljuje pojem standarda, prednosti standardov ter podrobno opisuje serijo varnostno informacijskih standardov ISO/IEC 27000. Opisan je tudi standard COBIT in pa ITIL, ki ni standard. Kot osnovo za opredelitev standardov sta uporabljena standarda [13, 14], razpoložljiva literatura [2] in internetni viri [15, 16, 17, 20].

5.2 Kaj je standard?

Standard je:

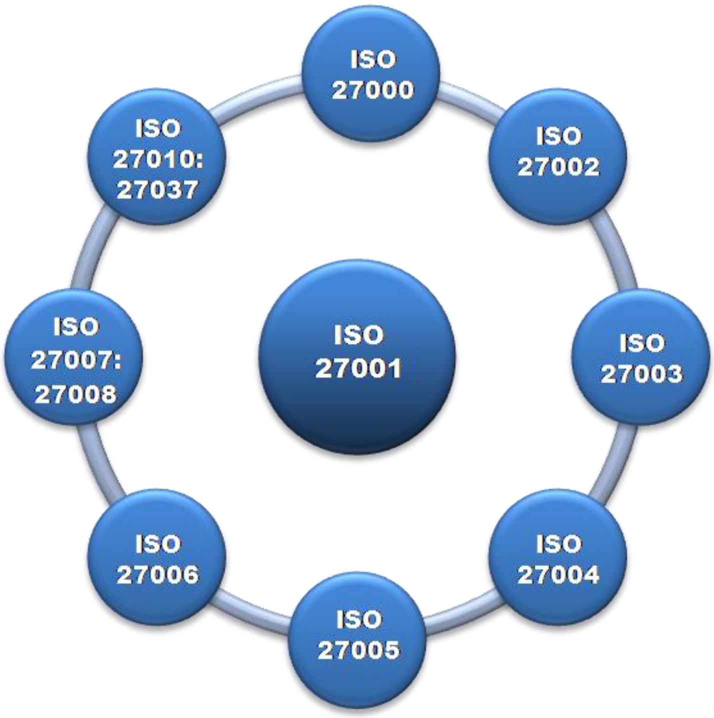
- zapisan sporazum, ki vsebuje tehnične specifikacije ali druge natančne zahteve, ki naj bodo stalno uporabljene kot pravila oziroma smernice,
- definicija karakteristik, ki zagotovijo skladnost materialov, proizvodov, procesov in storitev.

Standardi pogosto, ne da bi mi za to sploh vedeli, življenje naredijo varnejše in manj zapleteno, izdelki in storitve pa postanejo učinkovitejši in bolj ustrezajo pričakovanjem uporabnikov.

Danes je upravljavcem varovanja informacij na voljo več standardov, dobrih praks, postopkov, politik in metodologij. Nekatere so namenjene vsem organizacijam, kot je serija standardov ISO/IEC 27000, druge metodologije so bolj specializirane, na primer za produkte, kot je ISO 15408, ali za informacijsko tehnologijo ISO 13335, ki je okvir COBIT in podobno.

5.3 Serija standardov ISO/IEC 27000

Cilj standarda je doseganje kvalitativnih nivojev na področju varovanja informacij v okviru organizacije. Skladnost s standardom pomeni zaneslivejše delovanje, zmanjševanje posegov zaradi napak in zmanjševanje stroškov. Ta standard je najmočnejši v varnosti informacijske tehnologije, je pa nekoliko omejen s procesnega vidika.
Standard je razdeljen na več delov (Slika 1).



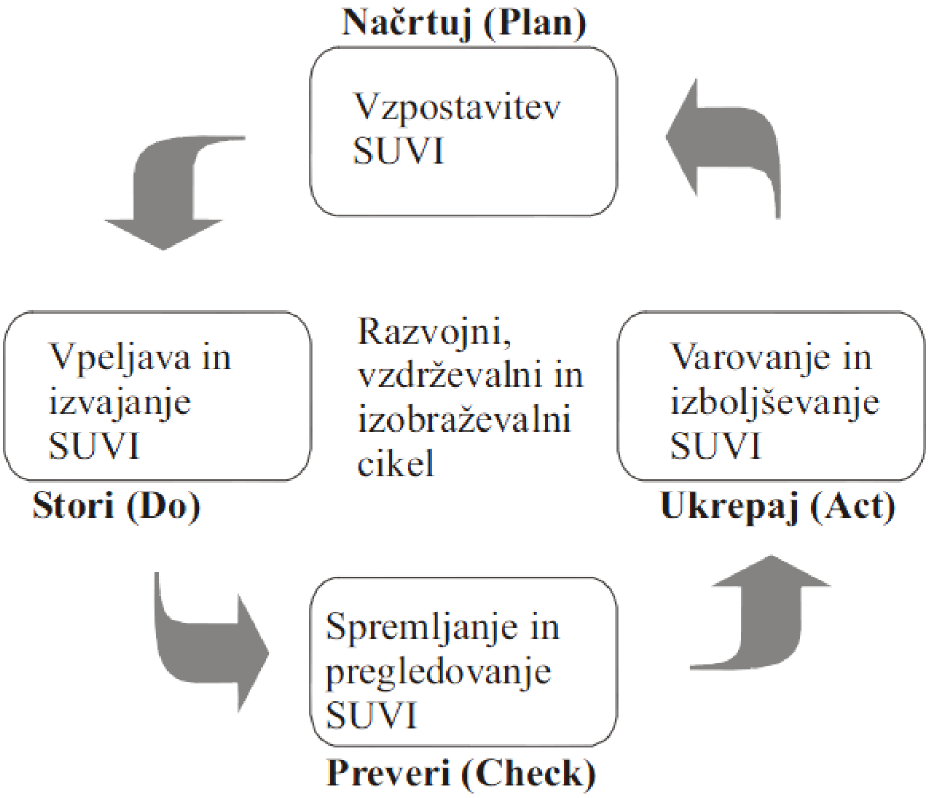
Slika 1: Osnovna struktura standardov ISO/IEC 27000.

5.3.1 ISO/IEC 27000 – Informacijska tehnologija – Varnostne tehnike – Temeljni principi in pojmovnik

Ta standard po vzoru ISO 9000 usklajuje strokovno izrazoslovje, osnovne principe in definicije za vso serijo standardov ISO/IEC 27000. Neustrezno definirani pojmi bi sicer vodili v zmedo in razvrednotenje formalnih ocen in certifikacije.

5.3.2 ISO/IEC 27001 – Informacijska tehnologija – Varnostne tehnike – Zahteve

Standard daje napotke, kako graditi, upravljati, vzdrževati in izboljševati sistem za upravljanje varovanja informacij (SUVI) v organizaciji. Glavne sestavine sistema za upravljanje varovanja informacij prikazuje Slika 2.



Slika 2: Faze sistema za upravljanje varovanja informacij.

Načrtuj (vzpostavitev SUVI): zajema vzpostavitev politike, ciljev, procesov in postopkov SUVI. Pomembno je, da so ocene varnostnih tveganj, ki ogrožajo informacije in pripravo načrta za primerno obravnavo teh tveganj, čim bolj pravilne. Podjetje mora tudi vse stopnje faze načrtuj dokumentirati.

Stori (izvajanje ter delovanje SUVI-ja): zajema vpeljavo in delovanje politike, kontrol, procesov in postopkov SUVI. Gre za vpeljavo izbranih kontrol ter izvedbo načrtovanih aktivnosti, ki so bile sprejete v prvi fazi (načrtuj).

Preveri (spremljanje ter pregledovanje SUVI-ja): faza zajema ocenjevanje in, kjer je izvedljivo, tudi merjenje delovanja procesov glede na politiko in cilje SUVI ter praktične izkušnje, in poročanje o dobljenih rezultatih vodstvu organizacije, ki naj jih pregleda. Vsi podatki, ki so zbrani v okviru faze preveri, se porabijo za merjenje uspešnosti SUVI pri doseganju poslovnih ciljev podjetja.

Ukrepaj (vzdrževanje ter izboljševanje SUVI): zadnja faza zajema sprejetje popravnih in preventivnih ukrepov na podlagi rezultatov notranje presoje SUVI in vodstvenega pregleda za doseganje trajnega izboljševanja SUVI.

Za izvajanje SUVI so v podjetju odgovorni vodstvo organizacije, pooblaščenec za informacijsko varnost, varnostni forum, krizni tim, vsi zaposleni, pogodbeni partnerji in stranke.

5.3.3 ISO/IEC 27002 – Informacijska tehnologija – Varnostne tehnike – Primeri dobre prakse implementacije sistema za upravljanje z varnostjo informacij

Namenjen je za implementacijo, izvajanje ali vzdrževanje SUVI. Ni formalni standard s specifikacijami, tako kot je ISO/IEC 27001. Standard ISO/IEC 27002 se uporablja za usmerjanje, če je cilj certificiranje v skladu z ISO/IEC 27001. ISO/IEC 27002 predlaga najboljše prakse na področju informacijskih varnostnih ukrepov. Nekoč se je ISO/IEC 27002 imenoval BS ISO/IEC 17799:2005, ki pa ni imel bistvenih vsebinskih razlik.

5.3.4 ISO/IEC 27003 – Informacijska tehnologija – Varnostne tehnike – Napotki za vzpostavitev SUVI

Standard ISO/IEC 27003 je vodnik in nudi pomoč pri vodenju projekta s ciljem doseganja skladnosti s standardom ISO/IEC 27001.

5.3.5 ISO/IEC 27004 – Informacijska tehnologija – Varnostne tehnike – Merila sistema za upravljanje informacijske varnosti

ISO/IEC 27004 pokriva področje vrednotenja upravljanja informacijske varnosti. Standard je namenjen kot pomoč organizaciji pri vrednotenju in poročanju o učinkovitosti svojih informacijskih sistemov pri upravljanju varnosti. Standard zagotavlja smernice za opredelitev in uporabo merilnih tehnik za zagotavljanje zanesljivosti.

5.3.6 ISO/IEC 27005 – Informacijska tehnologija – Varnostne tehnike – Upravljanje informacijskih tveganj

Dokument vsebuje navodila za obravnavanje tveganj, povezanih s sistemom za upravljanje informacijske varnosti. Standard pokriva ocenjevanje in vrednotenje tveganj, implementacijo ustreznih nadzorstev, nadzorovanje in pregledovanje tveganj kot stalen ali periodičen proces, vzdrževanje in stalno izboljševanje sistema nadzorstev.

5.3.7 ISO/IEC 27006 – Informacijska tehnologija – Varnostne tehnike – Zahteve za organe, ki izvajajo revizijo in certificiranje varnosti informacijskih sistemov

Namenjen je predvsem podpori certifikacijskih organov, ki zagotavljajo SUVI certificiranje. ISO/IEC 27006 določa zahteve in predvideva organe, ki zagotavljajo smernice za revizijo in certificiranje SUVI.

5.3.8 ISO/IEC 27007 – Informacijska tehnologija – Varnostne tehnike – Smernice za revidiranje SUVI

Standard zagotavlja smernice za certifikacijske organe, notranjo in zunanjo revizijo.

5.4 ITIL

ITIL ni standard. Predstavlja ogrodje najboljših praks in priporočil za upravljanje storitev na področju informacijske tehnologije. Upravljanje informacijske tehnologije (IT) po metodologiji ITIL prinaša naslednje koristi: izboljšano je upravljanje in nadzor nad spremembami, izboljšana razpoložljivost, zanesljivost in varnost storitev IT, zmanjšanje IT stroškov, zadovoljstvo uporabnikov.

5.5 COBIT

Leta 1996 je organizacija revizorjev informacijskih sistemov (ISACA) izdala publikacijo COBIT (Control Objectives for Information and Related Technology) kot pripomoček managerjem in lastnikom poslovnih procesov ter revizorjem IS.

COBIT model je zasnovan za nadzor izvajanja IT funkcij. Vsebina COBIT podpira IT nadzorstvo, da bi lažje dosegli naslednje cilje: IT je usklajen s poslovnim delom, IT podpira poslovni del in maksimira korist, IT tveganja so ustrezno upravljana, odgovorna uporaba IT virov.

COBIT predstavlja preverjen nabor dobrih praks in procesov, ki jih poslovne organizacije lahko uporabijo z namenom, da bi zagotovile čimbolj učinkovito delovanje IT-ja zaradi zmanjševanja tveganj, povezanih z IT-jem in maksimiranjem koristi investicij v tehnološke rešitve.

5.6 Prednosti standardov

Koristi standarda:

- tržne prednosti podjetja,
- zmanjša tveganja v informacijskih sistemih,
- zmanjša možnost nastanka nesreč na področju varovanja informacij,
- potrdilo o mednarodnem standardu,
- prihranek na času in denarju,
- zmanjšanje stroškov.

6. Primer analize varovanja informacij v podjetju “X”

6.1 Uvod

Poglavje podaja splošno predstavitev podjetja »X«, v katerem je bila izvedena analiza varovanja informacij. Prikazana je problematika in faze vpeljave serije standardov ISO/IEC 27000 v podjetju »X« in celovita analiza varovanja informacij v podjetju z podanimi predlogi za izboljšavo informacijske varnosti. Za predstavitev podjetja »X« je bila uporabljena interna dokumentacija podjetja [22], za analizo informacijske varnosti uporabljeni standardi [12, 13, 14] z razpoložljivo literaturo [7, 8] in internetnimi viri [16]. Pri oblikovanju tabel smo se zgledovali po [14].

6.2 Predstavitev podjetja »X«

6.2.1 Splošno o združbi »X«

Podjetje »X« je podjetje, organizirano kot družba z omejeno odgovornostjo, z zgodovino izdelave informacijskih rešitev, ki sega v leto 1989. Podjetje ima okrog 25 zaposlenih, približno 60 slovenskih občin je neposrednih uporabnikov informacijskih rešitev podjetja.

