REPUBLIKA E SHQIPËRISË
AUTORITETI I MBIKËQYRJES FINANCIARE
BORDI

UDHËZIM

MBI

PARIMET DHE RREGULLAT E PËRGJITHSHME TË SIGURISË SË INFORMACIONIT

Miratuar me Vendimin e Bordit nr. 20, datë 06.02.2018

1. Të Përgjithshme

1.1. Objekti

Objekt i këtij udhëzimi është përcaktimi i parimeve dhe rregullave të përgjithshme të sigurisë së informacionit në AMF dhe përcaktimi i përgjegjësive për veprimet që lidhen me sigurinë, me qëllim ruajtjen e integritetit, disponueshmërisë dhe konfidencialitetit të aseteve të informacionit të Autoritetit.

1.2. Baza Ligjore

Udhëzimi hartohet në bazë dhe për zbatim të nenit 14 të Ligjit nr. 9572, datë 03.07.2006 "Për Autoritetin e Mbikëqyrjes Finanaciare", i ndryshuar.

1.3. Fusha e Zbatimit

Ky udhëzim zbatohet për çdo pjestar të personelit, i cili akseson informacionin në pronësi ose të administruar nga AMF dhe synon të mbulojë në mënyrë të gjerë dhe të përgjithshme të gjitha burimet dhe sistemet e informacionit në pronësi ose përdorim nga AMF.

1.4. Parimet e Sigurisë

Në përputhje me Politikën e Sigurisë së Informacionit, objektivi kryesor për sigurinë e informacionit është të ruajë integritetin, disponueshmërinë dhe konfidencialitetin e aseteve të informacionit të Autoritetit. Termat e mësipërme përcaktohen si më poshtë:

INTEGRITETI

Gjatë gjithë kohës informacioni duhet të jetë i plotë, i saktë dhe i qëndrueshëm ndaj modifikimeve të paautorizuara ose ndaj dëmtimeve.

DISPONUESHMËRIA

Informacioni bëhet i aksesueshëm sa herë që është e nevojshme. Kjo do të thotë që të gjitha informacionet dhe të gjitha sistemet e informacionit përfshirë pajisjet, rrjetet e komunikimit, programet aplikativë dhe të dhënat që ato mbajnë janë të disponueshme dhe operacionale (të gatshme për punë) sa herë që nevojitet një gjë e tillë dhe të sigurohet afati dhe besueshmëria e aksesit dhe përdorimit të informacionit. Sidoqoftë, plotësimi i parimeve të sigurisë mbi përdorimin e pajisjeve kompjuterike, rrjeteve të komunikimit, programeve aplikativë, dhe aksesit në të dhëna do të kërkojë politika të kontrollit të aksesit. Objektivi i kontrollit të aksesit është se përdoruesit aksesojnë vetëm ato burime dhe shërbime që janë të caktuara për aksesim dhe se përdoruesit e kualifikuar nuk refuzohen të aksesojnë shërbimet që janë ligjërisht të aksesueshme nga ta.

KONFIDENCIALITETI

Informacioni konfidencial përdoret vetëm nga persona të autorizuar. Kjo është veçanërisht e rëndësishme për informacionet me ndjeshmëri të lartë. Aspekte të konfidencialitetit janë shumë të rëndësishme pasi përmbajnë çështje të privatësisë që duhet të parashikohen. Për të mirëmbajtur në mënyrë konstante, duhet të sigurohet se çdo individ ka të drejtën e kontrollit se çfarë informacioni grumbullohet mbi ta, si përdoret, kush e përdor, kush e mirëmban dhe për çfarë qëllimi përdoret.

PËRGJEGJËSIA

Të gjithë personat, qofshin këta nëpunës, kontraktues, konsulentë ose përdorues të jashtëm, mbajnë përgjegjësi për pasojat qe rrjedhin direkt nga veprimet e tyre dhe që kanë të bëjnë me asetet e informacionit të AMF-së. Çdo nëpunësi i bëhen të qarta përgjegjësitë e tij në lidhje me detyrën që kryhen.

1.5. Objektivat e Sigurisë

1. Përcaktimi i politikave organizacionale mbi vazhdimësinë e aktivitetit, të cilat përmbajnë detyrat dhe përgjegjësitë, qëllimin, kriteret e alokimit të burimeve/parimet, kërkesat për trajnim, planet backup, si dhe nivelet e aprovimit.
2. Plani i vazhdimësisë së aktivitetit të përfshijë plane për backup dhe për rimëkëmbje për pajisjet kompjuterike, të dhënat, programet aplikativë dhe për qendrën e të dhënave.
3. Te sigurohet se Autoriteti është i përgatitur për të menaxhuar të gjitha risqet kritike (nëpërmjet politikave të brendshme, procedurave dhe rregullave).
4. Të gjithë risqet domethënëse të identifikohen dhe maten në mënyrën e duhur (nëpërmjet praktikave më të mira të vlerësimit të riskut), gjithashtu të përcaktohen politika të përshtatshme të reduktimit të tyre.

5. Politikat e sigurisë së informacionit të mbulojnë të gjithë risqet operacionalë dhe të mbrojnë në mënyrë të arsyeshme të gjithë asetet e informacioneve kritike kundrejt humbjeve, dëmtimit dhe abuzimit.
6. Politikat e sigurisë së informacionit të jenë të organizuara në mënyrë të tillë që të mbrojnë të gjithë informacionin konfidencial lidhur me palët e brendshme dhe të jashtme.
7. Percaktimi i detyrave dhe përgjegjësive të qarta të TI lidhur me Politikat e Sigurisë së Informacionit për të evituar konfliktet e përgjegjësive ose dis-harmonive në aktivitetet e sigurisë së informacionit.
8. Politikat formale dhe të shkruara për komunikimet dhe operacionet e TI në Autoritet formojnë një mjedis të qëndrueshëm menaxherial për komunikimet e brendshme dhe të jashtme.
9. Garantimi se të gjithë punonjësit (përfshirë të kontraktuarit ose përdoruesit e të dhënave sensitive) janë të kualifikuar për mirëmbajtjen e të dhënave dhe njohin detyrat dhe përgjegjësitë e tyre, dhe se aksesi ndërpritet sapo ndërpritet kontrata e punësimit/kontraktimit.
10. Trajnime për njohuritë e duhura në lidhje me sigurinë e informacionit ndaj punonjësve të Autoritetit.
11. Garantimi i sigurisë fizike dhe ambientale të jetë në përputhje me kërkesat për siguri dhe me klasifikimin e sensitivitetit të aseteve TI.
12. Sigurimi i masave institucionale dhe fizike, të cilat garantojnë parandalimin e aksesit të paautorizuar.
13. Garantimi se ndërhyrjet e paautorizuar zbulohen dhe trajtohen mbeshtetur ne politika të brendshme të sigurisë.
14. Të sigurohet se vetëm përdoruesit e autorizuar kane akses ndaj informacioneve, duke përcaktuar politika aksesi, të cilat japin një bazë për kontrollin e ndërhyrjes ndaj informacioneve.
15. Vlerësimi nëse aplikacionet sigurojnë integritetin, vlefshmërinë dhe besueshmërinë e të dhënave në përputhje me parimet e sigurisë.
16. Outputi i aplikacioneve trajtohet në përputhje me klasifikimin e konfidencialitetit të aplikuar dhe gjithashtu shpërndarja e outputit ose raporteve është e mirë kontrolluar.
17. Aksesimi i të gjitha sistemeve të informacionit të Autoritetit kontrollohet rreptësisht për të garantuar integritetin dhe mbrojtjen e tyre.
18. Të gjitha sistemet (përfshirë këtu mjediset e zhvillimit, të testimit dhe produktet) mbrohen nga kërcënimet dhe nga dëmtimet fizike.
19. Të gjithë individët mbajnë përgjegjësi direkte për veprimet që kryejnë mbi asetet e informacionit të Autoritetit.
20. Për çdo mjedis të teknologjisë së informacionit (këtu përfshihen pajisjet në dhomën e serverave, bazat e të dhënave dhe të gjitha pajisjet e rrjetit të brendshëm të Autoritetit) hartohen masa/procedura sigurie. Ato klasifikohen si KONFIDENCIALE dhe kopja origjinale e tyre do të ruhet në mënyrë të sigurtë nga administratori përgjegjës i sigurisë i teknologjisë së informacionit.
21. Masat e sigurisë zhvillohen në përputhje me funksionimin e sistemeve të Autoritetit, prej një regjimi pune 24 orë në ditë, për 7 ditë në javë.

1.6. Kontrolli i dokumenteve

Administratori për sigurinë e informacionit (Personi i ngarkuar për sigurinë në Drejtorinë e Teknologjisë së Informacionit) është përgjegjes për këtë udhëzim dhe mban përgjegjësi për mbarëvajtjen e tij. Administratori për sigurinë e informacionit kujdeset që:

- I gjithë personeli i Autoritetit të inkurajohet vazhdimisht të bëjë komente dhe sygjerime tek administratori i sigurisë për modifikimin e udhëzimit;
- Administratori për sigurinë e informacionit paraqet një raport periodik me shkrim para Drejtorit të Teknologjisë së Informacionit në çdo periudhë të planifikuar, duke dhënë komentet mbi funksionimin e udhëzimit dhe rekomandimet për çdo modifikim ose shtesë të nevojshme;
- Udhëzimi të jetë objekt i një procedure zyrtare vjetore rishikimi, nën kontrollin e administratorit përgjegjës për sigurinë.

1.7. Politika dhe Procedura në funksion të Sigurisë së Informacionit

Drejtoria e Teknologjisë së Informacionit përgatit politika dhe procedura, në zbatim të këtij udhëzimi, për çështje të cilat janë të rëndësishme për ruajtjen e sigurisë së informacionit.

