D

REPUBLIKA E SHQIPËRISË
MINISTRIA E FINANCAVE DHE EKONOMISË
DREJTORIA E PËRGJITHSHME E TATIMEVE

Nr. 12445/1 prot. Tiranë, më 3.7.2020

RREGULLORE

Nr._____Datë___.___.2020

"PËR SIGURINË E INFORMACIONIT NË DREJTORINË E PËRGJITHSHME TË TATIMEVE"

Tabela e përmbajtjes

1. TË PËRGJITHSHME

1.1 Objekti

Objekt i kësaj Rregullore është përcaktimi i parimeve dhe rregullave të Përgjithshme të Sigurisë së Informacionit në DPT dhe përcaktimi i përgjegjësive për veprimet që lidhen me sigurinë me qëllim ruajtjen e integritetit, disponueshmërisë dhe konfidencialitetit të aseteve të informacionit të DPT.

1.2 Baza Ligjore

Rregullorja është hartuar në bazë dhe për zbatim të nenit 16 të ligjit nr.9920, datë 19.5.2008 "Për Procedurat Tatimore në Republikën e Shqipërisë, i ndryshuar", ligjin nr. 9154 datë 06.11.2003 "Për arkivat", ligjit nr. 8457, datë 11.02.1999 "Për informacionin e klasifikuar "sekret shtetëror", si dhe VKM nr. 189, datë 04.03.2015 "Për Sigurimin Fizik të Informacionit të Klasifikuar "Sekret Shtetëror", si dhe ligji nr. 152/2013 "Për Nëpunësin Civil", i ndryshuar.

1.3 Fusha e Zbatimit

Kjo rregullore zbatohet nga të gjithë përdoruesit/aksesuesit të përcaktuar pikën 2 të kësaj rregulloreje. Të gjithë përdoruesit/aksesuesit duhet ta kuptojnë dhe përvetësojnë këtë rregullore si dhe janë përgjegjës për garantimin e mbrojtjes dhe sigurisë së sistemeve të DPT-së dhe informacionit që përdorin. Ata kanë një funksion për të luajtur si dhe një kontribut për të dhënë në lidhje më përdorimin e sigurtë të teknologjisë dhe informacionit që përmban. Qëllimi i kësaj rregullore është garantimi i përputhshmërisë me aktet ligjore qe rregullojnë çështjet e sigurisë së informacionit si dhe praktikave më të mira siç përcaktohet në standardin e sigurisë ISO 27001.

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 DPT. 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 janë të disponueshme dhe operacionale (të gatshme për punë) sa herë që nevojitet një gjë e tillë.

KONFIDENCIALITETI

Informacioni konfidencial përdoret vetëm nga persona të autorizuar. Kjo është veçanërisht e rëndësishme për informacionet me ndjeshmëri të lartë.

PËRGJEGJËSIA

Të gjithë përdoruesit/aksesuesit mbajnë përgjegjësi për pasojat qe rrjedhin direkt nga veprimet dhe/ose mosveprimet e tyre që kanë të bëjnë me asetet e informacionit të DPT. Çdo përdoruesi/aksesuesi i bëhen të qarta përgjegjësitë e tij në lidhje me detyrimet qe lindin nga ushtrimi i detyrës.

MBROJTJA FIZIKE

Të gjitha asetet e informacionit të DPT mbrohen në shkallën më të lartë nga dëmtimet fizike.

1.5 Objektivat e Sigurisë

1. Aksesimi i të gjitha sistemeve të informacionit të DPT kontrollohet rreptësisht për të garantuar integritetin dhe mbrojtjen e tyre.

2. Të gjitha sistemet (përfshirë këtu mjediset e zhvillimit, të testimit dhe produktet) mbrohen nga kërcënimet dhe nga dëmtimet fizike.

3. Të gjithë individët mbajnë përgjegjësi direkte për veprimet që kryejnë mbi asetet e informacionit të DPT.

4. Çdo person që autorizohet të aksesojë sistemet e DPT, për identifikimin e tij, ka një llogari përdoruesi unike të përbërë nga një emër (*user name)* dhe një fjalëkalim (*password*). Përdoruesi detyrohet të mbajë të fshehtë fjalëkalimin e tij dhe ta ndryshojë atë në mënyrë periodike sa më shpesh të jetë e mundur. Fjalëkalimi duhet të jetë konform politikave të njohura të sigurisë të shpjeguara më poshtë. Aksesimi i pajisjeve dhe i sistemeve të DPT bëhet në përputhje me detyrat funksionale të përdoruesit, pas plotësimit nga eprori direkt i formularëve përkatës të miratuar për këtë çështje. Asnjë përdoruesi nuk i lejohet të aksesojë lirisht funksionet e ndryshme të sistemeve.

5. Ndalohet rreptësisht përdorimi i të njëjtës llogari, prej dy ose më shumë përdoruesve. Çdo rast i tillë trajtohet si një shkelje serioze e rregullave të sigurisë.

6. Çdo sistem i DPT në përdorim është i aksesueshëm nga një sistem menush dhe mbi bazën e aksesimit unik. Asnjë nga sistemet e DPT, në asnjë rrethanë, nuk do të lejojë hyrjen e njëkohshme të më shumë se një përdoruesi me të njëjtin fjalëkalim.