6.2.2 Poslanstvo in vizija

Temeljno poslanstvo podjetja je, da s skrbnim razvojem in vzdrževanjem informacijskih rešitev, zagotavljanjem podpornih storitev ter varnim, zanesljivim obratovanjem zagotovi vsem strankam zadovoljstvo in kakovost teh. Z inovativnimi in sodobnimi informacijskimi rešitvami skrbijo za doseganje stalne rasti in dodane vrednosti podjetja. Kot stabilno podjetje s svojimi usklajenimi rešitvami, izkušnjami in znanjem spodbujajo vsestransko zadovoljstvo in razvoj ter skrbijo za kvaliteten, skrben odnos s strankami. Podjejte »X« odlikuje rast kakovosti storitev, kadrov, strokovnosti in poslovna rast.

Vizija podjetja »X« je utrditi ime stabilne, zanesljive in zaupanja vredne družbe, ki bo svojim strankam ponujala najkakovostnejše izdelke in storitve po konkurenčnih cenah in dolgoročno zagotavljala dobiček združbi.

Temeljne vrednote, ki jih bo združba zasledovala pri svojem poslovanju, so kakovost storitev in produktov, stabilnost poslovanja, poslovna korektnost.

6.2.3 Dejavnosti združbe

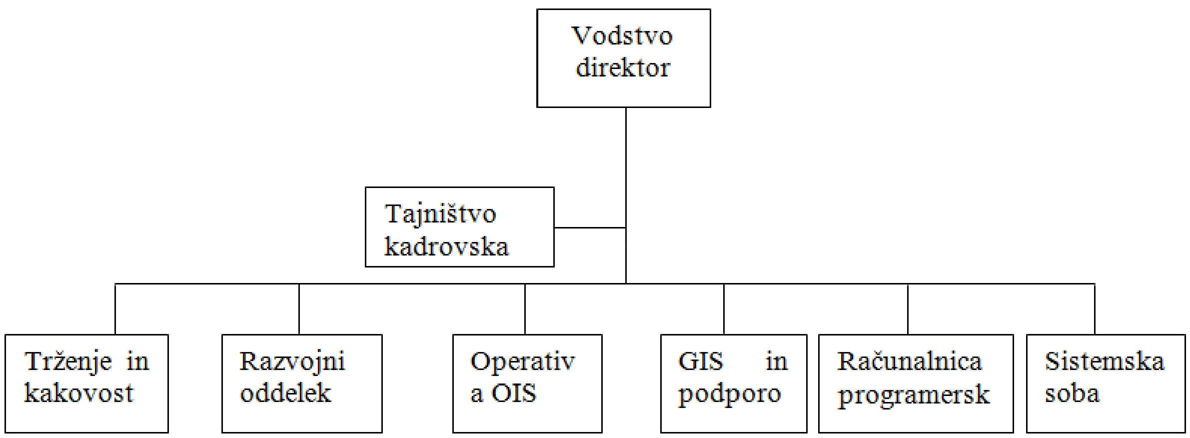
Podjetje »X« je pristojno tako za razvoj informacijskih rešitev kot za njihovo vzdrževanje. Prav tako nudi podporne storitve o uporabi informacijskih rešitev strankam.

Vodilo podjetja »X« je zadovoljiti želje in zahteve strank ter zagotavljati celovite in inovativne informacijske rešitve. Njihova usposobljenost in izkušnje jim omogočajo, da s svojimi strankami razvija dolgoročne in pristne partnerske odnose.

6.2.4 Organiziranost združbe

Delo v združbi je projektno organizirano. Na razvojnih projektih stalno sodelujejo magister računalništva in informatike, univerzitetni diplomirani inženirji računalništva, univerzitetni diplomirani inženir strojništva, inženirji organizacije ter inženirji prometa. Za specifične svetovalne in izvajalske aktivnosti na posameznih projektih v projektne time se po potrebi vključi dodatne zunanje strokovnjake.

Organizacijska shema združbe »X« je sestavljena iz osmih sektorjev: vodstvo, tajništvo, trženje in kakovost, razvoj, operativa in podpora občinskim informacijskim sistemom, podpora geografskim informacijskim sistemom, računalnica za dodaten razvoj ter sistemska soba. Na spodnji sliki je prikazana organizacijska struktura v podjetju »X«.



Slika 3: Organizacijska shema združbe.

a) Sistemska soba

V sistemski sobi nudijo svetovanje, izvedbo, vzdrževanje in zaščito storitev računalniškega sistema. Njihovo delo obsega delo z datotečnimi strežniki, SQL[7], delo s protivirusno opremo in z arhiviranjem pomembnih podatkov.

b) Razvojni oddelek

Za konstantno rast podjetja in zadovoljevanje pričakovanj strank skrbi razvojni oddelek, ki nenehno sledi tehnološkemu razvoju in uvaja inovacije v podjetju. Na tržišču nudijo aplikacije na ključ, prilagojene specifičnim potrebam in zahtevam naročnika.

c) Operativa – OIS

Oddelek nudi podporo občinskim informacijskim sistemom (OIS[8]) uporabnikom. Zadolženo je tudi za testiranje informacijskih rešitev pred izdajo v produkcijo in njihovo popravljanje, kjer ni potrebnih večjih posegov v izvorno kodo.

d) GIS in podpora

Sektor razvija geografske informacijske sisteme in nudi podporo. Raziskuje in razvija podatkovne baze geografskega informacijskega sistema in podatkovne strukture GIS[9]-u.

e) Računalnica

Računalnica ali programerska soba skrbi za dodaten razvoj informacijskih rešitev in razvoj internih razvijalskih orodij podjetja. Poteka tudi skeniranje map za geografski informacijski sistem.

f) Trženje in kakovost

Sektor skrbi za kakovostno informacijsko rešitev v produkciji in za stike z javnostjo.

6.2.5 Varnostna politika podjetja »X«

Varnostna politika v podjetju ni definirana sistematično in celovito. Izvajajo se le določeni varnostni ukrepi glede na znanje in izkušnje zaposlenih. Prav tako ni celovitega izobraževanja na področju varnosti.

---

[7] Povpraševalni jezik za delo s podatkovnimi bazami.
[8] Skupina aplikacij, namenjena celoviti računalniški podpori dejavnostim v lokalni samoupravi.
[9] Aplikacije, namenjene prikazovanju geokodiranih podatkov.

6.3 Faze projekta vpeljave serije standardov ISO/IEC 27000

Študija primera je zasnovana na osnovi posameznih sekcij standarda ISO/IEC 27001 in ISO/IEC 27002, kjer je analiza narejena s pomočjo kontrolnih vprašanj. Ugotovitve so neposredni odgovor na vprašanje o usklajenosti s standardom in odkrivajo varnostne pomanjkljivosti v sistemu. Na podlagi teh ugotovitev so napisana priporočila. Nekaterim kontrolam v tabeli so dodane povezave do določenih vzorcev (npr. vzorec varnostne politike). Tako je lahko vsak odgovorni za določeno področje imel predstavo o določenem dokumentu. Tabela, katero sem kreiral, predstavlja interno dokumentacijo podjetja »X«, zato so nekateri detajli zaradi varnosti odstranjeni.

6.3.1 Problematika in faze projekta vpeljave ISO/IEC 27000 v podjetju »X«

Serija standardov ISO/IEC 27000 je zelo obsežen varnostni standard. Namenjen je vsem vrstam podjetij: mikro, majhnim, srednjim in velikim. Podjetje, v katerem sem opravljal prakso, spada v srednje podjetje. Standard ISO/IEC 27001, ki vsebuje kontrolne točke, sem moral na primeren način preurediti in odvečno vsebino odstraniti; tako je postal primeren za podjetje »X«. Ker je podjetje relativno majhno, je razumljivo, da nimajo vseh postopkov formaliziranih. To dejstvo sem zato nekoliko upošteval, tako da je pripravljeni načrt vzpostavitve informacijske varnosti primeren za podjetje »X«. Bilo bi nesmiselno, da bi se striktno držal vseh smernic standarda ISO/IEC 27001 in ISO/IEC 27002, ker bi to dalo za podjetje »X« neuporabne rezultate. Projekt vpeljave varnostnega standarda ISO/IEC 27000 v podjetju »X« je razdeljen na tri faze, katera je vsaka podrobno opisana.

Prva faza projekta ISO/IEC 27000 je zajemala pripravo splošne predstavitve serije standardov ISO/IEC 27000 in vseh njegovih kontrolnih ciljev in dobrih praks. Predstavitev sem moral zelo posplošiti, da je bila razumljiva, saj je bilo 400 in več strani, kolikor vzameta standarda ISO/IEC 27001 in ISO/IEC 27002, skrajšanih na 50 strani prezentacije. Prezentacija je tako trajala kar dve uri in pol. Predstavitev pa je vsebovala tabelarično obliko opisa standarda, kjer je bila podana številka kontrolne točke standarda, sekcija kontrole in osnovna kontrolna vprašanja o skladnosti informacijske varnosti s standardom ISO/IEC 27001.

Druga faza projekta ISO/IEC 27000 je najobsežnejši del tega projekta. Potrebno je bilo proučiti ISO/IEC 27001 in ISO/IEC 27002 do potankosti ter razbrati pomembne informacije za potrebe podjetja »X«. Sestaviti je bilo potrebno tabelo, ki je vsebovala naslednja imena stolpcev: uradna številka kontrolne točke standarda, ime sekcije standarda, kontrolna vprašanja skladnosti s standardom, trenutno stanje v podjetju glede varovanja informacij, predlog za izboljšave ter odgovorna oseba za posamezno kontrolno točko standarda. Kontrolna vprašanja standarda predstavljajo kot povzetek dobrih praks iz ISO/IEC 27002 in pa kontrolnih točk standarda ISO/IEC 27001, saj je takšen način po mojem mnenju najprimernejši za popis trenutnega stanja v podjetju, v katerem delajo različni profili

uporabnikov. Kontrolna vprašanja v tabeli tako predstavljajo vprašanja za odgovorno osebo in sočasno še dajejo namig, kaj bi bilo potrebno izboljšati glede varovanja informacij.
ISO/IEC 27002, iz katerega sem med drugim izdelal kontrolna vprašanja, vsebuje na dolgo zapisane praktične rešitve glede varovanja informacij, pa še izrazi so strokovni, kar ni primerno za vsak profil uporabnikov. Vprašalnik mora biti razumljiv vsakemu zaposlenemu v podjetju. Stolpec trenutnega stanja je namenjen odgovorni osebi, katera zabeleži dosedanje ugotovitve glede varovanja informacij. Stolpec »predlog za izboljšave« pa je namenjen meni oziroma cenilcu informacijske varnosti, ki oceni in poda predloge za izboljšave v zvezi z varovanjem informacij na osnovi dobrih praks z pomočjo standarda ISO/IEC 27002. V nekaterih primerih je dodana povezava do določenega vzorca, kot je primer krovne politike podjetja; tako lahko ima odgovorna oseba predstavo o zahtevah trenutne kontrolne točke standarda oziroma sekcije standarda. Dodal sem javni direktorij v podjetju, v katerem so shranjeni nekateri primeri vzorcev, kot so: krovna politika podjetja, politika elektronske pošte, ravnanje v primeru varnostnega incidenta, popis vseh sredstev podjetja, politika uporabe dovoljene programske opreme, politika čiste mize ... Polje »odgovorna oseba« podaja informacijo, komu v podjetju je ta sekcija standarda oziroma kontrolna točka standarda namenjena. Lahko je namenjeno vodstvu, razvojnikom, sistemskemu administratorju, operaterju ali pa vsem zaposlenim v podjetju. Tako sem ISO/IEC 27001 in ISO/IEC 27002, ki skupaj vzameta več kot 400 strani teksta, skrčil v tabelarično obliko na 70 strani listov A4. Prikaz tabel sledi v nadaljevanju.

Tretja faza projekta ISO/IEC 27000 je zadnja faza, ki predstavlja celovit popis trenutnega stanja varovanja informacij v podjetju »X«. Ta faza je trajala do konca mojega praktičnega izobraževanja. Natisnjene pripravljene tabele sem porazdelil po vseh oddelkih podjetja. Tako sem od vsake odgovorne osebe pridobil popis trenutnega stanja varovanja informacij v podjetju. Tako sem lahko na osnovi popisa trenutnega stanja in lastnega raziskovanja v podjetju podal svoje predloge za izboljšavo varovanja informacij. Izkazalo se je, da so določene stvari v podjetju urejene in ustrezajo seriji standardov ISO/IEC 27000, določene pa ne, kar je tudi razumljivo, saj gre za manjše podjetje. Povečini pa je v slovenskih podjetjih značilno, da se namenja premalo pozornosti sistemu za varovanje informacij. Z zadnjo fazo projekta serije standardov ISO/IEC 27000 je nastal načrt vpeljave ISO/IEC 27000 v podjetje »X«. Za morebitno praktično vpeljavo načrta varovanja informacij pa je potrebnega veliko truda in pobud s strani vodstva in same ozaveščenosti uporabnikov. Če se vsi zaposleni v podjetju ne zavedajo pomena varovanja informacij, tudi tako dobra varnostna tehnologija, kot je požarni zid ali protivirusna programska oprema, ne bo zaščitila pred informacijskim tveganjem.

6.4 Popis trenutnega stanja varovanja informacij v podjetju »X« in dajanje predlogov za izboljšave

V nadaljevanju je prikazan popis trenutnega stanja varovanja informacij v podjetju »X« po standardu ISO/IEC 27001 in ISO/IEC 27002 ter podanimi predlogi za izboljšave. Popis je bil izveden v drugi in tretji fazi projekta vpeljave informacijske varnosti v podjetje »X«.