- Politika e sigurisë së informacionit.
- Politika për përdorimin e emailit dhe internetit.
- Procedurat e Back-up.
- Administrimi i fjalëkalimeve.
- Inventarizimi i aseteve të informacionit.
- Procedura për administrimin e kompjuterave portativë.
- Procedurat e administrimit të ndryshimeve.
- Procedura për administrimin e dokumentacioneve.
- Procedura per administrimin e sistemeve operative Windows 7 dhe 10.
- Procedura per aksesin fizik në dhomën e serverave.

2. SIGURIA E INSTITUCIONIT DHE PËRGJEGJËSITË

2.1. Përgjegjësitë për sigurinë

I gjithë personeli është përgjegjës për respektimin dhe për ruajtjen e nivelit të kërkuar të sigurisë gjatë kryerjes së detyrave. Ai vepron vazhdimisht në përputhje me udhëzimin për parimet dhe rregullat e përgjithshme të sigurisë së informacionit. Në këtë udhëzim, me "personel" kuptojmë të gjithë ata persona të cilëve u lejohet aksesi në asetet e Autoritetit dhe në mënyrë të veçantë asetet e informacionit. Këtu përfshihen:

- Punonjësit e Autoritetit;
- Kontraktorët e Autoritetit;
- Nëpunësit e ofruesve të shërbimeve (service providers) të Autoritetit;

- Konsulentët;
- Palë të tjera me të drejtë aksesi.

ADMINISTRATORI PËRGJEGJËS PËR SIGURINË

Administratori përgjegjës për sigurinë mban të gjitha përgjegjësitë për sigurinë e informacionit të AMF-së. Në veçanti ai:

- Shqyrton këtë rregullore dhe përcakton të gjitha përgjegjësitë;
- Monitoron ndryshimet e rëndësishme që ekspozojnë asetet ndaj kërcënimeve të mëdha;
- Shqyrton, monitoron, parandalon dhe kundërvepron ndaj thyerjeve të rënda të sigurisë;
- Miraton projekte të rëndësishme për përmirësimin e mëtejshëm të sigurisë. Administratori për sigurinë raporton rregullisht (jo më pak se një herë në tre muaj) tek Eprori direkt.

DREJTORËT E DREJTORIVE

Siguria e informacionit është përgjegjësi e çdo drejtuesi strukture. Në përputhje me këtë, të gjithë drejtuesit janë përgjegjës:

- Të sigurojnë njohjen e personelit me politikën e sigurisë së informacionit, me këtë udhëzim, procedurat dhe standardet e publikuara për sigurinë e informacionit në AMF;
- Për vlerësimin e vazhdueshëm të riskut të sigurisë në fushën ku ata drejtojnë;
- Të sigurohen që të gjitha të drejtat për aksesimin e aseteve të Autoritetit (përfshi këtu kompjuterat, llogaritë e përdoruesve, çelsat dhe çdo gjë tjetër) të hiqen menjëherë, për çdo pjesëtar të personelit (i përhershëm ose me kontratë) që largohet nga AMF ose që kalon në një departament apo në një detyrë tjetër;
- Për aplikimin e llogarive të reja për përdoruesit apo modifikimin e llogarive aktuale, për nivele të duhura sigurie dhe për të drejta aksesimi (përfshi aksesin fizik), për pjesëtarët e rinj të personelit;
- Për dhënien e së drejtës për aksesimin personelit jashtë departamentit të tyre, në lidhje me asetet e informacionit dhe sistemeve kompjuterike për të cilat ata janë përgjegjës;
- Për dhënien e së drejtës për ndryshimin (korrigjimin) e çdo hedhjeje gabim të të dhënave në sistemet specifike të teknologjisë së informacionit për të cilin ata janë përgjegjës.

ADMINISTRATORI I SIGURISË

Detyrë e Administratorit të Sigurisë është të krijojë, të zbatojë dhe të mirëmbajë një program sigurie që të ndihmojë Autoritetin në mbrojtjen e aseteve të informacionit. Administratori i Sigurisë është përgjegjës për:

- Krijimin, për të gjithë Autoritetin, të standardeve dhe të udhëzuesve për sigurinë e informacionit dhe sigurinë fizike;

- Përmirësimin e vazhdueshëm të këtij udhëzimi;
- Imponimin e zbatimit të rregulloreve dhe për ruajtjen e standardeve të sigurisë;
- Zhvillimin dhe kryerjen e një fushate të vazhdueshme për sigurinë për ndërgjegjësim e punonjësve të AMF-së;
- Trajnimin e personelit në lidhje politikat dhe me procedurat e sigurisë;
- Kryerjen dhe përmirësimin e vazhdueshëm (të paktën një herë në vit) të analizës së riskut;
- Rishikimin e vazhdueshëm (një herë në tre muaj) të të drejtave të aksesimit të informacioneve;
- Rishikimin e vazhdueshëm (një herë në gjashtë muaj) të masave të sigurisë ndaj ofruesve të shërbimeve të jashtme, veçanërisht personelit që punon me kontratë në ambientet e Autoritetit;
- Rishikimin e rregullt (një herë në tre muaj) të privilegjeve për aksesimin e sistemeve të kompjuterave;
- Kontrollin për heqjen e menjëhershme të llogarive të përdoruesve që japin dorëheqjen ose largohen nga puna për arsye të tjera;
- Drejtimin e kontrolleve të sigurisë, përfshi këtu organizimin e rregullt të kontrolleve të jashtme;
- Shqyrtimin e thyerjeve të sigurisë që raportohen;
- Raportimin rregullisht (të paktën një herë në tre muaj) tek Drejtori i Drejtorisë së Teknologjisë dhe Informacionit mbi gjendjen e sigurisë.

2.2. Aksesimi i të tretëve

Personat, të cilët nuk janë punonjës të AMF-së dhe institucionet (organizatat) e tjera, lejohen të aksesojnë asetet e informacionit të Autoritetit vetëm në bazë të kushteve të përcaktuara në një marrëveshje zyrtare duke nënshkruar një deklaratë, ku pranojnë se do të respektojnë të gjitha rregullat/procedurat e këtij udhëzimi. Këto kushte duhet të mbulojnë të drejtat dhe detyrimet e të gjithë personave dhe organizatave që janë të interesuara të aksesojnë asetet e informacionit të AMF-së, përfshirë këtu sipas mundësisë:

- Politikën e përgjithshme për sigurinë e informacionit të Autoritetit;
- Kufizimet në kopjimin dhe në shpërndarjen e informacionit;
- Një përshkrim për secilin prej shërbimeve që do të ofrohet nga Autoriteti;
- Nivelin e synuar dhe atë të papranueshëm të shërbimeve;
- Klauzolat për ndryshimin e personelit, nëse është e nevojshme;
- Detyrimet respektive të palëve që bëjnë marrëveshjen;
- Përgjegjësitë për të respektuar përputhjen me ligjin dhe me rregulloret;
- Mbrojtjen e të drejtës së autorit të Autoritetit, si dhe të palëve të treta;
- Metodat e lejuara të aksesimit dhe kontrolli i përdorimit të fjalëkalimit të përdoruesit;
- Procesin e dhënies të së drejtës për aksesim;
- Një kërkesë për të mbajtur një listë të personave të autorizuar për të përdorur shërbimet e kërkuara dhe të të drejtave të tyre përkatëse;

- Përcaktimin e kritereve të verifikueshme të performancës, monitorimin e tyre dhe raportimin;
- Të drejtën për të monitoruar dhe për të ndërprerë aktivitetin e përdoruesit;
- Të drejtën për të kontrolluar/verifikuar zbatimin e përgjegjësive kontraktore;
- Përgjegjësitë që kanë të bëjnë me instalimin dhe me mirëmbajtjen e pajisjeve dhe të programeve;
- Një strukturë të qartë raportimi dhe miratim të formateve të raportimit;
- Kërkesën për të zbatuar procedurat e Autoritetit për administrimin e ndryshimeve mbi sistemet e informacionit;
- mbrojtjen nga programet keqdashëse;
- Procedurat për raportimin, njoftimin dhe për shqyrtimin e thyerjeve të sigurisë;
- Detyrimin e palëve të treta për të kërkuar zbatimin e këtyre kushteve edhe nga nënkontratorët e tyre.

3. KLASIFIKIMI DHE KONTROLLI I ASETEVE

3.1. Përgjegjësia për asetet

Për Teknologjinë e Informacionit, menaxhimi i aseteve përfshin mirëmbajtjen e një inventari të saktë të pajisjeve TI, duke ditur se licencat janë për pajisjet përkatëse, mirëmbajtjen dhe mbrojtjen (kyçjen, dhomat e kontrolluara, etj.) të pajisjeve. Menaxhimi i aseteve TI përfshin gjithashtu menaxhimin e programeve dhe dokumentacionin e proceseve që janë të vlefshme për subjektin.

Për AMF-në menaxhimi i aseteve të TI është shumë i rëndësishëm, pasi kufizimet financiare mund të mos lejojnë zëvendësimin e aseteve të vjedhura ose të humbura në mënyrën më të arsyeshme. Për më tepër, autoriteti mund të jetë në risk nëse nuk ka një inventar të plotë të të gjitha aseteve në momentin e zhvillimit të programeve që nevojiten për kërkesat e së ardhmes.

Të gjitha asetet kryesore për aktivitetin normal të Autoritetit vlerësohen dhe për këtë ngarkohet një person përgjegjes i caktuar (pronar). Përgjegjësia për asetet garanton mbajtjen në mënyrë të vazhdueshme të një niveli të mjaftueshëm sigurie. Për të gjitha asetet e rëndësishme të informacionit do të përcaktohen "pergjegjesit" së bashku me përgjegjësitë përkatëse për ruajtjen e masave të duhura të sigurisë, të cilat duhet të specifikohen qartë. Zbatimi i masave të sigurisë mund të delegohet, por në çdo rast përgjegjësia duhet t'i mbetet pergjegjesit të asetit.

3.2. Regjistri i aseteve të informacionit

Për sistemet e informacionit, hartohet dhe mbahet në mënyrë të vazhdueshme një regjister (inventar) që mbulon të gjitha asetet kryesore për çdo sistem duke përfshirë:

- Asetet e informacionit: bazat e të dhënave dhe skedarët e të dhënave, kontratat dhe marreveshjet, dokumentacionin e sistemeve, informacionet kerkimore, manualet e përdoruesit, materialet e trainimit, procedurat operacionale apo mbeshtetese, planet e vazhdueshmërisë së punës, rregullat dhe procedurat e rekuperimit të të dhënave të humbura, informacionin e arkivuar dhe gjurmet e auditimit;
- Programet (asetet software): programet aplikative, programet e sistemit, mjetet për zhvillimin e mëtejshëm të tyre dhe mjetet ndihmse;
- Asetet fizike: pajisjet kompjuterike, pajisjet e komunikimit, pajisje të tjera teknike (për shembull. kabllot e energjisë elektrike, pajisjet e ajrit të kondicionuar, gjeneratore të energjisë), mobiljet;
- Shërbimet: shërbimet kompjuterike, shërbimet e komunikimit dhe utilitetet e përgjithshme;
- Njerezit dhe kualifikimet e tyre, aftesite dhe pervoja;
- Aktive jo materiale: të gjitha asetet, qellimi/funksioni i aktivit dhe proceset mbeshtetese.

Për çdo aset në regjistër mbahet:

- Përshkrimi i tij;
- Përgjegjësi i tij: Ky është administratori i njësisë (departamentit, drejtorisë ose sektorit) së AMF-së. Përgjegjësi është përgjegjës për pranimin e dizenjimit të sistemit dhe të funksionalitetit të tij dhe vendos rregullat për trajtimin, për administrimin dhe për aksesimin e aseteve të informacionit, në përputhje me rregullat e AMF-së;
- Kujdestari: Është njësia e Autoritetit e cila "kujdeset" për asetin e informacionit, domethënë zbaton dhe mbron rregullat e përcaktuara nga përgjegjësi. Derisa të mos jetë kryer ndonjë përcaktim për sistemet specifike, kujdestari për të gjitha sistemet e Autoritetit është Drejtoria e Teknologjisë së Informacionit;
- Klasifikimi: Nënkupton një tregues të ndjeshmërisë së informacionit siç përshkruhet në 3.3;
- Niveli i rëndësisë: përcakton rëndësinë e aseteve të informacionit për Autoritetin, në bazë të periudhës kohore maksimale gjatë të cilës Autoriteti mund të vazhdojë të punojë, pa i patur ato në dispozicion;
- Përdoruesit e autorizuar dhe tipet e lejuara të aksesimit (lexim, shkrim, kopjim, ndryshim, fshirje);
- Krijimi, mirëmbajtja dhe mbrojtja e regjistrit të aseteve të informacionit është përgjegjësi i Drejtorise së TI, e cila konsultohet me përgjegjesit. Regjistri duhet të rishikohet të paktën një herë në gjashtë muaj.

3.3. Klasifikimi i Informacionit

Disa nga informacionet të cilat trajton Autoriteti, i nënshtrohen klasifikimeve zyrtare të sigurisë së informacionit, siç përcaktohet në aktet e tjera rregullatore të Autoritetit në lidhje me transparencën dhe konfidencialitetin. Nivelet e klasifikimit të informacioneve jopublike janë "Informacion sekret" dhe "Informacion konfidencial". Si rregull, dokumentat që

përmbajnë informacione të klasifikuar në një vend tepër të dukshëm duhet të shënojnë dhe llojin e klasifikimt. Është e rëndësishme që Autoritetit të identifikojë:

- Informacionin, që do të klasifikohet "konfidencial" ose "sekret";
- Çdo informacion tjetër të Autoritetit, i cili mund të ketë nevojë për klasifikim të mëtejshëm më specifik.
  Pronari i çdo aseti informacioni është përgjegjës për klasifikimin e tij në përputhje me udhëzimet e Autoritetit.

3.4. Analiza e riskut

Administratori i sigurisë kryen një analizë vjetore zyrtare të riskut për asetet e informacionit të AMF-së sipas procedurave që rekomandohen në standardet ndërkombëtare të ndjekura nga institucionet e tjera homologe. Rezultatet e analizës së riskut do të përdoren për të përcaktuar strategjitë për zbutjen e çdo risku që identifikohet dhe do të rishikohen nga Drejtoria e TI, të paktën çdo vit. Analiza e riskut mbeshtetet ne nje proces te pershtatshem te identifikimit, vleresimit dhe percaktimit te perparesive ne lidhje me rreziqet.

3.5. Administrimi i ndryshimit të dokumenteve

Për të gjitha dokumentet e rëndësishme ndiqet Procedura e Administrimit të Dokumenteve. Çdo dokument duhet të përmbajë një seksion identifikues të personave të parashikuar për ta marrë ose për ta lexuar atë. Kur është e mundur, dokumenti duhet të identifikojë gjithashtu versionin, datën dhe natyrën e çdo ndryshimi në të.

4. SIGURIA E PERSONELIT

Duhet të përcaktohet qartë roli dhe përgjegjësia brenda Autoritetit. Për të gjithë të punësuarit duhet të sigurohet një nivel i përshtatshëm i ndërgjegjësimit, edukimit dhe trajnimit në sigurinë e informacionit dhe përdorimin e duhur të objekteve të përpunimit të informacionit duke garantuar se të gjithë punonjësit (përfshirë të kontraktuarit ose përdoruesit e të dhënave sensitive) janë të kualifikuar për mirëmbajtjen e të dhënave dhe njohin detyrat dhe përgjegjësitë e tyre, dhe se aksesi ndërpritet sapo ndërpritet kontrata e punësimit/kontraktimit te tyre.

4.1. Manualet e vendeve të punës dhe punësimi

Çdo punonjës ka përgjegjësitë e tij në lidhje me sigurinë. Përgjegjësia për sigurinë përcaktohet që në fazën e marrjes në punë dhe përfshihet në manualet e vendeve të punës dhe në kontratat e punësimit.

DREJTUESIT E DREJTORISË DUHET TË SIGUROJNË QË NË PËRSHKRIMIN E DETYRËS (MANUALET E VENDEVE TË PUNËS) TË ADRESOHEN ÇËSHTJET E SIGURISË QË LIDHEN ME TË.

Rolet dhe përgjegjësitë që lidhen me sigurinë, duhet të përfshihen në manualet e vendeve të punës, në mënyrë të veçantë për pozicionet drejtuese, kjo siguron përgjegjësinë e të gjithë

punonjësve. Manualet e vendeve të punës duhet të përfshijnë si përgjegjësitë që kanë të bëjnë me zbatimin ose me mirëmbajtjen e rregullave të përgjithshme të sigurisë, ashtu dhe ato specifike për mbrojtjen e aseteve të veçanta ose për ekzekutimin e proceseve të veçanta.

TË GJITHA APLIKIMET PËR PUNËSIM SHQYRTOHEN ME KUJDES NGA PIKËPAMJA E SIGURISË

Të gjitha pranimet duhet të bëhen në përputhje me rregullat e dokumentuara. Aplikimet për punësim duhet të kontrollohen me kujdes nga pikëpamja e sigurisë. Në të gjitha kontratat e pranimit në punë përfshihet një deklaratë ku punonjësit e rinj duhet të pranojnë me shkrim, se bihen plotësisht dakort me kërkesat e Autoritetit mbi konfidencialitetin.

4.2. Procedurat e fillimit dhe të largimit nga puna

PËRGJEGJËSIA E DREJTORËVE TE DREJTORIVE/SEKTORËVE PËR TË GARANTUAR ZBATIMIN E PROCEDURAVE TË SIGURISË NË PUNËSIM.

Drejtorët e drejtorive janë përgjegjës për të garantuar që punonjësve të rinj të strukturave përkatese u është dhënë niveli i duhur i aksesimit në pajisjet dhe në sistemet e Autoritetit, përfshi këtu llogaritë e përdoruesve për kompjuterat, miratimin e lejes së aksesimit të sistemeve, të dhomave të serverave, të nyjeve të rrjetit, kartat magnetike apo me chip për aksesimin e mjediseve, etj.

Të gjitha aplikimet që bëhen për dhënien e të drejtes së aksesimit në sistemet kompjuterike të Autoritetit (përfshi këtu llogarinë personale fillestare për pjesëtarët e rinj të personelit dhe çdo ndryshim në vazhdim në të drejtat për aksesimin e sistemeve) bëhen me shkrim, duke përdorur një formular standard, i cili firmoset nga drejtori i drejtorisë ku bën pjesë punonjësi. Ato miratohen nga Drejtori i Drejtorisë së Teknologjisë dhe Informacionit para se të kryhen veprimet nga njësia helpdesk.

Çdo pjesëtari të ri, i cili i bashkohet personelit të Autoritetit, duhet t'i kërkohet aty ku është e nevojshme, të firmosë për të gjitha pajisjet e aksesimit, duke pranuar njëkohësisht kushtet e përdorimit të tyre. Të gjithë pjesëtarëve të rinj u jepen instruksione të plota për procedurat e teknologjisë së informacionit dhe në veçanti për kërkesat në lidhje me çështjet e sigurisë. Këto instruksione duhet të përfshijnë të paktën:

- Përdorimin e përgjithshëm të mjeteve të teknologjisë së informacionit;
- Ndihmën e kualifikuar nga Drejtoria e Teknologjise së Informacionit (TI helpdesk);
- Familiarizimin me Politikën e Sigurisë së Autoritetit dhe rregullat e sigurisë;
- Trajtimin e informacioneve konfidenciale;
- Politikën e përdorimit të internetit, të emailit, etj.;
- Rregulloret për fjalëkalimet. Kjo bëhet para se atyre t'u hapet ndonjë llogari përdoruesi ose t'u jepen privilegje për të aksesuar sistemet e Autoritetit.