6.4.1 ISO 27001 – Varnostna politika

Cilj poglavja varnostne politike je zagotovitev, da vodstvo organizacije usmerja in podpira varovanje informacij v skladu s poslovnimi zahtevami in ustreznimi zakoni ter predpisi. Vodstvo organizacije naj bi z objavo in zagovarjanjem politike varovanja informacij določilo jasno in taktično usmeritev. Celotni organizaciji mora biti pokazano, kako pomembna je predanost varovanju informacij po celi organizaciji.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
5.1	**INFORMACIJSKA VARNOSTNA POLITIKA**				
5.1.1	Dokumenti varnostne politike.	- Dokument varnostne politike. - Dokument objavljen. - Z njim seznanjeni vsi zaposleni. - Dokument vsebuje opise usmeritev, načel, standardov.	Ne, treba izdelati dokument avarnostne politike.	Primer politike e-pošte - **Priloga <u>9.12</u>** **Predlog:** Organizacija naj izdela politiko varovanja informacij. Dokument naj je razdeljen v več nivojev. Najvišji nivo je krovna varnostna politika, srednji nivo politika za posamezna področja, najnižji nivo navodila, postopki za delo, predpisi. Dokumenti za končne uporabnike naj bodo v obliki kratkih, jasnih in razumljivih navodil.	Vodstvo.
5.1.2	Ocenjevanje in vrednotenje varnostne politike.	- Lastnik dokumenta, ki je odgovoren za vzdrževanje in ocenjevanje s predpisom za ocenjevanje. - Redno preverjanje dokumentov. - Redno usklajevanje in izboljševanje dokumentov.	Ne, treba izdelati dokumenta varnostne politike.	Primer obrazca preverjanja dokumentacije- **Priloga <u>9.5</u>** **Predlog:** Organizacija naj določi lastnika, ki je odgovoren za vzdrževanje varnostne politika. O spremembah varnostne politike naj bodo zaposleni redno obveščeni. Določeni naj bodo časovni intervali, v katerih skrbnik preveri vsebino in po potrebi vnese v dokumentacijo ustrezne popravke.	Lastnik dokumenta varnostne politike.

6.4.2 ISO 27001 – Organizacija varovanja informacij

Drugo poglavje standarda govori o organiziranosti varovanja. Poudari potrebo po oblikovanju varnostnega foruma, katerega namen je skrb za smernice varnostne politike v organizaciji. Bistvene zahteve, ki so podane pri organizaciji zaščite v podjetju, so skrb za pravilno gospodarjenje z informacijami, upravljanje z informacijsko varnostjo ter opredelitev varnostnih zahtev pri poslovanju z drugo organizacijo.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
6.1	**Notranja ureditev**				
6.1.1	Zavezanost vodstva varovanju informacij.	- Forum za upravljanje, ki ima jasne cilje in podpira varnostne pobude podjetja. - Določeni jasni cilji za doseganje informacijske varnosti. - Zagotovljena potrebna sredstva za zagotavljanje informacijske varnosti. - Zagotovljeno upravljanje in koordiniranje uvajanja informacijske varnosti v celotnem podjetju.	Forum je, ni pa kategorije za varnost. Delno formalno. Delno. Ne.	**Predlog:** Organizacija naj ustanovi odbor za varovanje informacij, katerega člani morajo imeti vplivno funkcijo v podjetju.	Člani odbora.
6.1.2	Koordinacija informacijske varnosti.	- Skupina strokovnjakov iz vseh nivojev upravljanja za koordinacijo in uvedbo varnostnih predpisov. - Upravljanje informacijske varnosti, skladno z dokumenti varnostne politike podjetja. - Prepoznava in dokumentiranje neskladnosti z varnostno politiko.	Ni organa za usklajevanje varovanja informacij. Ne, ni varnostne politike. Ne, ni varnostne politike.	**Predlog:** Ker je organizacija relativno majhna, ni potrebe po uvedbi usklajevalnega odbora. Tudi če se uporablja najboljša varnostna tehnologija, brez izobraževanja in osveščanja uporabnikov ne bo pomagala. Zato je pomembno izobraževanje o varnosti informacij.	Predstavniki različnih delov organizacije.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
		- Prepoznava bistvenih sprememb groženj in izpostavljenost informacij do spremenjenih groženj. - Načrtno izobraževanje in osveščanje uporabnikov.	Da. Ne.	Zelo velika verjetnost za grožnjo informacijske varnosti bodo neobveščeni uporabniki.	
6.1.3	Dodeljevanje odgovornosti za varovanje informacij.	- Popis vseh sredstev posameznih sistemov v podjetju. - Jasno definirana odgovornost za posamezna področja zagotavljanja informacijske varnosti. - Dokumentacija pristojnosti za vsako sredstvo informacijskega sistema. - Dokumentacija vseh ravni pooblastil.	Da, interni strežnik podjetja. Delno, le osnovno. Da, na internem strežniku. Delno.	Obrazec popisa sredstev - **Priloga <u>9.6</u>** Obrazec pooblastil za dostop do rač.sistemov - **Priloga <u>9.9</u>** **Predlog:** Organizacija naj določi vodjo oziroma pooblaščenca za informacijsko varnost, ki prevzema celotno odgovornost za razvoj in vpeljavo varovanja informacij.	Vodja za informacijsko varnost. Lastnik posameznega informacijskega sredstva, za katerega skrbi.
6.1.4	Postopek pooblaščanja delovnih sredstev.	- Upravljanje postopka pooblaščanja za vsako novo strojno in programsko opremo. - Preverjanje skladnosti nove programske in strojne opreme. - Preverjanje skladnosti programske in strojne opreme z drugimi elementi sistema.	Večinoma. Da. Da.	Obrazec pooblastil za dostop do rač.sistemov - **Priloga <u>9.9</u>** **Predlog:** Nakupi novih zmogljivosti naj bodo skladni s poslovnimi potrebami podjetja. Vsak nov nakup naj predhodno potrdi pooblaščenec za informacijsko varnost.	Vodstvo. Upravljavci.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
6.1.5	Opredelitev zaupnosti.	- Vsi zaposleni podpišejo izjavo o zaupnosti poslovnih podatkov. - Postopek o trajanju zaupnosti poslovnih informacij po prekinitvi delovnega razmerja. - Definirana pooblastila za uporabo zaupnih podatkov. - Postopki za nadzor nad uporabo zaupnih podatkov. - Postopek za obveščanje v primeru nepooblaščene uporabe zaupnih podatkov. - Klasifikacija ravni zaupnosti poslovnih informacij in podatkov.	Da. Da. Ne. Ne. Ne. Ne.	Obrazec izjave o zaupnosti - **Priloga <u>9.1</u>**	Vodstvo.
6.1.6	Sodelovanje med organizacijami.	- Vzpostavljeni kontakti s strokovnjaki področja prava, telekomunikacijskih storitev in podobno za primer grožnje in njihovo reševanje – njihovi nasveti.	Ni potrebe za opisano podjetje.		Vodstvo. Forum (odbor).
6.1.7	Sodelovanje s strokovnjaki.	- Vzpostavljeno sodelovanje z zunanjimi strokovnjaki za varnost zaradi izmenjave izkušenj.	Ni potrebe za opisano podjetje.		Vodstvo.
6.1.8	Neodvisni pregled varovanja informacij.	- Izvajanje neodvisne presoje varnosti informacijskega sistema.	Da.		Vodstvo. Zunanji revizorji.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
6.2	**ZUNANJE STRANKE**				
6.2.1	Prepoznavanje tveganj povezanih z zunanjimi strankami.	- Prepoznava tveganj, povezanih s poslovanjem z zunanjo stranko. - Implementirane ustrezne varnostne kontrole. - Beleženje dostopov zunanjih strank do elementov IS. - Nadzor nad delom zunanjih strank. - Definirana odgovornost zunanjih strank v primeru uresničitve varnostne grožnje.	Da. Da. Da. Da. Da.		Vodstvo. Računalniška soba.
6.2.2	Varnostne zahteve v pogodbah s tretjo stranko.	- V pogodbe pri sklepanju poslov zunanjih strank vključene varnostne zahteve v skladu z varnostno politiko in standardi podjetja. - Pogodbe s strankami vsebujejo točen opis predvidenih storitev. - Pogodbe s strankami vključujejo sistemske zahteve, ki omogočajo uporabo storitev. - Pogodba s stranko vključuje pravico do nadzora uporabe storitev. - Pogodba s stranko vključuje zaščito intelektualne lastnine podjetja. - Pogodba s stranko vključuje obvezo o spoštovanju obveznosti za obe strani.	Ne, ni definirane varnostne politike podjetja. Da. Da. Da. Da. Da.		Vodstvo. Računalniška soba.

6.4.3 ISO 27001 – Ravnanje s sredstvi

V tretjem poglavju standarda je glavna točka popis vseh sredstev, ker se edino tako lahko določi lastništvo nad pomembnejšimi sredstvi in določi odgovornost za vzdrževanje ustreznih količin.

Standard	**Sekcija**	**Kontrola (cilj)**	**Trenutno stanje**	**Rešitve / primeri dobre prakse**	**Odgovornost**
7.1	**ODGOVORNOST ZA SREDSTVA**				
7.1.1	Popis sredstev.	- Pravočasno dopolnjevanje registra sredstev z novimi informacijami in podatki. - Seznami informacij (podatkov, podatkovnih baz, pogodb, sistemske dokumentacije, priročniki ...). - Seznam programske opreme. - Seznam strojne opreme. - Seznam poslovnih procesov. - Seznam ljudi, njihove usposobljenosti, spretnosti in izkušnje. - Zavedanje zaposlenih, da je ugled in ime podjetja treba varovati.	Večinoma interni strežnik. Da, interni strežnik podjetja. Da. Da. Da. Da. Da.	Obrazec popisa sredstev - **Priloga <u>9.6</u>**	Vodstvo.
7.1.2	Lastništvo sredstev in informacij.	- V dokumentu vsa sredstva in informacije vsebujejo znane lastnike. - Odgovornosti lastnika (informacije ustrezno klasificirane).	Delno. Delno.	Obrazec popisa sredstev - **priloga <u>9.6</u>** **Predlog:** Pomembnost sredstev je določena zgolj formalno, ni pa analizirana, ovrednotena in zapisana. Zaupane ali pomembne informacije podjetja se lahko zaradi napačne uporabe izgubijo ali pokvarijo. Če podatki niso urejeni po pomembnosti in	Lastnik sredstva. Skrbnik.

				zaupnosti, je zelo težko bolje ščititi pomembne informacije, saj sploh ne vemo, katere so. Zato vse vrste sredstev razvrstimo glede na zaupnost, občutljivost, vrednost in kritičnost.	
7.1.3	Sprejemljiva uporaba sredstev.	- Pravila za primerno rabo elektronske pošte in interneta. - Pravila za primerno rabo mobilnih naprav.	Neformalno. Neformalno.	Primer politike e-pošte - **Priloga** **<u>9.12</u>**	Vodstvo.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
7.2	**KLASIFIKACIJA INFORMACIJ**				
7.2.1	Smernice za klasifikacijo.	- Sheme in smernice za razvrščanje informacij, ki pomagajo določiti ravnanje z informacijami in njihovo zaščito – klasifikacijski načrt . - Razvrstitev glede na njihovo vrednost, pravne zahteve, občutljivost in kritičnost. - Določen čas trajanja klasifikacije.	Ne. Ne. Ne.	**Predlog:** Organizacija naj izdela klasifikacijski načrt, s katerim postavi klasifikacijo. Klasifikacijski načrt naj bo v pisni obliki in na voljo vsem, ki so pooblaščeni za njegovo uporabo. Predlagam preprosto klasifikacijo; javna, zaupna in poslovna skrivnost. Za klasifikacijo informacij naj bodo odgovorni lastniki informacij.	Vodstvo. Lastnik sredstva. Računalniška soba.
7.2.2	Označevanje ter ravnanje z informacijami.	- Postopki za označevanje informacij (elektronsko označevanje, fizično označevanje) in ravnanje z njimi, ki so v skladu s klasifikacijskim načrtom.	Ne.	**Predlog:** Organizacija naj izdela postopke za označevanje in ravnanje z informacijami, ki naj bodo v skladu s klasifikacijskim načrtom. Najprimernejša oblika označevanja so fizične oznake.	Lastnik sredstva. Računalniška soba.

6.4.4 ISO 27001 – Varovanje človeških virov

Četrto poglavje standarda obravnava postopke, ki se opravljajo pred sklenitvijo zaposlitve, med njo in po prekinitvi ali menjavi. V poglavju izvemo, kako zmanjšati tveganje zaradi človeških napak, kraj, poneverb ali zlorab zmogljivosti. To pa rešijo razna ozaveščanja, izobraževanja in usposabljanja zaposlenih za varovanje informacij, preverjanje oseb pred zaposlitvijo in preverjanje pogodbenih strank.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
8.1	**PRED ZAPOSLITVIJO**				
8.1.1	Vloge in odgovornosti.	- Ustrezno opisane varnostne vloge in odgovornosti vseh zaposlenih, ki so odgovorni za varovanje informacij.	Da, v pravilniku.		Vodstvo. Kadrovska.
8.1.2	Pregledovanje in kontrola kandidatov za zaposlitev.	- Preverjanje kandidatov pred zaposlitvijo je stalna praksa (značajske lastnosti, življenjepis, akademske in profesionalne kvalifikacije, identiteta kandidata).	Da.	**Predlog:** Tudi med delom naj vodje preverjajo kredibilnost zaposlenih. Pozorni naj bodo predvsem na depresivne osebe, osebe z denarnimi težavami, osebe, ki veliko izostajajo z dela ...	Vodstvo. Kadrovska.
8.1.3	Določbe in pogoji zaposlovanja.	- Od kandidata za zaposlitev se zahteva podpis dokumenta o odgovornosti za varnost informacijskega sistema.	Da.	Obrazec izjave o zaupnosti - **Priloga <u>9.1</u>** **Predlog:** Ta odgovornost naj traja v podjetju, izven podjetja in v nekaterih primerih tudi za določen čas. Organizacija naj navede tudi ukrepe za primer kršitev navedenih varnostnih zahtev.	Vodstvo. Kadrovska.
8.2	**MED ZAPOSLITVIJO**				
8.2.1	Vpeljava in seznanitev z varnostno politiko.	- Vpeljavo novo zaposlenih nadzira vodstvo in pripravlja ustrezna navodila.	Da.		Vodstvo. Kadrovska.