Drejtorët e drejtorive janë përgjegjës për të garantuar zbatimin e procedurave të sigurisë në rastet kur pjesëtarë të personelit të tyre largohen nga puna. Është përgjegjësi e çdo drejtori departamenti/drejtorie/sektori të sigurojë, që kur një pjesëtar i personelit largohet nga puna, t'i hiqen të gjitha të drejtat e aksesimit dhe t'i kërkohet të dorëzojë të gjitha kartat e aksesimit,

çelsat, shënimet, kompjuterat, etj të cilat i ka patur në përdorim. Procedurat e teknologjisë së informacionit për mbylljen e llogarisë së përdoruesit dhe për heqjen e të drejtave të aksesimit të sistemeve të Autoritetit, duhet të bëhen para se pjesëtari i stafit të largohet fizikisht nga ambienti i punës. Personi përgjegjës i caktuar nga Drejtoria e Teknologjisë së Informacionit (helpdesk-u) informohet, sa më shpejt që të jetë e mundur, kur ndonjë pjesëtar i personelit e lë punën ose afati i tij i punësimit mbaron për çdo lloj arsyeje. Është përgjegjësi e drejtorit të drejtorisë përkatëse, të sigurojë që kjo gjë të kryhet sa më parë. Punonjësit të cilëve u nderpriten marrëdhëniet e punës, u kërkohet të largohen nga Autoritetit menjëherë. Ndërsa punonjësit, të cilët kanë kërkuar vullnetarisht largimin e tyre për arsye të ndryshme mund të vazhdojnë punën normalisht edhe për një periudhë mbasi ata të kenë kërkuar largimin. Njoftimi tek helpdesk-u, për largimin nga puna të një personi të caktuar, duhet të përmbajë udhëzimet për korrektimin e të drejtave të përdoruesit të personit qe do të largohet. Zgjedhjet për korektimin e të drejtave do të përfshijnë:

- Fshirjen e menjëhershme të llogarise së përdoruesit;
- Heqjen e disa privilegjeve të aksesimit;
- Mbajtja e nivelit aktual të privilegjeve të aksesimit që ka përdoruesi, por duke rritur nivelin e auditimit për këtë përdorues. Është përgjegjësi e drejtorit të departamentit përkatës të kërkojë nivelin e duhur të korrektimit.

4.3. Planet e vazhdueshmërisë dhe të zëvendësimit

Planet për vazhdueshmërinë dhe për zëvendësimin e të gjitha pozicioneve të rëndësishme (kyçe) të punës rishikohen periodikisht. Këto plane hartohen për rastet e emergjencës, përfshi këtu pamjaftueshmërinë, largimin dhe lëvizjet e planifikuara të personelit.

Këtu përfshihen jo vetëm pozicionet e administratorëve dhe mbikqyrësve, por gjithashtu, edhe ato që kanë lidhje me sigurinë e teknologjisë së informacionit.

4.4. Trajnimi

Personat që kanë akses në asetet e informacionit të Autoritetit janë të detyruar të jenë të vetëdijshëm për rregullat dhe standardet e sigurisë në Autoritetit. I gjithë personeli duhet të marrë trajnimin e nevojshëm për rregullat dhe për procedurat organizative dhe të sigurisë. Ky trajnim kryhet sa më shpejtë që të jetë e mundur pas fillimit të punës së punonjësve të rinj (shih 4.2). Objektivat e edukimit në lidhje me sigurinë duhet të jenë:

- Krijimi i kulturës së sigurisë në të gjithë Autoritetin;
- Edukimi i personelit mbi pasojat e veprimeve të tyre mbi sigurinë e informacionit;
- Udhëzimi i personelit për rregullat dhe procedurat e sigurisë sipas pozicioneve përkatëse;
- Përcaktimi i përgjegjësive që mban çdo person mbi sigurinë dhe detyra e secilit për të raportuar çdo shkelje të rregullave të sigurisë.

Gjithashtu, i gjithë personeli duhet të trajnohet për përdorimin korrekt të sistemeve kompjuterike dhe të aseteve të informacionit. Kjo bëhet para se t'u jepet e drejta të aksesojnë sistemet. Drejtoria e TI përgjegjet për zhvillimin dhe për shpërndarjen e materialeve të trajnimit.

Stafi duhet të jetë i trajnuar dhe i ndërgjegjshëm për përgjegjësitë e tyre referuar parandalimit, zvogëlimit, dhe reagimit ndaj situatave emergjente. Për shembull stafi mbështetës i sigurisë së informacionit duhet të kryejë trajnime periodike në procedurat e emergjencës nga zjarri, uji, dhe incidenteve alarmuese, si dhe mbi përgjegjësitë e tyre në fillimin dhe ekzekutimin e një vendndodhje tjetër përpunimi të dhënash. Gjithashtu, nëse përdoruesit e jashtëm janë kritikë për operacionet e Autoritetit, ata duhet të informohen mbi hapat që mund të ndërmarrin në një situata emergjence.

PERSONELI I DREJTORISË SË TEKNOLOGJISË SË INFORMACIONIT

Të gjithë specialistët e teknologjisë së informacionit duhet të marrin rregullisht trajnime përmirësuese në fushat e tyre të specializimit. Kjo duhet të përfshijë veçanërisht personelin e sigurisë, administratorët e bazave të të dhënave, administratorët e sistemeve operative dhe sistemeve të sigurisë (p.sh. Firewall, IDS, IPS, Network Management, Content Filtering, Application Security, etj.) I gjithë personeli i teknologjisë së informacionit duhet të ndjekë seminare periodike në fushat e interesit të përgjithshëm, veçanërisht në ato që lidhen me sigurinë.

4.5. Përgjigja ndaj incidenteve

Menaxhimi i incidenteve të sigurisë së TI përfshin monitorimin dhe zbulimin e ngjarjeve të sigurisë në një kompjuter ose rrjet kompjuterash, si dhe ekzekutimin e reagimit të përshtatshëm ndaj këtyre ndodhive.

Një incident sigurie është çdo ngjarje e cila mund të ndikojë në integritetin, disponueshmërinë dhe në konfidencialitetin e informacionit. Dëmtimet si pasojë e incidenteve të sigurisë dhe të keqfunksionimeve minimizohen dhe, sa herë që është e mundur të parandalohen. Incidentet që ndikojnë mbi sigurinë duhet të vlerësohen me seriozitet dhe të raportohen menjëherë.

RAPORTIMI I INCIDENTEVE OSE DOBËSIVE TE SIGURISË

Për të gjitha rastet e ngjarjeve që lidhen me sigurinë ndiqet një procedurë formale për raportimin e incidenteve. Të gjithë nënpunësit, kontraktorët dhe personeli i ofruesve të jashtëm të shërbimeve duhet të jenë të vetëdijshëm (ta njohin e ta zbatojnë) për këtë procedurë. Përveç kësaj, i gjithë personeli inkurajohet për të raportuar çdo dobësi të sigurisë ose çdo kërcënim të vënë re në procedura, në sisteme dhe në shërbime.

RAPORTIMI I KEQFUNKSIONIMIT TË PROGRAMIT TEK DREJTORIA TI

Për të minimizuar çdo ndërprerje të shërbimeve apo çdo dëmtim të të dhënave, është shumë e nevojshme që keqfunksionimi i programeve të korrektohet sa më shpejt që të jetë e mundur. Keqfunksionimet e dukshme të programeve i raportohen Drejtorise se TI, e cila përgjigjet menjëherë dhe udhëzon në lidhje me mënyrën e veprimit në raste të tilla.

4.6. Shkelja (thyerja) e rregullave dhe procedurave të sigurisë

Kur administratori (drejtor drejtorie/sektori) gjykon se veprimtaria e një punonjësi nuk është në përputhje me rregullat dhe procedurat e sigurisë, për çfarëdolloj arsyeje, ai është i detyruar të organizojë një takim me punonjësin për të diskutuar çështjen dhe për të planifikuar veprimet korrigjuese.

NË ÇDO RAST DYSHIMI PËR SHKELJE TË RREGULLAVE DHE PROCEDURËS SË SIGURISË, NDIQET NJË PROCES ZYRTAR DISIPLINOR.

Drejtori i drejtorisë nën përgjegjësinë e të cilit është personi i dyshuar për shkelje njofton sa më shpejt të jetë e mundur dhe siguron dokumentacion të plotë për Drejtorinë e TI. Në rastet kur shkelja vërtetohet dhe është mjaft serioze, rishikohet vazhdimi i punës për individin në fjalë. Në rrethana të veçanta tepër serioze, shkelja mund të raportohet në organet përkatese sipas ligjit.

4.7. Ndarja e përgjegjësive

Për të minimizuar mundësinë e mashtrimit ose të keqperdorimit të të dhënave, asnjë individ nuk merr i vetëm përgjegjësi të plotë për një proces të tërë. Proceset e hedhjes dhe daljes së të dhënave duhet të realizohen nga individë të ndryshëm. Në mënyrë të ngjashme, të gjitha njohuritë në lidhje me një sistem, një proces ose për një pjesë të tyre, nuk duhet të mbahen asnjëherë nga një person i vetëm. Njohuritë dokumentohen në mënyrë të qartë dhe të njihen të paktën edhe nga një person tjetër.

5. SIGURIA FIZIKE DHE E MJEDISEVE

5.1. Siguria e ambienteve (ndërtesave)

Aksesimi i të gjitha ambienteve të sistemeve të informacionit në Autoritet do të kontrollohet rreptësisht dhe në çdo kohë, në mënyrë që të parandalohen humbjet ose kompromentimet e aseteve të informacionit dhe të aseteve të tjera.