8.2.2	Ozaveščanje, izobraževanje in usposabljanje za varovanje informacij.	- Zaposleni se morajo zavedati groženj in biti ustrezno izobraženi. - Načrt usposabljanja za posameznika v skladu z njegovim znanjem in delovnim mestom.	Delno - samoiniciativni posamezniki.	**Predlog:** Organizacija naj za vse zaposlene organizira usposabljanje za osnovno varnostno ozaveščanje.	Vodstvo. Kadrovska.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
8.2.3	Disciplinski postopki.	- Formalni disciplinski postopek za uslužbence, ki kršijo varnostno politiko.	Ne.	**Predlog:** Organizacija naj po uvedbi varnostne politike tudi za to področje izvaja disciplinske postopke ter se s tem primerno odzove na kršitve varovanja. Disciplinski postopek naj bo po eni strani svarilo vsem, ki kršijo varnostno politiko, po drugi strani pa zagotovilo pravilne in poštene obravnave hujših kršitev varnostne politike.	Vodstvo. Kadrovska.
8.3	**PREKINITEV ALI SPREMEMBA ZAPOSLITVE**				
8.3.1	Odgovornosti po koncu zaposlitve.	- Jasno definirani postopki in odgovornosti ob prekinitvi ali menjavi zaposlitve.	Da.		Kadrovska.
8.3.2	Vrnitev sredstev.	- Postopek vračanja vseh sredstev podjetja (logičnih in fizičnih sredstev).	Da.		Kadrovska.
8.3.3	Odvzem dostopnih pravic.	- Pravice dostopa do posameznih sredstev se ukinejo nemudoma po prekinitvi ali menjavi zaposlitve.	Da.		Sistemski administrator.

6.4.5 ISO 27001 – Fizična zaščita in zaščita okolja

Peto poglavje standarda je namenjeno fizičnemu varovanju, predvsem varovanju vitalnih informacijskih sredstev. Poglavje zajema zaščito sredstev pred nepooblaščeno uporabo, zaščito opreme pred naravnimi in drugimi nesrečami, ločenost območja za dostavo od zmogljivosti za obdelavo informacij. Kritične in občutljive poslovne informacije morajo biti shranjene v prostorih, ki so ustrezno varovani z vstopnimi kontrolami.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
9.1	**VAROVANA OBMOČJA**				
9.1.1	Fizični varnostni pas.	- Fizične omejitve za zaščito elementov informacijske tehnologije - (elektronske ključavnice, dostopne kartice, ločeni vhod, ločen prostor za strežnike in diske ...).	Ni potrebe za trenutno stanje podjetja.		Vodstvo.
9.1.2	Kontrola fizičnega dostopa.	- Vhodne kontrole v podjetju - (evidentiranje vstopov osebja ...).	Delno.	**Predlog:** Organizacija naj nadzoruje in pregleduje vse dostope, beleži točen čas vhoda in izhoda.	Vodstvo.
9.1.3	Varovanje pisarn, sob in naprav.	- Prostori zaprti. - Omare s ključavnico. - Varnostne omare. - Prostori zaščiteni pred nesrečami človeka in narave. - Onemogočanje potencialnih nevarnosti v sosednjih prostorih.	Ni zaklepanj. Da. Da. Da. Ne, problem lesenih pregrad - možnost širjenja požara.	**Predlog:** Gorljivi predmeti naj bodo ločeni od varovanih območij, prav tako naj bodo od varovanih prostorov ločena tudi rezervna oprema in varnostne kopije.	Vsi.
9.1.4	Zaščita pred zunanjimi grožnjami in grožnjami iz okolja.	- Fizična zaščita pred ognjem. - Fizična zaščita pred poplavo. - Fizična zaščita pred potresom.	Da, gasilni aparat. Da. Da.		Vsi.
9.1.5	Delo na varovanih območjih.	- Varnostna kontrola dostopa za tretjo osebo, ki dela v varovanem območju.	Delno, spremstvo osebi.	**Predlog:** Organizacija naj bo dosledna pri najavi del v varovanem območju in naj to delo tudi nadzira.	Vsi.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
9.1.6	Javni dostop, dostava in območja za odpošiljanje.	- Področje za transport materiala ločeno od področja, kjer je obdelava informacij.	Ni potrebe za opisano podjetje.		
9.2	**VAROVANJE OPREME**				
9.2.1	Namestitev in zaščita opreme.	- Oprema shranjena v prostoru, ki zmanjšuje nepooblaščen dostop. - Ločevanje posebej zaščitene opreme od ostale opreme. - Varovanje, ki zmanjšuje tveganje pred krajo, ognjem, vodo, eksplozijo, motnje z oskrbo elektrike. - Pravila o pitju, prehrani in kajenju znotraj prostorov za obdelavo podatkov. - Meritve okoljskih parametrov, ki vplivajo na opremo za obdelavo podatkov.	Delno, ni zaklepanj. Da. Delno, lesene pregrade. Delno. Da, temperatura in vlaga zraka.	**Predlog:** Organizacija naj pri zaščiti opreme izhaja iz ocene tveganj. Oprema naj bo nameščena tako, da bo tveganje pred naravnimi in drugimi nesrečami ter nepooblaščenim dostopom čim manjše. Organizacija naj postavi tudi pravila glede hranjenja v bližini informacijske opreme.	Vsi.
9.2.2	Zaščita pred energijskim tveganjem.	- Zaščita opreme pred prekinitvijo oskrbe z električno energijo - UPS, generator, glavno stikalo.	Da.	**Predlog:** Organizacija naj redno, najmanj pa enkrat letno, preveri delovanje naprav.	Vodstvo. Administrator sistema.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
9.2.3	Varovanje kabelskih vodov.	- Zaščita energetskih in telekomunikacijskih vodov pred poškodbami in možnostmi prestrezanja. - Ločevanje energetskih in telekomunikacijskih vodov zaradi motenj. - Jasno prepoznavne oznake na kablih in opremah.	Delno, ni zaklepanj prostorov. ? Ne.	**Predlog:** Prostori nadzornih in končnih točk naj se vedno zaklepajo.	Vodstvo. Administrator sistema.
9.2.4	Vzdrževanje opreme.	- Redno vzdrževanje opreme v skladu z navodili in priporočili proizvajalcev. - Vzdrževanje izvaja za to pooblaščeno osebje. - Dnevnik napak, preventivnih in korektivnih ukrepov.	Delno. Da, interni vzdrževalec. Ne.	**Predlog:** Organizacija naj opremo vzdržuje v skladu z navodili proizvajalca. Beležijo naj se dejanske okvare, popravila in preventivna vzdrževalna dela.	Pooblaščenec.
9.2.5	Varovanje opreme izven prostorov organizacije.	- Vodstvo mora odobriti uporabo opreme zunaj delovnih prostorov. - Varnost opreme zunaj delovnih prostorov enakovredna varnosti v podjetju.	Da. Da.		Vodstvo.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
9.2.6	Varno uničenje ali ponovna uporaba opreme.	- Varno prepisani ali fizično uničeni podatkovni nosilci z občutljivo vsebino.	Da, razkosanje ali prepisovanje z 0 bitom.	**Predlog:** Zgolj brisanje podatkov z medijev za popolno zaščito ne zadošča, zato naj uporabi razmagnetenje, razkosanje.	Administrator sistema.
9.2.7	Odstranitev lastnine.	- Opremo, informacije in programsko opremo se lahko odnese iz podjetja z ustrezno odobritvijo. - Občasne in redne kontrole opreme. - Seznanitev zaposlenih o pregledih.	Ne. Delno. Ne.	**Predlog:** Podjetje naj za iznos opreme in občutljivih dokumentov uvede uradna pooblastila. Organizacija naj ve, kje vse se njena oprema nahaja. Organizacija naj ima spisek vse opreme, ki se uporablja za delo od doma.	Vodstvo. Administrator sistema.

6.4.6 ISO 27001 – Upravljanje s komunikacijami in s produkcijo

V šestem poglavju je obravnavana varnost omrežij in računalnikov. Ločiti se mora testne in produkcijske zmogljivosti, potrebno je redno preverjanje varnostnih kopij pomembnih poslovnih informacij in programske opreme, varovanje prenosa podatkov znotraj in zunaj podjetja ter ohranjanje celovitosti procesov in komunikacij. Opredeljeni so tudi načini in postopki o uničenju nosilcev podatkov, katerih več ne potrebujemo.

Standard	**Sekcija**	**Kontrola (cilj)**	**Trenutno stanje**	**Rešitve / primeri dobre prakse**	**Odgovornost**
10.1	**POSTOPKI IN ODGOVORNOSTI PRODUKCIJE**				
10.1.1	Dokumentirani delovni postopki.	- V varnostni politiki določeni operativni postopki za arhiviranje, vzdrževanje opreme. - Pripravljena navodila za primer, če pride do napake pri izvajanju določenega opravila. - Omogočena in dosegljiva podpora, kamor se uporabniki obrnejo v primeru tehničnih težav. - Določen postopek ponovnega zagona sistema v primeru hujše napake. - Dokumentacija na voljo vsem, kateri jo potrebujejo.	Ni varnostne politike. Neformalna. Da. ? Da, interni strežnik podjetja.	Primer prijave incidenta - **Priloga <u>9.2</u>** **Predlog:** Organizacija naj po izdelavi varnostne politike vse v njej naštete postopke dokumentira in vzdržuje. Za vsak postopek naj se navede navodila kot solastništvo, ravnanje z informacijami, časovna razporeditev dela.	Vodstvo.
10.1.2	Upravljanje s spremembami.	- Vsa programska oprema podvržena strogi kontroli sprememb. - Načrtovanje in testiranje vseh sprememb. - Dnevniki vseh sprememb programske opreme. - Sporočanje podrobnosti o spremembah vsem odgovornim osebam. - Postopki za vrnitev v prejšnje stanje.	Ne. Da. Da. Da. Neformalno.	**Predlog:** Organizacija naj izdela postopke za nadzor in spremembe v produkciji. Vse spremembe naj se spremljajo, o njih pa naj se hrani natančne zapise.	Razvoj.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
10.1.3	Ločevanje nalog.	- Obveznosti in področja odgovornosti ločena tako, da se zmanjša možnost nepooblaščenih sprememb in uporabe informacij - ločene naloge upravljanja in izvajanja.	Da, vsak ima svoje pravice v računu.		Vodstvo.
10.1.4	Ločevanje razvojnih, testnih in produkcijskih zmogljivosti.	- Razvojni in testni programi ločeni od operativnih izvajanj. - Pravila za prenos programske opreme iz testnega v operativno okolje. - Razvojna orodja nedostopna v operativnem okolju. - Lastnosti testnega okolja podobne ali enake operativnemu okolju. - Različni uporabniški profili za testno in produkcijsko okolje.	Delno. Ne. Ne, so dostopna. Da. /	**Predlog:** Organizacija naj ločuje razvojno, testno in produkcijsko okolje. Kjer je to mogoče, naj so razvojno, testno in produkcijsko okolje ločeni tudi fizično, kar pomeni, da tečejo na različnih strežnikih. Testne verzije morajo imeti dostop do svojih baz podatkov. Te baze naj bodo karseda podobne tistim v operativnem okolju, le podatki morajo biti izmišljeni oziroma generirani avtomatično. Pripraviti je potrebno splošne kontrolne točke, s katerimi mora biti preverjana programska oprema v testnem okolju. V primeru, da je programska oprema v vseh točkah ustrezna, se lahko prenese v operativno okolje.	Vsi.
10.2	**UPRAVLJANJE STORITEV ZUNANJIH IZVAJALCEV**				
10.2.1	Izvajanje storitev.	- Pogodbe z zunanjimi izvajalci vsebujejo tudi kontrole in vsebino, ki se nanaša na varnost.	Ne. Dogovori sklenjeni na sestankih.	**Predlog:** Organizacija naj v pogodbo vključi tudi varnostne zaščite in delovne kontrole.	Vodstvo. GIS.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
10.2.2	Kontrola storitev zunanjih izvajalcev.	- Preverjanje in kontrola upoštevanja varnosti, storitev, poročil in zapisov zunanjih izvajalcev - (sestanki, obiski). - Postopki za reševanje problemov.	Da. Da.	Primer prijave incidenta - **priloga** **9.2**	Odgovoren.
10.2.3	Upravljanje sprememb storitev zunanjega izvajalca.	- Zunanjim izvajalcem se sporoča napake, katere smo odkrili v obstoječi storitvi. - Zunanji izvajalci redno pošiljajo popravke za obstoječe storitve.	Da. Napake beležijo interno in sklic sestanka z zunanjimi izvajalci. Da. V procesu izdelave redno. V produkciji se lahko stanje spremeni.		Odgovoren. GIS.
10.3	**NAČRTOVANJE IN PREVZEM SISTEMA**				
10.3.1	Upravljanje zmogljivosti.	- Spremljanje izkoriščenosti kapacitet in načrtovanje povečanja v prihodnosti.	Da.	Obrazec popisa sredstev - **Priloga** **9.6**	Vodstvo. Kadrovska. Administrator sistema.
10.3.2	Prevzem sistema.	- Kriteriji o sprejemljivosti novih sistemov, nadgradnjah in novih verzijah. - Preverjanje nove strojne in programske opreme pred uvajanjem. - Potrebna izobraževanja ob uvedbi novega sistema.	Da. Da. Da.		Vsi.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
10.4	**VAROVANJE PRED ZLONAMERNO KODO**				
10.4.1	Kontrole proti zlonamerni kodi.	- Ukrepi za zaščito pred uporabo zlonamerne programske kode. - Uporaba protivirusne programske opreme. - Redno obnavljanje protivirusne programske opreme. - Preverjanje prometa iz nezanesljivih omrežij. - Pravila za prepoved uporabe neodobrene programske opreme. - Dokumentirani postopki za snemanje datotek iz tujih in lastnih strežnikov. - Določene odgovornosti v primeru okužb.	Da. Da. Da. Ne. Ne. Ne. Ne.	Navodila nastavljanja protivirusnika - **Priloga 9.11** Dovoljena programska oprema - **Priloga 9.4** Prenos programske opreme - **Priloga 9.7** Ravnanje v primeru okužb - **Priloga 9.10** **Predlog:** Organizacija naj več naredi na področju ozaveščanja uporabnikov, saj je to najboljša pot do preventive. Uvedejo naj se postopki in odgovornosti za izvajanje zaščite proti zlonamerni kodi. Pripraviti dokument, s katerim se bodo uporabniki seznanili s tem, da na računalnike, ki so last podjetja, ne smejo nameščati dodatnih programov, brez da bi o tem obvestili odgovorno osebo. Uporabnike je potrebno tudi obvestiti, kakšen je postopek prenašanja datotek iz tujih strežnikov – vsako datoteko, ki jo prenesejo, naj preverijo s protivirusnim programom, preveriti	Vodstvo. Administrator sistema.

				je potrebno, ali je programska oprema plačljiva. Potrebno je obvestiti vse uporabnike, da v primeru okužbe ne ukrepajo po lastni presoji, ampak obvestijo sistemskega administratorja.	
10.4.2	Zaščita pred zlonamerno mobilno kodo.	- Ukrepi za zaščito pred uporabo zlonamerne mobilne kode – blokiranje izvrševanja programov brez vednosti uporabnika.	Ne.	**Predlog:** Organizacija naj uvede tovrstno zaščito na ravni operacijskega sistema in varnostnih nastavitev v domeni.	Vodstvo. Administrator sistema.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
10.5	**VARNOSTNE KOPIJE**				
10.5.1	Varnostne kopije.	- Redno arhiviranje ključnih poslovnih informacij. - Varno in ločeno hranjenje medijev podatkov od mesta kreiranja. - Redno preverjanje medijev za arhiviranje, če so informacije zapisane pravilno. - Beleženje napak v dnevnik dela. - Postopki za povrnitev v prvotno stanje. - Urnik izvajanja varnostnega kopiranja.	Da. Ne. Da. Da. Da. Da.	Primer prijave incidenta - **Priloga <u>9.2</u>** Zadolžitve v primeru izpada IS - **Priloga <u>9.3</u>** **Predlog:** Varnostne kopije naj se hranijo v ognjevarnem sefu, ločene od sistema, ki se varuje. Kopije naj bodo podvržene istemu nivoju varnosti, kakor ga ima njen izvirnik.	Administrator sistema. Operativa.
10.6	**UPRAVLJANJE OMREŽNE VARNOSTI**				
10.6.1	Kontrole omrežja.	- Ločeno omrežje. - Ustrezni ukrepi za upravljanje oddaljene opreme. - Ustrezni ukrepi za zagotavljanje zaupnosti in celovitosti podatkov pri prenosu v javnem omrežju - VPN,... .	Da. Da. Da.		Administrator sistema.

10.6.2	Varnost omrežnih storitev.	- Varnostna pravila o mrežnih storitvah. - Obvezna uporaba požarnih zidov. - Beleženje vdorov - IDS.	Ne. Delno. Ne.		Administrator sistema.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
10.7	**RAVNANJE Z NOSILCI PODATKOV**				
10.7.1	Ravnanje s prenosnimi računalniškimi mediji.	- Postopki za upravljanje s prenosnimi mediji ─ trakovi, diski ...	Ne.	**Predlog:** Organizacija naj dokumentira vse postopke in pooblastila v zvezi s prenosnimi računalniškimi mediji. Dokumentirajo naj se tudi postopki brisanja medijev. Pri proizvajalcu je potrebno preveriti, kakšna je življenjska doba medijev, na katerih se shranjujejo podatki oziroma varnostne kopije.	Vodstvo. Administrator sistema.
10.7.2	Uničenje medijev.	- Varna in zanesljiva odstranitev neuporabnih medijev - sežig, raztrganje. - Beleženje odstranjenih medijev z občutljivo vsebino.	Da. Ne.	**Predlog:** Pripraviti dokument, v katerem bo zapisan datum, odgovorna oseba za uničenje, in kratek opis vsebine uničenih medijev.	Odgovorni.
10.7.3	Ravnanje z informacijami.	- Označevanje medijev, da se lahko razbere vsebina in stopnja zaupnosti. - Preverjanje pravilnosti zapisa podatkov. - Seznam shranjenih podatkov – evidenca izposoje, prostor hrambe.	Delno. Da. Delno.	**Predlog:** Pripraviti nalepke za medije in na njih napisati lastnika, ključne besede o vsebini medija in datum nastanka. Mediji ne smejo biti dostopni nepooblaščenim osebam. Priprava razpredelnice oziroma programske opreme, v kateri se bo vodila evidenca medijev. Za vsak	Odgovorni.

				medij je potrebno napisati, kje je shranjen, kdo je odgovoren za opravljanje z njim, ali je na voljo za izposojo in kdo in kdaj si ga je izposodil.	
10.7.4	Varovanje sistemske dokumentacije.	- Zaščita sistemske dokumentacije pred nepooblaščenim dostopom – gesla, kriptiranje, VPN ... - Priročnik za delo s sistemom. - Informacije o konfiguraciji sistema.	V kuverti pri direktorju. Ne. Ne.		Vodstvo. Administrator sistema.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
10.8	**IZMENJAVA INFORMACIJ**				
10.8.1	Pravilnik o izmenjavi informacij.	- Pravilnik za izmenjavo podatkov in programske opreme. - Kriptiranje podatkov. - Prisotnost osebe pri tiskanju z javno dostopnim tiskalnikom.	Neformalno. Da. Da.	**Predlog:** Dokumentirati je potrebno postopke za zavarovanje informacij. V dokument je potrebno napisati, kako opremiti podatke pri shranjevanju in prenosu, in poskrbeti za ustrezno izobraževanje kadrov, da se bodo predpisanega tudi držali.	Vodstvo. Računalniška soba.
10.8.2	Sporazumi o izmenjavi informacij.	- Sporazum vključuje varnostne zahteve na osnovi občutljivosti poslovnih podatkov. - Odgovornosti in obveznosti v primeru incidentov pri varovanju informacij. - Sistem za označevanje občutljivih informacij.	Da. Delno. /	Primer prijave incidenta - **Priloga <u>9.2</u>**	Vodstvo. Odgovorni.
10.8.3	Varnost medijev med transportom.	- Upoštevanje tveganja med prenosom in transportom medijev.	Da.		Vodstvo.

10.8.4	Elektronska izmenjava informacij.	- Elektronska sporočila zaščitena pred nepooblaščenim dostopom in spremembami. - Strožje varnostne kontrole za dostopanje do elektronskih sporočil iz javnega omrežja. - Elektronsko podpisovanje elektronske pošte in šifriranje.	Da. Da. Da.		Vodstvo. Odgovorni. Računalniška soba.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve/primeri dobre prakse	Odgovornost
10.8.5	Poslovni informacijski sistemi.	- Smernice za izmenjavo podatkov med različnimi poslovnimi informacijskimi sistemi.	Ne.	**Predlog:** Razvije naj se politika in postopki za zaščito informacij, povezanih z medsebojnim povezovanjem poslovnih informacijskih sistemov.	Vodstvo. Računalniška soba.
10.9	**STORITVE ELEKTRONSKEGA POSLOVANJA**				
10.9.1	Elektronsko trgovanje.	- Politika elektronskega poslovanja. - Zaščita informacij med prehodi v javnih omrežjih - šifriranje, podpisi. - Pogodba o elektronskem poslovanju med partnerji vključuje pogoje poslovanja in varnostne zahteve. - Preverjanje pristnosti in avtorizacije.	Neformalno. Da. Da. Da.	Primer politike e-pošte - **Priloga** **9.12**	Vodstvo. Administrator sistema. Računalniška soba.
10.9.2	On-line poslovanje.	- Šifrirani in zaščiteni prenosi informacij med strankami – digitalni podpisi.	Da.		Odgovorni. Računalniška soba.
10.9.3	Javno dostopne informacije.	- Preverjanje javnih informacij pred objavo. - Javne objave informacij zaščitene pred nepooblaščenimi	Da. Da.	Zahtevek dodelitve uporabniških pravic - **Priloga** **9.8**	Vodstvo. Administrator sistema.

		spremembami. - Postopki dostopa do zaupnih vsebin.			

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
10.10	**NADZOR**				
10.10.1	Preverjanje prijav v sistem.	- Dnevniki prijav v sistem vsebujejo informacije o uporabnikovih dejavnostih, izjemne dogodke in dogodke s področja varnosti.	Ni na nivoju podjetja. Lokalni dnevniki na PC-jih.		Administrator sistema.
10.10.2	Nadzor uporabe sistema.	- Postopki za spremljanje uporabe informacijskih sredstev - Nadzor s pomočjo programske opreme.	Delno.	**Predlog:** S spremljanjem uporabe informacijskih sredstev in analiziranjem napačnih prijav uskladimo nadzor sistema s standardom.	Administrator sistema.
10.10.3	Varovanje podatkov v operativnih dnevnikih.	- Zaščita operativnih dnevnikov pred spreminjanjem in brisanjem.	Da.		Administrator sistema.
10.10.4	Dnevnik administratorja in operaterja.	- Beleženje aktivnosti administratorja in operaterja v dnevnik.	Lokalni dnevniki na PC-jih.		Vodstvo.
10.10.5	Beleženje okvar.	- Beleženje in analiziranje napačnih prijav v sistem.	Delno.	Primer prijave incidenta - **Priloga** **9.2** Zadolžitve v primeru izpada IS - **Priloga** **9.3**	Odgovorni.
10.10.6	Sinhronizacija sistemskega časa.	- Sinhronizacija sistemskega časa z ustreznim izvorom točnega časa.	Da.		Administrator sistema.

6.4.7 ISO 27001 – Nadzor dostopa

Dostop do informacij in poslovnih procesov mora temeljiti na poslovnih in varnostnih zahtevah organizacije. Sedmo poglavje standarda govori o tem, kako se mora ravnati z dostopi do sistema, o dodeljevanju pravic, gesel, o varnosti podatkov in računalniške opreme, ko ti niso v uporabi, iskanju in razpoznavanju nepooblaščenih dostopov.

Standard	**Sekcija**	**Kontrola (cilj)**	**Trenutno stanje**	**Rešitve / primeri dobre prakse**	**Odgovornost**
11.1	**ZAHTEVE ZA NADZOR DOSTOPA**				
11.1.1	Politika nadzora dostopa.	- Poslovne zahteve za kontrolo dostopa definirane in dokumentirane. - Dokument vsebuje pravila in pravice vsakega uporabnika ali skupine uporabnikov.	Ne, ni politike nadzora dostopa.	**Predlog:** Organizacija naj izdela politiko nadzora dostopa, ki naj bo skladna s poslovnimi potrebami.	Vodstvo.
11.2	**RAVNANJE Z DOSTOPNIMI PRAVICAMI**				
11.2.1	Registracija uporabnika.	- Formalni postopki za vpis in izpis uporabnikov za dodelitev dostopa sistemov in storitev.	Delno, vpis je opisan, izpis pa ne.	_Zahtevek dodelitve uporabniških pravic - **Priloga 9.8** Obrazec pooblastil za dostop do rač.sistemov- **Priloga 9.9** **Predlog:** Uporabnike je potrebno umakniti iz seznama takoj, ko so premeščeni na drugo delovno mesto ali ko zapustijo organizacijo.	Vodstvo. Administrator sistema.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
11.2.2	Upravljanje posebnih pravic.	- Dodelitev in uporaba posebnih pravic omejena in kontrolirana - pravice sistemskega administratorja ... - Potrebna formalna odobritev.	Delno. Da.	**Predlog:** Uporabnikov s posebnimi pravicami naj bo čim manj. Organizacija naj definira postopke pridobivanja in odvzemanja posebnih pravic serviserjem v primerih okvar.	Vodstvo.
11.2.3	Ravnanje z uporabniškimi gesli.	- Dodeljevanje in spreminjanje gesel formalno kontrolirano. - Uporabnik podpiše izjavo o zaupnosti gesel.	Ne, definirano naj bo v politiki varovanja informacij.	**Predlog:** Organizacija naj definira postopek sporočanja začasnih gesel uporabnikom, ob upoštevanju možnosti razkritja in izkoriščanja. Geslo naj se vedno izda za eno osebo, kajti pri souporabi je odgovornost težko določiti. Gesla naj se zaščitena hranijo na centralnem mestu.	Vodstvo.
11.2.4	Pregled uporabniških pravic do dostopa.	- Postopek občasnega preverjanja dostopnih pravic.	Ne, definirano naj bo v politiki varovanja informacij.	**Predlog:** Organizacija naj definira postopek za redno pregledovanje uporabniških pravic do dostopa. Posebej je to pomembno za uporabnike s posebnimi pravicami, ki naj se jih kontrolira vsake 3 mesece. Ostale uporabnike pa vsakih 6 mesecov.	Vodstvo.
11.3	**ODGOVORNOSTI UPORABNIKOV**				
11.3.1	Uporaba gesel.	- Uporabniška navodila o izbiri in vzdrževanju gesel.	Delno, ni politike ravnanja z gesli. Na internem strežniku podjetja je manjše navodilo o ustrezni dolžini in kompleksnosti gesla.	**Predlog:** Organizacija naj izdela politiko za ravnanje z gesli, kjer naj bo natančno opisano, na koliko časa naj se gesla menjavajo, kako naj bodo sestavljena, kakšna naj bo dolžina. Prepove naj se souporaba gesel. Če se uporabniki	Vodstvo.

				prijavljajo v več različnih sistemih, se priporoča uporaba enega kakovostnega gesla.	
11.3.2	Zaščita uporabnikove opreme.	- Uporabniki opozorjeni na odgovornost in varnostne zahteve ter postopke za zaščito opreme – ponovne prijave v sistem, časovne omejitve ...	Delno.	**Predlog:** Uporabniki naj svojo opremo ob odsotnosti primerno zaščitijo. Takoj ko prenehajo z delom, naj sejo s strežnikom prekinejo, računalnik pa zavarujejo z mehanizmom za zaklepanje. Naj uporabijo ohranjevalnik zaslona, ki naj bo zavarovan z dovolj dobrim geslom.	Vodstvo.