KARTAT E AKSESIMIT

Të gjitha ambientet kritike sigurohen me sisteme aksesimi dhe karta elektronike, ku çdo punonjës i Autorizuar për një ambient specifik pajiset me një kartë individuale aksesi. Administratori i ndërtesave është personi përgjegjes për mbajtjen e të dhënave në lidhje me të gjitha aksesimet e autorizuara, ku përfshihen detaje si: emri i punonjësit, drejtoria, data kur është lëshuar karta, ora dhe dita deri kur i lejohet aksesimi. Është e detyrueshme mbajtja e logeve për të gjitha aktivitetet e aksesimit, kur sistemet e aksesimit të ambienteve e lejojnë një gjë të tillë.

VIZITORËT

Vizitorëve të Autoritetit nuk duhet t'u lejohet lëvizja e lirë, e pakontrolluar në ambientet kritike. Identiteti i vizitorëve verifikohet nga rojet, të cilët janë përgjegjës për njoftimin e personave që do të shoqërojnë vizitorët. Çdo vizitor duhet të pajiset me një shenjë identifikimi të përkohshme para se të lejohet të hyjë. Vizitorët, punonjësit e mirëmbajtjes dhe persona të tjerë të huaj, duhet të shoqërohen gjatë gjithë kohës nga punonjës të autorizuar të Autoritetit. Në veçanti, vizitorëve nuk duhet t'u lejohet të aksesojnë ambientet me akses të

kufizuar, sidomos në vendndodhjet e serverave, të pashoqëruar nga një person i autorizuar nga Drejtori i Drejtorisë së Teknologjisë dhe Informacionit. I gjithë personeli duhet të inkurajohet të nxjerrë jashtë çdo person të panjohur, të cilin mund ta gjejë në hapësirat me akses të kufizuar. Përgjegjësia për të siguruar largimin e vizitorit nga godina pasi puna e tij ka përfunduar, dhe rikthimi i çdo karte që i është dhënë, mbetet mbi personin e fundit i cili ka qenë në kontakt me vizitorin.

5.2. Siguria e pajisjeve

Të gjitha pajisjet e Drejtorisë së Teknologjisë së Informacionit dhe të gjitha pajisjet e tjera kritike duhet të mbrohen fizikisht nga kërcënimet e sigurisë dhe nga rreziqet e mjedisit.

DHOMAT E SERVERAVE

Të gjithë serverat dhe pajisjet e komunikimit (domethënë routerat, switch-et, firewall-et, PBX etj.) duhet të vendosen në dhoma apo në ambiente të mbyllura e të sigurta. Aksesi në këto dhoma duhet të lejohet vetëm për personelin e autorizuar nga Drejtori i Drejtorisë së Teknologjisë dhe Informacionit.

Të gjitha aksesimet në dhomat ekompjuterave dhe në nyjet e rrjetit duhet të jenë të kontrolluara dhe të mbahen log-e ku të shënohet emri i personit ose i personave, arsyet e hyrjes, data/ora dhe veprimet e kryera. Dhomat e kompjuterave duhet të pajisen me karta sigurie, ajër të kondicionuar, me kamera, me UPS, detektorë dhe me fikësa zjarri. Të gjitha pajisjet në dhomat e serverave duhet të sigurohen kundër dëmtimeve apo tërmeteve.

KOMPJUTERAT PERSONALË

Kompjuterat personalë (PC) duhet të vendosen në përputhje me standardet e Autoritetit për instalimin dhe përdorimin e PC. Në veçanti, ata nuk duhet të vendosen në vende ku personat e paautorizuar kanë mundësi të shohin informacionet sensitive që ndodhen në to. Ato duhet të instalohen ose të transferohen (lëvizen) vetëm nga një personel i trainuar dhe i autorizuar nga Drejtori i Drejtorisë së Teknologjisë dhe Informacionit.

NXJERRJA JASHTË GODINAVE

Ky seksion zbatohet për kompjuterat personal apo çdo formë tjetër mjetesh që mbajnë ose që përpunojnë informacione. Të gjitha pajisjet e Autoritetit, të cilat duhet të nxirren jashtë ndërtesave duhet të jenë po aq të sigurta sa edhe pajisjet që ndodhen brenda tyre, duke marrë parasysh riskun e të punuarit jashtë godinave të Autoritetit. Të dhënat në hard-disk për kompjuterat portabël (laptop), do të enkriptohen duke përdorur programe të miratuara enkriptimi. Gjithashtu skedarët apo dokumentat në këto laptopë duhet të sigurohen dhe t'i jepen privilegje eskluzive aksesimi vetëm ndaj llogarive të përdoruesve që kanë të drejta t'i aksesojnë ato. Pajisjet dhe mediat (përfshi këtu dokumentet sensibël në letër) që nxirren jashtë godinave të Autoritetit, nuk duhet të lihen në vende publike (përfshi këtu makinat) të pambrojtur. Është e detyrueshme që ato të shkatërrohen në mënyrë të parekuperueshme kur nxirren përfundimisht jashtë pune.

5.3. Siguria e aseteve

I gjithë personeli është përgjegjës për të garantuar sigurinë e aseteve që janë nën kontrollin e tyre.

SENDET ME VLERA TË VEÇANTA

Pajisjet dhe media magnetike të ruajtjes të të dhënave (dispozitivët me shirit magnetik) do të nxirren jashtë vendndodhjes së tyre vetëm në përputhje me procedurën e dokumentuar për lëvizjet dhe me miratimin më parë te drejtorit të drejtorisë përkatëse.

INFORMACIONI SENSITIV

Informacioni i klasifikuar Konfidencial ose Sekret, në letër ose në trajtë elektronike, duhet të nxirret jashtë vetëm në përputhje me procedurat e lëvizjes dhe duke patur më parë miratimin e drejtorit të drejtorisë përkatëse.

LARGIMI I MEDIAVE MAGNETIKE

Asetet e informacionit mund të kompromentohen nga pakujdesia në largimin e pajisjeve. Përpara se të nxirren jashtë përdorimit ose të eliminohen, të gjitha pajisjet kompjuterike duhet të kontrollohen për t'u siguruar që të dhënat dhe programet e licencuara janë hequr në përputhje me procedurat e paracaktuara nga Autoriteti. Këtu përfshihen edhe pajisjet që nxirren jashtë Autoritetit për t'u riparuar. Tape-t magnetikë të nxjerrë përfundimisht jashtë Autoritetit duhet të shkatërrohen mundësisht të digjen.

5.4. Siguria e komunikimit

Të gjitha format e komunikimit duhet të jenë të mbrojtura kundër humbjeve, ndërhyrjeve dhe korruptimit.

TELEFONAT

Pajisjet telefonike sigurohet të jenë të mbrojtura nga aksesimi dhe përdorimi i paautorizuar. Masat që duhet të merren përfshijnë:

- Kontrolle fizike për aksesimin e pajisjeve të centralit telefonik;
- Kontrolle për ndalimin e përdorimit të modemeve (ose të pajisjeve të tjera) për aksesimin e rrjeteve te jashtëm duke përfshirë dhe internetin;
- Ruajtjen e të dhënave (logeve) për çdo thirrje telefonike dhe ekzaminimin e tyre për të parë nëse ka thirrje të pazakonta ose të paautorizuara.

6. ADMINISTRIMI I SISTEMEVE TE INFORMACIONIT

6.1. Procedurat e operimit

APLIKIMET

Përgjegjësitë dhe procedurat e administrimit dhe të aktivitetit, mbi të gjitha aplikimet kompjuterike, do të jenë të dokumentuara si pjesë përbërëse e procesit të zhvillimit të tyre. Procedurat e aktivitetit testohen nga Drejtoria e TI.

OPERACIONET E TEKNOLOGJISË SË INFORMACIONIT

Të gjitha procedurat që lidhen me teknologjinë e informacionit dokumentohen. Kjo gjë përfshin një grup të procedurave dhe proceseve institucionale që sigurojnë përpunim korrekt të të dhënave në Autoritet. Gjithashtu përfshin procedurat e dokumentimit mbi të dhënat, kanalet e komunikimit, procedurat e emergjencave, regjistrimin e sigurtë në rrjet dhe procedurat e backup-it.

Procedurat e operimit mbulojnë si operacionet normale ashtu edhe administrimin e incidenteve. Mbulohen maksimalisht incidentet e parashikueshme, duke përfshirë keqfunksionimin e pajisjeve ose të programeve, të dhënat jo të sakta ose të dëmtuara, difektet në pjesët që i përkasin ofruesve të jashtëm të shërbimeve ose të partnerëve në biznes (business partner), sulmet keqdashëse dhe thyerjet e konfidencialitetit.

KONTRAKTORËT E BURIMEVE TË JASHTME

Kërkesat e sigurisë së Autoritetit duhet t'i bashkëngjiten të gjitha kontratave që bëhen me ofruesit e shërbimeve, për të garantuar sigurinë mbi veprimet e punonjësve të tyre gjatë lidhjeve me rrjetin e Autoritetin.

6.2. Kontrolli i ndryshimeve

Të gjitha ndryshimet në pajisjet dhe në sistemet që përpunojnë informacionin i nënshtrohen procedurave zyrtare të administrimit të ndryshimeve duke përfshirë identifikimin dhe rregjistrimin e ndryshimeve të rendesishme, planifikimin dhe testimin e ndryshimeve, dhe proceduren e miratimit të ndryshimeve të propozuara.