Standard	**Sekcija**	**Kontrola (cilj)**	**Trenutno stanje**	**Rešitve / primeri dobre prakse**	**Odgovornost**
11.3.3	Politika čiste mize in čistega zaslona.	- Avtomatsko zaklepanje ekrana. - V odsotnosti uslužbenca zaupni dokumenti zaklenjeni.	Da. Da.		Vodstvo.
11.4	**NADZOR DOSTOPA DO OMREŽJA**				
11.4.1	Politika uporabe omrežnih storitev.	- Predpisi o uporabi omrežja in omrežnih storitev.	Ne, izdela naj se načrt za varovanje omrežnih virov.	Obrazec pooblastil za dostop do rač.sistemov - **Priloga 9.9** Primer politike e-pošte - **Priloga 9.12** **Predlog:** Organizacija naj primerno nadzira uporabo omrežnih virov. Natančno naj se opredeli, kakšen dostop je posameznim uporabnikom dovoljen. Uporabniki naj imajo v omrežnih sistemih dostop le do virov, ki jih potrebujejo za opravljanje svojega dela. Opredeli naj se,	Vodstvo.

				kdo lahko dostopa do operacijskega sistema glavnih strežnikov.	
11.4.2	Preverjanje pristnosti za zunanje povezave.	- Mehanizmi preverjanja pristnoti zunanjih povezav - VPN dostop ...	Da.		Vodstvo. Računalniška soba. Administrator sistema.
11.4.3	Prepoznavanje opreme v omrežju.	- Preverjanje pristnosti vozlišča pri oddaljeni povezavi - programska oprema za samodejno prepoznavanje opreme.	Da.		Vodstvo. Administrator sistema.
11.4.4	Zaščita oddaljenih diagnostičnih in konfiguracijskih vrat.	- Vrata za diagnostiko, ki so namenjena za komunikacijo med sistemom in serviserjem, ustrezno varovana in kontrolirana z varnostnim mehanizmom.	Da.	**Predlog:** Organizacija naj na določeno obdobje preveri varno in uspešno delovanje diagnostičnih vrat.	Vodstvo. Administrator sistema.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
11.4.5	Ločevanje v omrežjih.	- Ločena omrežja ločena med seboj z varovalnimi mehanizmi – požarni zidovi.	Da.		Administrator sistema.
11.4.6	Kontrola omrežnih povezav.	- Kontrole za deljena omrežja čez meje podjetja in povezovanje omrežij – kontrole preko požarnega zidu, usmerjevalnika.	Ni potrebe, ker ni deljenega omrežja.	Primer politike e-pošte - **Priloga <u>9.12</u>**	Administrator sistema.
11.4.7	Kontrola omrežnega usmerjanja.	- Računalniške povezave in pretok podatkov ne kršita politike dostopa do poslovnih aplikacij. - Lahko se ugotovi izvor in ponor usmeritve – NAT tabela.	? Da.	**Predlog:** Organizacija naj pri ponudniku interneta preveri, kako zagotavlja celovitost, razpoložljivost in neprekinjeno uporabo poti. Preveri naj tudi alternativne poti v primeru izpada primarnega voda.	Administrator sistema.

11.5	**NADZOR DOSTOPA DO OPERACIJSKEGA SISTEMA**				
11.5.1	Samodejno prepoznavanje terminala.	- Mehanizem za avtomatsko prepoznavanje delovne postaje za preverjanje pristnosti povezave. - Evidentiranje vseh prijav – uspešnih in neuspešnih.	Ne. Da.	**Predlog:** Organizacija naj za dostop do občutljivih aplikacij uporablja samodejno prepoznavanje terminalov.	Vodstvo. Administrator sistema.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
11.5.2	Prepoznavanje in overjanje uporabnikov.	- Vsak uporabnik ima enolično dodeljen in prepoznaven račun.	Da.		Vodstvo.
11.5.3	Upravljanje z gesli.	- Politika upravljanja z gesli – osebna gesla, periodično spreminjanje gesel, šifrirano shranjevanje gesel, dolžina gesla, kompleksnost gesla.	Delno, ni politike upravljanja z gesli. Osnovni napotki za ustreznost gesla so.		Vodstvo. Administrator sistema. Računalniška soba.
11.5.4	Raba sistemskih pripomočkov.	- Raba sistemskih sredstev in komercialnih programov je omejena in pod nadzorom. - Uporaba posebnih programskih orodij je omogočena samo pooblaščenim osebam.	/ /	Obrazec pooblastil za dostop do rač.sistemov - **Priloga** **<u>9.9</u>**	Vodstvo. Administrator sistema.
11.5.5	Prekinitev seje.	- Neaktiven proces na delovni postaji se po določenem času samodejno prekine.	Da.		Administrator sistema.
11.5.6	Časovna omejitev povezave.	- Časovna omejitev povezave za aplikacije z visoko stopnjo tveganja – določeni časovni intervali …	Da, običajno 60 minut v stanju mirovanja.		Vodstvo. Administrator sistema.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
11.6	**NADZOR DOSTOPA DO APLIKACIJ IN INFORMACIJ**				
11.6.1	Omejitev dostopa do informacij.	- Omejitve dostopa do aplikacij za posameznike ali skupine uporabnikov – določene pravice za vsakega uporabnika.	Da.		Vodstvo. Sistemski administrator.
11.6.2	Osamitev občutljivih sistemov.	- Delovanje občutljivih sistemov v izoliranem računalniškem okolju - varna soba, omejen dostop, deljeno omrežje in pravice ...	Ne. Strežniki v svoji sobi, vsi imajo dostop do sobe, isto omrežje, dostop z digitalnimi ključi – SSH.	**Predlog:** Organizacija naj na osnovi analize tveganj poišče najbolj občutljive sisteme in zanje preveri smiselnost uvedbe te kontrole.	Administrator sistema.
11.7	**MOBILNA RAČUNALNIŠKA OPREMA IN ODDALJENO DELO**				
11.7.1	Prenosni računalniki.	- Upoštevanje tveganj pri delu s prenosnimi računalniki. - Uporaba šifriranj na mobilnih napravah, protivirusniki ...	Da. Da.		Vodstvo.
11.7.2	Delo na daljavo.	- Politika za oddaljeno delo – VPN, šifriranje, digitalni podpisi, pooblaščeni dostopi ...	Da.		Vodstvo.

6.4.8 ISO 27001 – Nakup, razvoj in vzdrževanje informacijskega sistema

Osmo poglavje standarda je namenjeno razvoju in vzdrževanju informacijskega sistema še posebej z vidika varnosti aplikacij, datotek preko kriptiranja. Poglavje zajema vgrajevanje varnosti v informacijske sisteme, zaščito zaupnosti, verodostojnosti in celovitosti informacij, preprečevanje izgub, zlorabe in sprememb podatkov.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
12.1	**VARNOSTNE ZAHTEVE IS**				
12.1.1	Analiza in opredelitev varnostnih zahtev.	- Upoštevanje varnostnih zahtev pri načrtovanju novih sistemov in širitvi obstoječih.			Vodstvo.
12.2	**PRAVILNA OBDELAVA V APLIKACIJAH**				
12.2.1	Preverjanje vhodnih podatkov.	- Potrjevanje vhodnih podatkov za zagotavljanje pravilnosti in ustreznosti – preverjanje vhodnih podatkov med vnosom (dolžina, pravilnost znakov ...).	Da.		Vodstvo. Razvoj.
12.2.2	Nadzor notranje obdelave podatkov.	- Definirana področja tveganja znotraj obdelav podatkov. - V pomembnejših aplikacijah vgrajena preverjanja, ki odkrivajo napačno obdelavo podatkov.	Da.		Vodstvo. Razvoj.
12.2.3	Celovitost sporočil.	- Preverjanje pristnosti in celovitosti sporočil med elektronsko izmenjavo podatkov – kriptografija ...	Samo tam, kjer se povezujejo sistemi preko interneta, sicer ne.	**Predlog:** Organizacija naj na osnovi analize tveganj ugotovi smiselnost uporabe overjanja sporočil. Uvedba je smiselna predvsem tam, kjer se zahteva, da je sporočilo res poslala oseba, ki to trdi, in da sporočila med prenosom ni nihče spreminjal.	Razvoj.

12.2.4	Preverjanje izhodnih podatkov.	- Preverjanje izhodnih podatkov, da so shranjene ustrezno in pravilno.	Da.		Razvoj.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
12.3	**KRIPTOGRAFSKE KONTROLE**				
12.3.1	Politika rabe šifrirnih kontrol.	- Politika rabe kriptografskih kontrol. - Pri razvoju programske opreme se uporablja šifriranje, kjer je to potrebno.	Ne, razvoj politike kriptografije. Da.	**Predlog:** Organizacija naj razvije politiko uporabe kriptografskih kontrol za zaščito svojih informacij. Za aplikacije določimo posebne standarde za šifriranje, definiramo tveganja in postopke za testiranje.	Vodstvo. Razvoj.
12.3.2	Upravljanje z digitalnimi ključi.	- Uporaba sistema, ki podpira uporabo šifrirnih metod v podjetju – generiranje, shranjevanje in arhiviranje ključev. - Dokumentiranje vsake izdaje ključa.	Ni potrebe za opisano podjetje.		Vodstvo.
12.4	**VAROVANJE SISTEMSKIH DATOTEK**				
12.4.1	Kontrola programske opreme.	- Kontrolni mehanizmi za namestitev programske opreme na operativne sisteme – nadgradnje programske opreme izvrši pooblaščeni. - Postopki za povrnitev v obstoječe stanje. - Dnevnik posodobitev programske opreme.	Da.	Dovoljena programska oprema - **Priloga <u>9.4</u>** Prenos programske opreme - **Priloga <u>9.7</u>**	Administrator sistema.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
12.4.2	Zaščita testnih podatkov sistema.	- Sistemski testni podatki zaščiteni in pod nadzorom. - Pooblastila za testiranje. - V testne namene uporaba produkcijskih podatkov se izogne, uporabi se testne podatke.	Ne. Delno zaščiteni podatki (gesla v bazi podatkov, ki pa jih večinoma poznamo). Še vedno nimamo popolnoma testnih podatkov.	Obrazec pooblastil za dostop do rač.sistemov - **Priloga** **9.9** **Predlog:** Organizacija naj izdela načrte za testiranje. Za namene testiranja in razvoja je potrebno ustvariti drugačne uporabniške račune za bazo podatkov in uporabiti drugačna uporabniška imena in gesla kot v produkciji. V primeru, da se uporabljajo zasebni ali občutljivi podatki, morajo biti ti podatki spremenjeni do nerazpoznavnosti.	Razvoj.
12.4.3	Nadzor dostopa do izvorne kode.	- Stroga kontrola dostopa do izvorne programske kode. - Dnevnik dostopa in sprememb do izvorne kode.	Delno. Dostop do izvorne kode (CVS) z gesli, dnevnik sprememb, dnevnika dostopa pa ni.	**Predlog:** Organizacija naj beleži dostope do izvorne kode in redno spremlja. Če se uporablja temu primeren strežnik za upravljanje z izvorno kodo, so vsi dnevniki dostopni na tem strežniku. Tako, da ni potrebno voditi posebne dokumentacije glede te točke.	Razvoj.
12.5	**VARNOST V PROCESU RAZVOJA IN PODPORE**				
12.5.1	Nadzorovanje sprememb.	- Strogi kontrolni postopki pri implementaciji sprememb informacijskega sistema. - Vodenje verzij programske opreme.	Da. Da.	Obrazec pooblastil za dostop do rač.sistemov - **Priloga** **9.9**	Vodstvo. Odgovorni.