Kur bëhen ndryshime ose futen sisteme të reja të merret pasasysh sa me poshtë:

- Identifikimi i arsyeve dhe rregjistrimi i rastit të procesit;
- Personat e autorizuar për zbatimin e ndryshimeve të përcaktuar në mënyrë të qartë;
- Planifikimi dhe testimi i ndryshimeve/sistemeve të reja;
- Vlerësimi i ndikimeve te mundshme, duke përfshirë ndikimet në siguri (vlerësimi i riskut kryhet para zbatimit të ndryshimeve);
- Procedura e miratimit për ndryshimet e propozuara/sistemeve;
- Planifikimi i migrimit/transferimit në zonën e prodhimit (duke i kushtuar vëmendje sigurisë së SI);
- Komunikimi për të gjithë personat përkatës;
- Procedurave të Fallback, përfshirë procedurat dhe përgjegjësitë për ndërprerjen dhe rikuperimin nga ndryshimet e pasuksesshme dhe ngjarjet e paparashikuara gjatë vendosjes së sistemeve të reja.

6.3. Programet keqdashëse

Të gjitha pajiset e teknologjisë së informacionit duhet të jenë të mbrojtura nga programet keqdashëse, (ku përfshihen viruset e kompjuterave, si dhe çdo tip tjetër i njohur dhe i klasifikuar si kërcënim informatik). Në qëllim të kësaj instalohen sisteme për kontrollin dhe për parandalimin e veprimeve keqdashëse. Në të gjitha PC dhe serverat e Autoritetit instalohet dhe vihet në funksionim një program i licensuar antivirus. Ai duhet të përditësohet automatikisht, në mënyrë të vazhdueshme, nën kontrollin e punonjësve të teknologjisë së informacionit. Ç'instalimi ose ç'aktivizimi i programeve antivirus trajtohet si shkelje serioze.

6.4. Backup-i i të dhënave

BAZAT E TË DHËNAVE TË AUTORITETIT

Drejtoria e Teknologjisë dhe Informacionit është përgjegjëse për të siguruar që të gjitha të dhënat sensitive të mbajtura në serverat e Autoritetit t'u bëhet backup (kopje) i rregullt në përputhje me procedurat e përcaktuara, për çdo sistem (përfshi këtu edhe file/print servers). Kopjet (backup-et) e të dhënave duhet të ruhen në vende të mbrojtura nga zjarri dhe jashtë ambienteve ku mbahen serverat prej të cilëve janë marrë ato. Kopjet (backup) e të dhënave duhet të testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme. Procedurat e rikrijimit (restore) të të dhënave duhet të testohen rregullisht për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar.

TË DHËNAT QË NDODHEN NË KOMPJUTERAT PERSONALË TË PËRDORUESVE

Çdo individ, i cili ruan të dhëna në një kompjuter personal, është përgjegjës personalisht për të siguruar kopjet e duhura të backup-it për të mbrojtur të dhënat nga humbjet duhet të firmosë një dokument të pranimit të kësaj përgjegjësie.

6.5. Mbajtja e log-eve

Është e detyrueshme të mbahen e të ruhen log-e (shënime të shkurtuara) për të gjitha aksesimet në sistemet e Autoritetit dhe per të gjitha përdorimet e sistemeve. Log-et shqyrtohen rregullisht, me qëllim identifikimin e shkeljeve (thyerjeve) të sigurisë, për të gjithë përdoruesit e brendshëm e të jashtëm

Autoriteti duhet të përcaktojë një politikë të shkruar për menaxhimin e log-eve sipas kërkesave të tij. Kjo politikë duhet të specifikojë qartë të gjitha kërkesat për ruajtjen e log-eve përkatëse për çdo sistem/pajisje të autoritetit, procedurat e administrimit dhe përgjegjësitë.

Log-et duhet të ruhen në ambiente të cilat kanë sigurinë e nevojshme fizike dhe janë të mbrojtura nga lagështira, fushat magnetike, zjarri etj dhe duhet të ruhen nga aksesi prej personave të paautorizuar në mënyrë që të sigurohet integriteti, konfidencialiteti dhe besueshmëria e tyre.

6.6. Politika e përdorimit të Internetit dhe të Postës Elektronike

I gjithë personeli i Autoritetit (përfshi këtu kontraktorët dhe konsulentët), të cilit i është dhënë akses në Internet dhe në shërbim email-i zbaton politikën e përdorimit të internetit si dhe rregullat dhe procedurat qe rrjedhin nga ajo.

KONTROLLI I AKSESIT

Për çdo burim informacioni të Autoritetit, përdoruesve u jepet akses vetëm në përputhje me funksionet e tyre për kryerjen e detyrave dhe ky akses kontrollohet me rreptësi për të ruajtur integritetin dhe sigurinë e aktivitetit. Hapi i parë i kontrollit të aksesit është identifikimi i përdoruesit. Kjo mbulon procedurat për t'u siguruar që çdo sistem është i aftë të njohë personat e autorizuar dhe të kryejë veprimet e duhura, në rastet e përpjekjeve për aksesim të paautorizuar. Çdo përdorues i sistemeve, qoftë ai personel i brendshëm i Autoritetit, aplikues (kandidat) i jashtëm, nëpunës i një institucioni ose organizate tjetër, kontraktues, konsulent ose pjesëtar i personelit që punon për ofruesit e shërbimeve, identifikohet në mënyrë individuale nëpërmjet një llogarie unike përdoruesi, e cila do të caktohet vetëm nëpërmjet një autorizimi me shkrim nga një drejtues Departamenti i Autoritetit dhe me miratimin e Drejtorit të Drejtorisë së Teknologjisë dhe Informacionit. Kjo zbatohet për të gjithë personat, pavarësisht nga rolet e tyre. Ndalohet rreptësisht shpërndarja e llogarisë personale në persona të tjerë. Thyerja e këtij rregulli do të trajtohet si një shkelje e rëndë. Një llogari unike përdoruesi nuk siguron vetëm mënyrën e autentifikimit për përdoruesit e ligjshëm, por gjithashtu garanton që Autoriteti do të jetë gjithmonë e aftë të përcaktojë përgjegjësinë e individëve për aktivitetet e tyre në sistemet e saj. Ndalohet rreptësisht dy ose më shumë aksesime të njëkohshme me të njëjtën llogari përdoruesi. Fillimisht përdoruesit nuk do të kenë asnjë të drejtë aksesimi. Atyre do t'u jepet akses vetëm në pjesët minimale të sistemit, që u nevojiten për kryerjen e aktivitetit te tyre.

Në të gjitha rastet, ndiqen procedura të dokumentuara për:

- Rregjistrimin e përdoruesve të rinj;
- Ndryshimin e statusit për një përdorues ekzistues (për shembull ndërprerjen e llogarisë së përdoruesit kur ai largohet nga puna ose mungon për një kohë të gjatë ose ndryshimin e privilegjeve të aksesit të tij);
- Mbylljen përfundimtare të një llogarie përdoruesi.

Natyra e këtyre procedurave dhe përgjegjësitë për administrimin e tyre mund të ndryshojnë në varësi të kategorisë së përdoruesit.

Çdo person që autorizohet të aksesojë sistemet e AMF-së, për identifikimin e tij, ka një llogari përdoruesi unike të përbërë nga një emër (user name) dhe një fjalëkalim (password). Fjalëkalimi duhet të jetë konformë politikave të njohura të sigurisë dhe aksesimi i pajisjeve dhe i sistemeve të AMF-së bëhet në përputhje me detyrat funksionale të përdoruesit.

6.7. Përdoruesit e brendshëm

Përdoruesit e brendshëm përfshijnë punonjësit e Autoritetit, kontaktorët, konsulentët dhe punonjësit e ofruesve të shërbimeve të Autoritetit. Aksesi për përdoruesit e brendshëm në sistemet e Autoritetit duhet të jetë në përputhje me detyrat që ata kanë. Detyrat do të jenë të përcaktuara qartë, dhe për të minimizuar rrezikun e aktiviteteve mashtruese ose keqdashëse, ndarja e tyre do të jetë e detyrueshme. Kur një përdorues ndryshon detyrë, ai humbet të drejtat e aksesimit që lidheshin me detyrën e mëparëshme. Akumulimi në kohe i privilegjeve evitohet dhe të monitorohet vazhdimisht nga Drejtoria e TI-së.

Fillimisht, punonjësit e Autoritetit nuk kanë të drejta aksesimi në sistemet e saj. Më pas, atyre u jepet vetëm një nivel minimal aksesimi, i domosdoshëm për kryerjen e detyrave që ata mbulojnë.

LLOGARITË E PËRDORUESVE

Llogaritë e përdoruesve krijohen dhe administrohen nga punonjësit e drejtorise sëteknologjisë së informacionit. Ata përdoren për aksesimin e të gjitha shërbimeve të teknologjisë së informacionit të Autoritetit, përfshi këtu rrjetin e brendshëm, pajisjet dhe sistemet e Autoritetit. Procedura për administrimin e llogarive të përdoruesve të Autoritetit dokumentohet sipas një rregullore të vecantë. Kjo procedurë zbatohet në të gjitha rastet kur:

- Nevojitet një llogari e re (për shëmbull për një punonjës të ri);
- Llogaria e një punonjësi duhet të pezullohet për një periudhë kohe ose kur duhet të riaktivizohet mbas pezullimit;
- Do të ndryshohen privilegjet e aksesimit (për shembull kur kalohet në një rol me përgjegjësi më të madhe);
- Një nëpunës, pjesëtar i personelit të Autoritetit, largohet nga puna (fshirja e përhershme e llogarisë).

ADMINISTRIMI I FJALËKALIMEVE

Të gjithë përdoruesit e Autoritetit instruktohen në lidhje me mënyrat e administrimit të fjalëkalimeve.

Politikat e fjalekalimit duhet të zbatohen për të zvogëluar rrezikun e hyrjes së paautorizuar.

Këtu futet:

- Zgjedhja e fjalëkalimit fillestar;
- Ndryshimi i fjalëkalimit dhe këshilla të njohura sigurie për zgjedhjen e tij;
- Mbrojta e fjalëkalimit si dhe ndalimi i dhënies së fjalëkalimit midis përdoruesve;
- Inicializimi ose mbivendosja e fjalëkalimit (në qoftë se një llogari përdoruesi është mbyllur ose në qoftë se përdoruesi ka harruar fjalëkalimin). Mbivendosja e fjalëkalimit duhet të bëhet vetëm nga personeli i autorizuar i teknologjisë së informacionit pas një kërkesë me shkrim. Përdoruesve u kërkohet të firmosin një marrëveshje ku pranojnë se ata i kanë lexuar e i kanë kuptuar rregullat, dhe se do t'i zbatojnë ato. Kjo procedurë përfshihet në procedurat e punësimit të personelit të Autoritetit.

MONITORIMI I PROFILEVE TË PËRDORUESVE

Është e rëndësishme të garantohet që:

- Vetëm përdoruesve të duhur u është lejuar akses në sistemet e Autoritetit (janë eliminuar të gjitha llogaritë që kanë skaduar);
- Përdoruesit nuk kanë privilegje aksesimi të niveleve më të larta nga ato që u duhen për të kryer punën e tyre (është eliminuar "shtimi i privilegjeve"). Për të detyruar zbatimin e kërkesat e mësipërme, të gjithë llogaritë e përdoruesve dhe caktimi i profileve të tyre do të rishikohen nga drejtori i drejtorisë përkatëse. Kjo bëhet një herë në gjashtë muaj. Si rezultat i këtij rishikimi hartohet lista e emrave të të gjithë përdoruesve të brendshëm të vlefshëm, me profilet e tyre përkatës. Kjo listë do të mbahet dhe do të kontrollohet nga Departamenti i TI.

6.8. Përdoruesit e jashtëm

Tek përdoruesit e jashtëm përfshihen të gjithë individët jashtë kategorisë së përdoruesve të brendshëm, që janë të autorizuar të aksesojnë sistemet e Autoritetit.

LLOGARITË E PËRDORUESVE

Caktimi i llogarive të përdoruesve është përgjegjësi e drejtorive përkatëse të Autoritetit. Përdoruesit e jashtëm instruktohen që të ruajnë konfidencialitetin e llogarisë së tyre, gjatë procesit të trainimit për përdorimin e sistemeve. Formati i llogarive të përdoruesve standardizohet, aq sa është e mundur, për të gjithë përdoruesit e jashtëm, me anë të një bashkëpunimi midis teknologjisë së informacionit dhe drejtorive të Autoritetit Ky format do të jetë pjesë e dokumentacionit të sistemeve. Lista e të gjithë përdoruesve të jashtëm të autorizuar, bashkë me llogaritë e tyre, duhet të mbahet nga Drejtoria e TI.

AUTENTIFIKIMI

Të gjithë përdoruesit e jashtëm, para se t'u jepet akses në sistemet e informacionit të Autoritetit, identifikohen në mënyrë të vetme. Niveli i autentifikimit që duhet të kërkohet për përdoruesit e jashtëm, varet nga ndjeshmëria e të dhënave që do të aksesohen dhe risku që i shoqëron në qoftë se këto të dhëna kompromentohen. Mënyrat e autentifikimit që përdor Autoriteti janë:

- Kombinimi i emrit të përdoruesit dhe fjalëkalimit e identifikuar me emrin llogari;
- Përdorimi i smart cards ose i formave të tjera hardware të autentikimit Përpara kalimit të çdo aplikimi në mjedisin "produkt", përdoruesi i aplikimit duhet të ndërmarë një vlerësim zyrtar të tij, duke u konsultuar me specialistët të Drejtorisë së Teknologjisë së Informacionit, për:
  - Sensitivitetin e të dhënave që përpunohen;
  - Nivelin e rrezikut nga aksesi i përdoruesve.

MARRËVESHJET ME KONTRATË

Kërkesat e sigurisë përfshihen në të gjitha kontratat ndërmjet Autoritetit dhe përdoruesve të jashtëm për të administruar aksesin e tyre direkt (online) në sistemet e Autoritetit. Këtu mund të përfshihet:

- Një deklaratë për pranimin dhe për respektimin e të drejtave të aksesimit;
- Deklaratë për pranimin e procedurës "Administrimi i Fjalëkalimeve";
- Të marrin përsipër përdorimin e programeve antivirus të miratuara nga Autoriteti, në të gjithë kompjuterat që mund të lidhen me sistemet e Autoritetit, dhe të garantojnë që programet antivirus rinovohen (update) të paktën një herë në ditë;
- Të marrin përsipër ruajtjen e konfidencialitetit të plotë për të gjitha të dhënat dhe informacionet që ata mund të marrin nga sistemet e Autoritetit.

DHËNIA E PRIVILEGJEVE

Në rastet e përdoruesve të jashtëm, privilegjet caktohen në bazë të profileve të sigurisë. Këto profile zbatohen dhe testohen zyrtarisht, përpara testimit të tyre prej përdoruesve. Për privilegjevet e përdoruesve vendos dhe të firmos drejtori i drejtorisë përgjegjëse të sistemit, duke marrë në konsideratë mendimin e specialistëve të Drejtorisë së Teknologjisë së Informacionit. Çdo ndryshim i tyre duhet të miratohet zyrtarisht nga drejtori i drejtorisë përgjegjëse të sistemit. Privilegjet përcaktohen në dokumentacionet e aplikimeve dhe ruhen të sigurta sipas rregullave të kontrollit zyrtar të dokumenteve, nga Drejtoria e TI.

ENKRIPTIMI

Të gjitha të dhënat që shkëmbehen ndërmjet sistemeve të Autoritetit dhe përdoruesve të jashtëm duhet të enkriptohen.

7. ZHVILLIMI DHE MIRËMBAJTJA E SISTEMEVE

7.1. Zhvillimi i programeve

Kërkesat e sigurisë dizenjohen brenda programeve/aplikimeve, duke reflektuar vlerat e aseteve të informacionit dhe dëmtimet e mundshme, të cilat mund të vijnë si rezultat i dështimit ose mungesës së sigurisë. Si rregull ato miratohen nga Drejtoria e TI, përpara fillimit të punës për zhvillimin e aplikimit. Masat e sigurisë përcaktohen qartë në dokumentacionin e programeve/aplikimeve, përfshi këtu procedurat operacionale. Në mënyrë të veçantë, të gjitha aplikimet dizenjohen në mënyrë të tillë që të parandalojnë mundësinë e aksesimit të njëkohshëm të shumë përdoruesve, me të njëjtin kod.

7.2. Kalimi nga mjedisi i zhvillimit në atë produkt

Krijimi i çdo lloj programi kalon nëpër tri ndarje logjike (dhe zakonisht edhe fizike) të mjediseve, të cilat emërtohen Zhvillim, Testim dhe Produkt. Procesi i kalimit të programeve nga Zhvillimi në Testim dhe pastaj në Produkt, bëhet në përputhje me procedurat e Administrimit të ndryshimeve të Autoritetit.

MJEDISI I ZHVILLIMIT

Mjedisi i zhvillimit është nën kontrollin e ekipit që zhvillon (krijon) aplikimin, i cili është përgjegjës për sigurinë e tij. Drejtoria e Teknologjisë së Informacionit është përgjegjëse për funksionimin dhe për mirëmbajtjen e sistemeve që janë në zhvillim.

MJEDISI I TESTIMIT

Mjedisi i Testimit është nën kontrollin e Drejtorisë së Teknologjisë së Informacionit. Të gjitha profilet e sigurisë dhe lejet e aksesimit përcaktohen dhe jepen me miratimin e Drejtorisë së Teknologjisë së Informacionit. Kur pjesë të reja të zhvillimit të programeve janë gati për t'u testuar, ato duhet të migrohen nga mjedisi në zhvillim (krijim) në atë për testim. Kjo procedurë kryhet në përputhje me procedurat e administrimit të ndryshimeve, të cilat kërkojnë që:

- Zhvilluesit (krijuesit) përgjegjës të shkruajnë një dokumentacion të plotë, që mbulon instalimin, testimin dhe funksionimin e programit të ri;
- Drejtoria e Teknologjisë së Informacionit të përcaktojë se kush do ta instalojë, do ta testojë dhe do ta ekzekutojë programin, në përputhje me dokumentacionin;
- Në qoftë se konstatohet ndonjë problem ose gabim, ai do të dokumentohet nga Drejtoria e Teknologjisë së Informacionit dhe do të kthehet për korrigjim;
- Kjo procedurë të përsëritet sa herë që është e nevojshme derisa të dyja palët të jenë të kënaqura me rezultatet e testimit;
- Në fund, programi të përgatitet për kalimin në produkt.

MJEDISI I PRODUKTIT

Kur bëhet instalimi në mjedisin produkt, programet/aplikimet nuk mund të ndryshohen ose të modifikohen në asnjë lloj mënyrë, përveç rasteve të ndërhyrjeve urgjente, të kontrolluara rreptësisht për të rregulluar një problem operacional serioz, siç përshkruhet në pikën 8.3 . Mjedisi produkt është nën kontrollin e Drejtorisë së Teknologjisë së Informacionit. Të gjitha profilet e sigurisë dhe lejet e aksesimit përcaktohen me miratimin e Drejtorisë së Teknologjisë së Informacionit. Migrimi i programeve të rinj, nga Test në Produkt, bëhet në përputhje me procedurat e "Administrimit të ndryshimeve". Pas migrimit ato janë nën kontrollin e palëve përkatëse, të cilat mbajnë përgjegjësi për funksionimin në mjedisin produkt.