12.5.2	Tehnični pregled sistemskih sprememb.	- Kontrola in preizkušanje aplikacij po uvedbi sistemskih sprememb – novi operacijski sistem.	Da.		Odgovorni.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
12.5.3	Omejitve sprememb programske opreme.	- Spremembe programske opreme se omeji samo na potrebne spremembe pod nadzorom. - Dokumentiranje sprememb programske opreme.	Ne, določiti postopke pri spremembah programske opreme.	**Predlog:** Pred vsako spremembo naj se izdela analiza tveganj, s katero naj se ugotovi vpliv spremembe na ranljivost programa.	Vodstvo.
12.5.4	Uhajanje informacij.	- Preverjanje, da se po nadgradnji sistema ne pojavijo skrivni prehodi, ki omogočajo uhajanje informacij - pregledi sistema, sledenje dostopov ...	Da. Log datoteke, testiranje pravic uporabnikov, bocrep logi.		Razvoj. Odgovorni.
12.5.5	Razvoj programske opreme pri zunanjih izvajalcih.	- Programsko opremo, ki jo razvijajo zunanji izvajalci, se preverja v skladu z licenčnimi dogovori. - Preverjanje kakovosti programske opreme. - Preverjanje pred instalacijo.	Da. Da. Da.		Vodstvo. Razvoj.
12.5.6	Upravljanje tehnične ranljivosti.	- Popis programske opreme v podjetju – verzija, vrsta oprema, zagotavljanje pravočasnih informacij, šibke točke.	Da, interni strežnik podjetja.	Obrazec popisa sredstev - **Priloga 9.6**	Vodstvo. Odgovorni.

6.4.9 ISO 27001 – Upravljanje incidentov pri varovanju informacij

Namen devetega poglavja standarda je določanje postopkov za ravnanje in upravljanje ob uresničitvi grožnje varnosti. Pripravljene morajo biti formalne poti za poročanje o vseh uresničitvah groženj varnosti, ki bi lahko vplivale na varnost premoženja organizacije.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
13.1	**POROČANJE O DOGODKIH PRI VAROVANJU INFORMACIJ**				
13.1.1	Poročanje ob uresničitvi grožnje varnosti.	- Formalni postopki za hitro poročanje o napakah po ustreznih poteh - obvestitev vodje, ustrezna komunikacijska sredstva. - Disciplinsko kaznovanje v primeru uhajanja informacij.	Neformalno. Ne.	Primer prijave incidenta - **Priloga** <u>**9.2**</u> Zadolžitve v primeru izpada IS - **Priloga** <u>**9.3**</u> Ravnanje v primeru okužb – **Priloga** <u>**9.10**</u> **Predlog:** Za poročanje predpišemo ustrezne postopke in dosledno zahtevamo njihovo uporabo. V primeru kršitev uvedemo disciplinski postopek zoper kršitelja. Vsak incident naj se prijavi, izdela naj se analiza in ugotovi vzrok. Na osnovi tega naj se vpeljejo ukrepi za preprečevanje ponovnega pojava incidenta.	Vsi.
13.1.2	Poročanje o slabostih pri varovanju.	- Postopek ali navodilo za poročanje o ranljivosti sistema in o varnostnih grožnjah.	Neformalno.	Primer prijave incidenta - **Priloga** <u>**9.2**</u>	Vsi.

				Predlog: Zaposlene naj se spodbuja, da prijavijo vse pomanjkljivosti oziroma sume nanje. O vseh pomanjkljivostih mora biti obveščen pooblaščenec za informacijsko varnost.	
13.2	**UPRAVLJANJE INCIDENTOV**				
13.2.1	Odgovornosti in postopki.	- Postopki za poročanje o različnih napakah programske opreme.	Neformalni.	Primer prijave incidenta - **Priloga <u>9.2</u>**	Vodstvo.
13.2.2	Učenje iz napak.	- Mehanizmi ocene tipa, obsega in višine nastalih stroškov ob grožnji varnosti.	Ne.	**Predlog:** Organizacija naj uvede mehanizme, s katerimi lahko izmeri in spremlja vrsto, obseg in stroške incidentov in okvar. S tem naj se ugotovijo ponavljajoči incidenti in tisti, ki organizacijo stanejo največ. Tako se omeji pogostost in škoda incidentov.	Vodstvo.
13.2.3	Zbiranje dokazov.	- Postopki za zbiranje dokazov ob uresničitvi grožnje varnosti.	Ne.	Primer prijave incidenta - **Priloga <u>9.2</u>** **Predlog:** Organizacija naj izdela postopke za zbiranje dokazov, ki zagotavlja njihovo ustrezno kakovost. Dokazi naj se začnejo zbirati takoj ob odkritju incidenta v primeru, če bi se šlo na sodišče.	Vodstvo.

6.4.10 ISO 27001 – Upravljanje neprekinjenega poslovanja

Deseto poglavje se nanaša na pomembnost zagotavljanja neprekinjenega poslovanja in na zaščito kritičnih poslovnih procesov pred večjimi okvarami in nesrečami. Implementirano mora biti tako, da zmanjšuje posledice nepričakovanih prekinitev in varnostnih napak. Vse kritične napake in prekinitve moramo analizirati in z izsledki analiz dopolniti scenarije naključnih, nepredvidenih dogodkov.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
14.1	**VIDIKI UPRAVLJANJA NEPREKINJENEGA POSLOVANJA**				
14.1.1	Proces neprekinjenega poslovanja.	- Postopek za razvoj in vzdrževanje neprekinjenega poslovanja v celotnem podjetju vključno z informacijsko varnostjo.	Ne, definirati v politiko varovanja informacij.	**Predlog:** Organizacija naj analizira tveganja in posledice ter na osnovi tega izdela načrt neprekinjenega poslovanja. Obseg načrta naj bo skladen z varnostnimi in poslovnimi zahtevami.	Vodstvo.
14.1.2	Neprekinjeno poslovanje in ocena tveganja.	- Dogodki, ki lahko povzročijo prekinitev poslovanja, kakšna je stopnja tveganja in obstoj strategije za pristop.	/		Vodstvo.
14.1.3	Razvoj in implementacija načrta stalnega poslovanja.	- Načrti za obnovo poslovanja po prekinitvi poslovnega procesa.	Ne.	**Predlog:** Načrt mora pokrivati vse vitalne in kritične faze poslovnega procesa in akcije, ki so potrebne, da se poslovni proces vzpostavi v delujoče stanje. Če načrta ni, ni testiran ali ne deluje, ko je aktiviran, se lahko zgodi, da se delujoče stanje ne vzpostavi nikoli več.	Vodstvo.
14.1.4	Okvirni načrt neprekinjenega poslovanja.	- Skupen okvir za načrtovanje neprekinjenega poslovanja. - Redno preverjanje in vzdrževanje načrta stalnega poslovanja.	Ne, izdelati načrt neprekinjenega poslovanja.		Vodstvo.

14.1.5	Testiranje, vzdrževanje in ponovno ocenjevanje načrta neprekinjenega poslovanja.	- Redno testiranje načrtov neprekinjenega načrtovanja za zagotavljanje njihove ažurnosti in učinkovitosti.	Ne, izdelati načrt neprekinjenega poslovanja.	Primer obrazca preverjanja dokumentacije – **Priloga** **9.5** **Predlog:** Če načrt ni testiran ali ne deluje, ko je aktiviran, se lahko zgodi, da se delujoče stanje ne vzpostavi nikoli več. Vodstvo in osebje morata poznati in razumeti svoje vloge v izvajanju načrta. Če uporabnik svojih vlog ne pozna, lahko tudi pri testiranem načrtu neprekinjenega poslovanja pride do zastojev in nedelovanja.	Vodstvo. Odgovorni.

6.4.11 ISO 27001 – Usklajenost

Enajsto poglavje standarda pa obravnava usklajenost informacijskega sistema z zakonodajo, tako na področju pravnih zahtev, kot tudi varnostnih pregledov informacijskega sistema.

Standard	**Sekcija**	**Kontrola (cilj)**	**Trenutno stanje**	**Rešitve / primeri dobre prakse**	**Odgovornost**
15.1	**USKLAJENOST Z ZAKONSKIMI ZAHTEVAMI**				
15.1.1	Prepoznavanje veljavne zakonodaje.	- Statutarne, pravne in pogodbene zahteve eksplicitno definirane in dokumentirane.	Da. Akti podjetja.		Vodstvo.
15.1.2	Zaščita intelektualne lastnine (ZIL).	- Postopki o uporabi avtorskih del, zaščitnih znamk. - Programska oprema se uporablja v skladu z dogovorom o pravici do uporabe.	Da, vendar ni nadzora. Da, vendar ni nadzora.	Dovoljena programska oprema - **priloga 9.4** **Predlog:** Organizacija naj strogo nadzira uporabo programske opreme. Vzdržujejo naj se dokumenti o vsem programskem inventarju posameznega sistema. Odgovorni se morajo zavedati, da so lahko za zlorabo intelektualne lastnine kazensko odgovorni.	Vodstvo.
15.1.3	Varovanje zapisov podjetja.	- Pomembni zapisi o podjetju ustrezno zaščiteni pred izgubo in poškodbami – varnostne kopije, arhiviranje.	Da.		Vodstvo.
15.1.4	Zaščita podatkov in varovanje osebnih podatkov.	- Postopki za varovanje in zaščito osebnih podatkov, ki so v skladu z veljavno zakonodajo.	Da. Interna navodila.		Vodstvo. Odgovorni.
15.1.5	Preprečevanje zlorab med obdelavo podatkov.	- Obvezna odobritev vodstva za nepooblaščeno in neslužbeno obdelavo podatkov.	Da.	Obrazec izjave o zaupnosti - **Priloga 9.1**	Vodstvo.

Standard	Sekcija	Kontrola (cilj)	Trenutno stanje	Rešitve / primeri dobre prakse	Odgovornost
15.1.6	Urejanje postopkov šifriranja.	- Šifriranje v skladu s predpisi področja in državnimi predpisi.	Kritični javni strežniki uporabljajo SSL na internih strežnikih občin brez SSL-ja.	**Predlog:** Organizacija naj preveri pravne in zakonske zahteve glede kriptografije. Posebej je potrebno paziti pri uporabi kriptografije v poslovanju s tujino, ker ni nujno, da sta zakonodaji kompatibilni.	Vodstvo. Razvoj.
15.2	**SKLADNOST Z VARNOSTNIMI POLITIKAMI IN STANDARDI**				
15.2.1	Skladnost z varnostno politiko in standardi.	- Vsa področja podjetja so predvidena za redno preverjanje skladnosti z varnostno politiko podjetja.	Ne, nima varnostne politike.	**Predlog:** Po uvedbi varnostne politike naj organizacija zagotovi izvajanje vseh varnostnih postopkov, njihovo redno pregledovanje in zagotavljanje skladnosti.	Vodstvo. Odgovorni.
15.2.2	Preverjanje tehnične ustreznosti.	- V sistemih redno preverjanje usklajenosti z varnostnimi standardi.	Ne, potrebna izdelava načrta za preverjanje tehnične združljivosti.	**Predlog:** Pogostost izvajanja celovitih tehničnih pregledov naj se določi na osnovi analize tveganj. Pregledi naj bodo dokumentirani.	Administrator sistema.
15.3	**PRESOJA IS**				
15.3.1	Preverjanje sistema.	- Presoja IS je načrtovana in ne prekinja poslovnega procesa.	Da.		Vodstvo.
15.3.2	Zaščita orodij za preverjanje IS.	- Dostop do orodij za preverjanje IS-ja ustrezno zavarovano, da se prepreči zlorabe orodja – ločitev od razvojnih in produkcijskih sistemov.	Ni potrebe za opisano podjetje.		Vodstvo.

6.5 Uspešnost programa za varovanje informacij

Kot zaključek celotnega popisa informacijske varnosti v podjetju »X« in dajanju predlogov za izboljšave naj navedem nekaj ključnih komponent uspešnega programa za varovanje informacij, katere so nujne v vsakem podjetju. Ta področja so:

- program za varovanje informacij mora biti last direktorja podjetja,
- odgovornost varovanja informacij je predana osebju z vodilnih položajev,
- ustanovitev odbora za nadzor in vodenje varovanja informacij,
- uvedba postopkov merjenja za upravljanje programa,
- izdelava tekočega načrta za izboljšanje varnosti,
- izvedba neodvisnega pregleda programa za varovanje informacij,
- računalniško okolje razdeljeno na področja,
- varnostni program naj se začne z osnovami in nato naj se ga izboljšuje,
- varovanje informacij naj bo bistvena naložba v podjetju.

7. Sklepne ugotovitve

Informacije, ki jih podjetja uporabljajo, morajo biti točne, zanesljive in pravočasne. Take informacije pa zagotavlja le dobro urejeno varovanje informacij. Rešitev na področju informacijske varnosti je več. Med najbolj razširjenimi je serija standardov ISO/IEC 27000, ki omogoča izboljšanje informacijske varnosti. Prednosti, ki jih s standardom pridobimo, so predvsem te, da so v standardu zajete aktivnosti in dobre prakse pri upravljanju informacijske varnosti. Slabost pa je v tem, da vzpostavitev procesov, katerih rezultat bo usklajena in učinkovita varnostna politika, zahteva pripravo ogromnega števila predpisov, navodil in evidenc. Vendar pa standardizacija na nivoju tehničnih ukrepov ne zagotavlja ustrezne zaščite informacijskih tehnologij in informacijskih sistemov. Bistveno tveganje še vedno predstavlja posameznik, na katerega lahko vplivamo s pomočjo izobraževanja in ozaveščanja. Odgovornost in zavest o pomenu informacijske varnosti se mora usidrati v miselnost posameznika.

Problem informacijske varnosti počasi pridobiva zanimanje v najvišjih vodstvenih krogih organizacije. To zavedanje je še posebej pomembno, kajti varovanje informacij je vodstvena aktivnost, ki mora poleg finančnih sredstev zagotoviti tudi upravljanje znanja, prave ljudi in primerno politiko upravljanja.