Mjediset e zhvillimit, të testimit dhe produktet janë maksimalisht të ndara. Asnjë zhvillim/ndryshim aplikimi nuk duhet të kryhet në mjedise testimi ose produkti. Për këtë do të jetë e detyrueshme kryerja me rigorozitet e kontrolleve të zëvendësimit dhe të kalimit të aplikimeve nga ambienti i tyre i zhvillimit në atë të testimit dhe nga ai i testimit, në atë te produktit.

7.3. Aksesi në mjediset Test dhe Produkt

Personeli i zhvillimit të aplikimit i lejohet nëse është e nevojshme të ketë akses në sistemet test dhe produkt ashtu si dhe në mjedisin në zhvillim. Aksesime të tilla duhet të kontrollohen me kujdes:

- Niveli i aksesit të lejuar, për çdo pjestar të grupit të zhvillimit të aplikimit, do të jetë minimumi i duhur për të kryer ndërhyrjet e nevojshme;
- Të gjitha aksesimet do të caktohen dhe do të miratohen nga drejtori i departamentit pronar të sistemit dhe nga Drejtori i Drejtorisë së Teknologjisë së Informacionit;
- Të gjitha aksesimet duhet të kryhen sipas procedurave të "Administrimit të ndryshimeve", të shoqëruara me loge për të gjitha veprimet që kryhen;
- Të gjitha aksesimet duhet të kryhen duke u konsultuar në mënyrë të vazhdueshme me përfaqësuesit e Drejtorisë së Teknologjisë së Informacionit. Konsultime të tilla mund të kryhen me telefon ose brenda institucionit ose nëpërmjet takimeve direkte;
- Në mjediset produkt nuk do të bëhet asnjë ndryshim i kodit të programit pa u testuar më parë në mjedisin test. Bëjnë përjashtim rastet, kur nevojitet urgjentisht të korrigjohet menjëherë një dëmtim serioz i sistemit apo si pjesë e procedurave të rekuperimit (recovery), të tij. Të gjitha korrigjimet e tilla do të kryhen nga specialistët e Teknologjisë së Informacionit;
- Për çdo përmirësim të kodit ose për çdo ndryshim i të dhënave, që do të bëhet në mjedisin produkt, duhet të mbahen shënime të plota.

8. ADMINISTRIMI I VAZHDUESHMËRISË SË AKTIVITETIT

Duke u konsultuar me drejtorët e të gjitha departamenteve, Drejtoria së Teknologjisë së Informacionit zhvillon dhe mban plane për rikrijimin e të gjitha proceseve dhe shërbimeve kritike të aktivitetit, në rastet e ndërprerjeve serioze. Ndërprerje të tilla mund të shkaktohen nga shkaqe natyrore, nga aksidente, nga difekte të pajisjeve, nga veprime të qëllimshme ose nga difekte të shërbimeve.

8.1. Vazhdueshmëria

Planet për vazhdueshmërinë e aktivitetit përfshijnë masat për reduktimin e riskut, për kufizimin e pasojave të shkaktuara prej një kërcënimi që mund të ndodhë, dhe për garantimin e rifillimit sa më të shpejtë të operacioneve kritike. Planet për vazhdueshmërinë e aktivitetit përgatiten për çdo aktivitet të Autoritetit. Planet e vazhdueshmërisë duhet të mundësojnë funksionimin në vazhdimësi të aktiviteteve në raste dëmtimesh, difektesh ose humbjesh të shërbimeve apo të pajisjeve. Ato përfshijnë:

- Identifikimin dhe vendosjen e prioriteteve për proceset kritike të biznesit;
- Identifikimin e kërcënimeve të mundshme që mund të kenë efekt në këto procese;
- Përcaktimin e ndikimit të mundshëm të katastrofave të ndryshme në aktivitetet e biznesit;
- Identifikimin dhe realizimin e marrëveshjeve për çdo përgjegjësi, në rast gjendjeje të jashtëzakonshme;
- Dokumentacionin për procedurat dhe proceset për të cilat është rënë dakord;
- Edukimin e personelit në ekzekutimin e procedurave;

- Testimin e planeve;
- Përmirësimin e vazhdueshëm të planeve.

Procesi i planifikimit të vazhdueshmërisë së aktivitetit duhet të sigurojë, mbajtjen në punë të proceseve dhe shërbimeve kritike të Autoritetit. Drejtuesit e drejtorive janë përgjegjës për planet e vazhdueshmërisë së aktivitetit për sistemet dhe pajisjet që kanë në pronësi të tyre. Të paktën një kopje e çdo plani të tillë duhet të ruhet në një vend të sigurt, jashtë ndërtesës, përtë siguruar disponueshmërinë e tij në çdo kohë. Plane të tilla krijohen për sistemet e informaciont në një vit nga hyrja në fuqi e dokumentit.

8.2. Rikrijimi i informacionit në rast katastrofash

Për të rindërtuar (rikrijuar) sistemet dhe shërbimet prioritare kompjuterike në raste katastrofash është e domosdoshme krijimi dhe të ruajtja e planeve për këtë qellim. Rifillimi i këtyre sistemeve duhet të bëhet në një interval kohe sa më të shkurtër. Për çdo sistem dhe shërbim krijohet një plan rindërtimi (recovery), i cili mbahet nga një person i caktuar. Këtu përfshihen edhe shërbimet që sigurohen nga ofruesit e jashtëm. Përgjegjësia për procedurat në raste katastrofash, për manualet dhe planet e zëvendësimittë të dhënave të humbura dhe për planet e vazhdueshmërisë, është e departamenteve që janë pronarë të tyre.

8.3. Përmirësimi

Të gjitha planet për vazhdueshmërinë e aktivitetit dhe planet e rikrijimit rishikohen e përmirësohen të paktën një herë në vit. Planet të cilat vjetërohen shpejt, si rezultat i ndryshimeve që ndodhin brenda ose jashtë institucionit përmirësohen (updating) në mënyrë të vazhdueshme me qëllim mbrojtjen e investimit mbi planin fillestarë dhe për të garantuar efektshmërinë e vazhdueshme të vazhdueshmërisë. Çdo departament, drejtori apo sektor duhet të ketë një person të autorizuar, i cili do të jetë përgjegjës për identifikimin dhe për aplikimin e ndryshimeve në këto plane. Nevoja për ndryshime të veçanta mund të rishikohet çdo muaj. I tërë plani duhet të jetë subjekt i një rishikimi vjetor nga Drejtorisë së Teknologjisë së Informacionit.

9. PËRPUTHJA ME LIGJIN

9.1. Kërkesat ligjore

LEGJISLACIONI

Drejtorëve të drejtorive u kërkohet të njohin kërkesat e legjislacionit dhe akteve nënligjore, në të cilat AMF mbështët veprimtarinë e saj, dhe të sigurohen që personeli i tyre vepron në pajtim me kërkesat e legjislacionit në fuqi.

PRONA INTELEKTUALE (E DREJTA E AUTORIT)

Shkelja e të drejtës së autorit çon në veprime antiligjore dhe, për çështje serioze në procedim penal. Pronësia e programeve përcaktohet nëpërmjet licencës, e cila kufizon përdorimin e produktit në kompjutera të caktuar.

- Asnjë program nuk instalohet në kompjuterat e Autoritetit pa patur një dokument të shkruar e të firmosur nga përgjegjësi i Drejtorisë së Teknologjisë së Informacionit. Si rregull i përgjithshëm, të gjitha programet instalohen vetëm nga personeli i helpdesk-ut;
- Programet nuk lejohet të kopjohen nga një kompjuter në një tjetër, pa patur të dokumentuar të drejtën e kopjimit nga pronari i tij;
- Kopjimi i programeve që janë në pronësi të Autoritetit, për t'u përdorur në kompjuterat që nuk i përkasin Autoritetit, për çfarëdo lloj qëllimi të ndryshëm nga aktivitetet e autorizuara, përbën thyerje të të drejtës së autorit dhe do të trajtohet si shkelje serioze.

9.2. Politika e Sigurisë

Elementet e nje politike sigurie TI janë si mëposhtë:

- Përkufizim i sigurisë së informacionit - objektivat dhe qëllimi (përfshirë konfidencialiteti i të dhënave);
- Parimet, standardet dhe kërkesat e detajuara të përputhshmërisë;
- Përkufizim të përgjegjësive të përgjithshme dhe specifike për të gjitha aspektet e sigurisë së informacionit;
- Përdorimi i aseteve të informacionit dhe aksesi në email, Internet;
- Mënyra dhe metodat e aksesit;
- Procedurat e backup-it;
- Elemente të trajnimit dhe të edukimit mbi sigurinë;
- Procesi për raportimin e incidenteve të dyshimta të sigurisë;
- Planet e vazhdueshmërisë së biznesit;
- Procedurat e trajtimit të programeve me ndikim negativ;
- Metodat e komunikimit me stafin mbi politikat dhe procedurat e përshtatura për sigurinë e SI;
- Dispozitat e trajnimit/arsimimit dhe politikat disiplinore;
- Një deklaratë mbi përkushtimin e menaxhimit, i cili mbështet qëllimin dhe parimet në përputhje me strategjinë dhe funksionet e përgjithshme të sigurisë së informacionit.

KONTROLLET

Të gjitha departamentet dhe degët janë subjekt i një kontrolli zyrtar vjetor për të siguruar zbatimin e rregullave dhe standardeve të sigurisë. Pronarët e aseteve të informacionit mbështesin rregullisht auditime për përputhjen e sistemeve të tyre me këtë udhëzim. Të gjitha pajisjet kompjuterike kontrollohen nga Drejtoria e Teknologjisë së Informacionit për

përputhjen me standardet e zbatimit të sigurisë. Këto kontrolle përfshijnë ekzaminimin e sistemeve operacionale për t'u siguruar që kontrollet e sigurisë të pajisjeve dhe të programeve janë zbatuar me korrektësi.

DREJTOR I PËRGJITHSHËM EKZEKUTIV

ERVIN KOÇI