V diplomski nalogi sem izvedel kvalitativno analizo informacijske varnosti podjetja „X“. Prvi del diplomske naloge je teoretičen in zajema pojem varnosti informacij, prav tako so opisane nekatere grožnje, na katere moramo biti pozorni in pa nekatere zaščite zoper grožnjam varnosti informacij. Prvi del naloge tako prispeva k boljšemu razumevanju samega področja informacijske varnosti. Razlaga pa tudi pomen standardov na področju informacijske varnosti.

Drugi, praktični del diplomske naloge pa prikazuje analizo odstopanj od priporočil serije standardov ISO/IEC 27000 v podjetju »X« ter podanimi predlogi za izboljšave.

Rezultat diplomske naloge je tako analiza stanja s področja informacijske varnosti na osnovi serije standardov ISO/IEC 27000 v podjetju. Prikazal sem natančen opis informacijske varnosti podjetja, njegove tehnične karakteristike ter opisal obstoječe stanje s stališča fizične in logične varnosti. Vsakemu tveganju sem predlagal izboljšave informacijske varnosti.

Pri analizi so bile ugotovljene nekatere pomanjkljivosti, ki se jih da dokaj hitro odpraviti in doseči skladnost s standardom. Na nekaterih področjih pa bo potrebnega več truda, da bi dosegli popolno skladnost s standardom. Slednje velja predvsem za evidentiranje in vrednotenje sredstev ter izdelavo in redno preverjanje dokumentov.

Skozi diplomsko delo smo spoznali, da strogi varnostni predpisi niso vedno rešitev, saj se ob ostrejših ukrepih varnost sicer poveča, vendar je lahko ob takšnih zaostritvah utežen normalen delovni proces. Zato je potrebna prava meja med predpisi, zdravim razumom in tehnološkimi rešitvami.

Pri vsem tem se je potrebno zavedati, da popolne varnosti ni in da je potrebno stalno preverjati vpeljevanje in rezultate vpeljanih kontrol in nadzorov.

8. Literatura in viri

[1] Aldin Kočan, *Analiza varnosti informacijskega sistema v podjetju*, diplomsko delo, Ljubljana: FOV, 2009.

[2] Aleš Erjavec, *Varovanje informacij v skladu s serijo standardov ISO/IEC 27000*, specialistična naloga, FVV, 2010.

[3] Karmen Arnuš, *Nekateri ključni pristopi za zagotavljanje informacijske varnosti, diplomsko delo*, FERI, 2010.

[4] Damjan Petrović: Analiza informacijske varnostne politike v agenciji RS, diplomsko delo, EF, 2007.

[5] Ed Skoudis, Counter Hack, *A Step-by-Step Guide to Computer Attack and Effective Defenses*, Upper Saddle River: PH PTR, 2002, pogl. 5, 6, 7, 10.

[6] Jože Florjančič, *Informatika in management, IZBRANA POGLAVJA*, Kranj: Založba Moderna organizacija, 2003, pogl. 1, 21.

[7] Jule Hintzbergen, *Foundations of Information Security, Based on ISO27001 and ISO27002*, Zaltbommel: Van Haren, 2010, pogl. 4, 5, 7, 9, 11.

[8] Mark Egan, *Varovanje informacij*, Ljubljana: Pasadena, 2005, pogl. 1, 2, 4, 6.

[9] Miran Mihelčič, *Organizacija in ravnateljevanje*, Ljubljana: FRI, 2008, pogl. 19.

[10] Tomaž Bratuša, *Hekerski vdori in zaščita,* Ljubljana: Pasadena, 2006, pogl. 1, 4, 12.

[11] Tone Vidmar, *Informacijsko – komunikacijski sistem*, Ljubljana: Pasadena, 2002, pogl. 1, 14.

[12] BSI, BS ISO/IEC 17799:2005, Informacijska tehnologija – Varnostne tehnike – Kodeks za upravljanje varovanja informacij, 2005, pogl. 0, 9, 5.

[13] BSI, BS ISO/IEC 27000:2005, Information technology – Security techniques – Information security management systems – Overview and vocabulary, Switzerland:ISO, 2009, pogl. 4.

[14] BSI, BS ISO/IEC 27001:2005, BS 7799-2:2005, Informacijska tehnologija – Varnostne tehnike – Sistemi za upravljanje varovanja informacij - Zahteve, 2005, pogl. 0, Priloga A.

[15] (2010) COBIT. Dostopno na: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx.

[16] (2010) ISO/IEC 27000. Dostopno na: http://www.27000.org/.

[17] (2010) ITIL. Dostopno na: http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library.

[18] (2010) Socialni inženiring. Dostopno na: http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf.

[19] (2010) Spam. Dostopno na: http://www.sc-nm.com/e-gradivo/OMR/nezaelena_pota__spam.html.

[20] (2010) Struktura ISO27000. Dostopno na: http://www.ascenris.com/template1/images/27K1.png.

[21] (2010) Vohunski programi. Dostopno na: http://www.nasvet.com/vohunski-programi/.

[22] Interna dokumentacija podjetja »X«.

9. Priloge

9.1 Izjava o varovanju informacij

IZJAVA O VAROVANJU INFORMACIJ

Spodaj podpisani ________________________ izjavljam, da sem seznanjen z informacijsko varnostno politiko organizacije, se z njo strinjam in bom njena določila dosledno upošteval.

V primeru kršitve te politike se lahko sprožijo ukrepi, kot jih predvideva veljaven disciplinski postopek. Glede na interese organizacije se lahko uporabijo tudi drugi, nedisciplinski ukrepi.

Ta izjava je napisana v dveh izvodih, od katerih prejme en izvod podpisnik, drugega pa pooblaščenec za informacijsko varnost.

Koper, dne __________ Podpisnik:_______________

9.2 Poročilo o incidentu

POROČILO O INCIDENTU

Oznaka:____

Naslov:____

Datum vnosa:____

Datum incidenta:____

Trajanje izpada:____

Podrobnosti o incidentu:____

Podrobnosti reševanja:____

Podrobnosti o nastali škodi:____

Kraj odkritja:___________________________

Datum in ura odkritja:__________________

Odkril:________________________________

Podrobnosti o storilcu:____

Storilec identificiran:____

Storilec:____

Način identifikacije:____

Podrobnosti o izboljšavi:____

9.3 Izpad posameznega informacijskega sistema

ZADOLŽITVE IN POSTOPKI V PRIMERU IZPADA POSAMEZNEGA IS

INFORMACIJSKI SISTEM

Informacijski sistem/rešitev:____

Lastnik/nosilec področja:____

Kontaktna oseba:____

Ključni dobavitelji:____

ZADOLŽITVE

Odgovoren za izvedbo:____

Izvajalec:____

Zadolžen za obveščanje:____

Obvestiti:____

PREDVIDEN ČAS OBNOVE SISTEMA

Predviden čas celotne obnove sistema:______________________________________

Predviden čas obnove prioritetnih delov sistema:______________________________

REŠEVANJE

Postopek reševanja:____

POMEMBNO

Ne pozabi:____

9.4 Dovoljena programska oprema

NAMEŠČANJE IN UPORABA PROGRAMSKE OPREME

Na računalnike, ki so v lasti organizacije "X", je dovoljeno nameščati in uporabljati zgolj programsko opremo, za katero ima organizacija kupljene licence. V primeru, da uporabnik želi namestiti programsko opremo po izbiri, mora o tem obvestiti odgovorno osebo, ki lahko odobri ali zavrne nameščanje.

SEZNAM DOVOLJENE PROGRAMSKE OPREME

Ime	**Izdajatelj**	**Datum nakupa licence**
Nod32	ESET	1.1.2009
Office 2007	Microsoft	2.4.2009
Windows 7	Microsoft	1.7.2009
Windows XP	Microsoft	12.2.2010
Visual Studio 2007	Microsoft	7.4.2010

9.5 Kontrolna lista preverjanja dokumentacije

KONTROLNA LISTA PREVERJANJA VARNOSTNE DOKUMENTACIJE

	Mesec	**Dokumentacija usklajena DA/NE**	**Kontroliral vodja**	**Podpis**
1	Januar			
2	Februar			
3	Marec			
4	April			
5	Maj			
6	Junij			
7	Julij			
8	Avgust			
9	September			
10	Oktober			
11	November			
12	December			

9.6 Popis sredstev

POPIS SREDSTEV

Področje/Organizacijska enota:____

Odgovornost:____

Datum:____________________

Tip sredstva:____

Številka sredstva	**Naziv sredstva**	**Lastnik**	**Skrbnik**	**Lokacija**	**Vrednost**	**Opombe**

9.7 Prenos programske opreme

PRENOS PROGRAMSKE OPREME S TUJIH STREŽNIKOV

Programska oprema, ki je prenesena s strežnikov, kateri niso v lasti organizacije "X", je potrebno preveriti s protivirusnim programom Nod32, po prenosu je potreben desni klik miške na preneseno datoteko in izbira pregleda s protivirusnim programom.

Pred nameščanjem je potrebno preveriti, ali je programska oprema na seznamu dovoljene in odobrene programske opreme. V primeru, da se tam ne nahaja, je potrebno obvestiti odgovorno osebo, ki lahko odobri ali zavrne nameščanje.

9.8 Dodelitev uporabniških pravic

ZAHTEVEK DODELITVE UPORABNIŠKIH PRAVIC

Številka:________________

Predlagatelj:_______________ Telefon:_________________ Datum:__________

Vzrok (ustrezno obkroži): DODELITEV UKINITEV

Delo v aplikacijah:____

Želeni rok:_______________

Opis dela:____

Priloge:____

Predlagal:__________________ Datum:____________

Odobril:___________________ Datum:____________

Prevzel:___________________ Datum:____________

9.9 Pooblastilo za dostop do računalniškega sistema

ZAHTEVEK ZA PRIDOBITEV POOBLASTILA DOSTOPA DO RAČUNALNIŠKEGA SISTEMA

Služba/Sektor/Oddelek:____

Ime in priimek vlagatelja:____

Potrebujem osebni računalnik: DA NE

Posebne zahteve:____

	Zahtevana programska oprema	**Usposobljenost vlagatelja**
Visual Studio 2007	DA	DA
Internet	DA	DA
Office 2007	DA	DA

Datum:_________________________

Vodja oddelka:___________________ Vodja sektorja:_____________________

9.10 Ravnanje v primeru okužb

RAVNANJE V PRIMERU OKUŽB

V primeru zaznane okužbe s strani protivirusnega programa je potrebno morebitno grožnjo izbrisati z izbiro “Delete”. V primeru nadaljnih težav je potrebno obvestiti odgovorno osebo.

9.11 Nastavljanje programov za preverjanje škodljive kode

NASTAVLJANJE PROTIVIRUSNEGA PROGRAMA

Program za preverjanje škodljive kode je protivirusni program ESET Nod32 Antivirus. Za učinkovito delovanje mora biti ustrezno nastavljen. Omogočen mora biti avtomatski zagon programa po nalaganju operacijskega sistema, omogočene morajo biti vse možnosti preverjanja, ki jih program omogoča. V primeru, da se program ne posodablja pravilno, je potrebno obvestiti odgovorno osebo.

9.12 Politika elektronske pošte

POLITIKA ELEKTRONSKE POŠTE

CILJ

Preprečiti izgubo, spremembo ali zlorabo informacij in nepooblaščen dostop do njih.
Zagotoviti splošno zanesljivost in dostopnost storitve, učinek hitrejšega odpošiljanja. Vse uporabnike seznaniti z njihovimi pravicami in odgovornostmi v povezavi z elektronsko pošto.

SPLOŠNA PRAVILA

Uporaba sistema elektronske pošte
Sistem elektronske pošte se uporablja samo v službene namene. Nedopustna je uporaba, ki je v nasprotju z veljavnimi predpisi.

Pravice nad podatki
Vse pravice nad sistemom elektronske pošte in vsemi sporočili pripadajo organizaciji.

ELEKTRONSKI POŠTNI PREDAL

Odpiranje in zapiranje predala
Organizacija ima enoten elektronski poštni predal. Elektronska sporočila, ki prispejo v ta predal, odpirajo samo pooblaščene osebe.

Uporaba predala
Uporabnik ne sme uporabljati predala, ki je bil dodeljen drugemu uporabniku.

Privzete nastavitve predala

Uporabnik ne sme spreminjati nastavitev svojega predala.

ELEKTRONSKA SPOROČILA

Velikost elektronskih sporočil
Največja velikost pri pošiljanju ali sprejemanju elektronske pošte skupaj s priponko med posameznimi sistemi elektronske pošte je praviloma omejena.

Načelo varnosti in racionalnosti
Pri pošiljanju elektronskih sporočil morajo uporabniki upoštevati načelo racionalnosti in varnosti.

Odpiranje elektronskega sporočila
Če uporabnik po pomoti prejme elektronsko sporočilo, ki ni namenjeno njemu, vsebine tega sporočila ne sme shraniti ali uporabiti v katerikoli namen.

Preusmeritve elektronskih sporočil
Preusmeritve elektronskih sporočil so dovoljene samo znotraj sistema.

Posredovanje in prejemanje elektronskih sporočil
Pri izmenjavi dokumentov oziroma elektronskih datotek veljajo varnostna pravila, ki veljajo za klasično pošto.

Računalniški virusi
Uporabniki elektronske pošte naj sumljiva sporočila zbrišejo, ne smejo zaganjati priponk in dokumentov v elektronski pošti, ne smejo namerno nameščati ali pošiljati računalniških virusov.

UPRAVITELJI

Posebna pooblastila
Za varno in nemoteno delovanje sistema elektronske pošte skrbijo upravitelji elektronskih poštnih strežnikov.

NADZOR

Sledenje
Upravitelji lahko v primeru zlonamernih sporočil vzpostavijo sledenje takim sporočilom.

Zbiranje statističnih podatkov

Upravitelji lahko zbirajo statistične podatke, povezane z uporabo sistema elektronske pošte.