7. Për të gjitha përdorimet e sistemeve mbahen log-e (shënime të shkurtuara). Log-et shqyrtohen rregullisht me qëllim identifikimin e shkeljeve (thyerjeve) të sigurisë.

8. Përpara se të bëhen zhvillime/ndryshime aplikimesh, hartohen masa/procedura sigurie, të miratuara nga Drejtoria TIK e AKSHI-t në DPT (në vijim Drejtoria TIK).

9. Mjediset e zhvillimit, të testimit dhe produktet janë maksimalisht të ndara. Asnjë zhvillim/ndryshim aplikimi nuk duhet të kryhet në mjedise 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 të produktit.

10. 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 DPT) hartohen masa/procedura sigurie. Ato klasifikohen si Konfidenciale dhe kopja origjinale e tyre do të ruhet në mënyrë të sigurtë nga anëtari i Komitetit të Sigurisë, përgjegjës për TIK.

11. Masat e sigurisë zhvillohen në përputhje me funksionimin e sistemeve të DPT, prej një regjimi pune 24 orë në ditë, për 7 ditë në javë.

AKSESI I PËRDORUESVE – PËRDORUESIT E BRENDSHËM

12. Fillimisht, punonjësit e DPT nuk kanë të drejta aksesimi në sistemet e saj. Çdo punonjësi në varësi të detyrave funksionale të përcaktuara në Rregulloren e Brendshme të Administratës Tatimore Qendrore, të miratuar, i krijohet mundësia e aksesimit nëpërmjet plotësimit të formularëve përkatës të menaxhimit të llogarive të postës elektronike dhe të sistemeve miratuar nga eprori direkt. Në rast të ndryshimit të pozicionit të punës bëhet dhe ndryshimi i të drejtave të aksesimit në sisteme, nëpërmjet plotësimit të këtyre formularëve nga eprori direkt.

13. Dhënia e të drejtave të aksesimit në sisteme bazohet në pozicionin e punës të punonjësit të DPT duke marrë parasysh detyrat e tij funksionale.

14. Aksesimi i sistemeve të DPT përcaktohet në bazë të detyrave të punonjësve, të cilat përcaktohen qartë. Kur një përdorues i sistemeve ndryshon detyrë, ai humbet të drejtat e aksesit që lidheshin me detyrën e mëparshme.

15. Akumulimi në kohë i privilegjeve duhet të monitorohet dhe të shmanget nga eprori direkt dhe nga Drejtoria TIK.

AKSESI I PËRDORUESIT – PËRDORUESIT E JASHTËM

16. Asnjë përdorues i jashtëm nuk mund të ketë akses në sisteme të DPT-së derisa të autorizohet me shkrim nga DPT.

17. Përpara se t'u jepet e drejta e aksesimit, të gjithë përdoruesit e jashtëm të sistemeve të DPT nënshkruajnë një deklaratë përgjegjshmërie, ku pranojnë se do të respektojnë të gjitha rregullat/procedurat e kësaj rregullore.

18. Të gjithë përdoruesit e jashtëm identifikohen në mënyrë të qartë (log-in) para se t'u jepet e drejta e aksesimit në sisteme.

19. Të dhënat që vijnë nga përdoruesit e jashtëm të sistemeve të DPT mbrohen gjatë gjithë kalimit dhe hyrjes së tyre në sisteme.

1.6 Kontrolli i dokumenteve

Komiteti është përgjegjës për këtë rregullore dhe mban përgjegjësi për zbatimin e tij. Komiteti kujdeset që:

- I gjithë personeli i DPT të inkurajohet vazhdimisht të bëjë komente dhe sugjerime për modifikimin e rregullores.
- Komiteti paraqet një raport periodik me shkrim, para Drejtorit të Përgjithshëm, çdo 6 muaj, si dhe raportim të menjëhershëm në rastet e dyshuara të thyerjes së sigurisë, mbi gjendjen e sigurisë, duke dhënë komentet mbi funksionimin e rregullores dhe rekomandimet për çdo ndryshim të nevojshëm.
- Rregullorja është objekt i një procedure zyrtare vjetore rishikimi, nën kontrollin e komitetit.

KOMITETI PËRGJEGJËS PËR SIGURINË

DETYRAT E ANËTARËVE TË KOMITETIT

Detyrë e anëtarëve është të krijojnë, të implementojnë dhe të mirëmbajnë një politikë sigurie që të ndihmojë DPT në mbrojtjen e aseteve të informacionit. Anëtarët janë përgjegjës për:

- monitorimin dhe garantimin e zbatimit të kësaj rregullore me qëllim ruajtjen e standardeve të sigurisë;
- përmirësimin e vazhdueshëm të kësaj rregullore;
- zhvillimin dhe kryerjen e një fushate të vazhdueshme për sigurinë, për ndërgjegjësim e punonjësve të DPT;
- sigurimin e trajnimit të vazhdueshëm të personelit të institucionit në lidhje me politikat dhe procedurat e sigurisë
- kryerjen dhe përmirësimin e vazhdueshëm (të paktën një herë në vit) të analizës së riskut;
- rishikimin e vazhdueshëm (sa herë kryhen ndryshime në legjislacion lidhur me politikat kombëtare të sigurisë së Informacionit, si dhe ndryshime në sisteme në rolet e tyre) të të drejtave të aksesimit të informacioneve, në bashkëpunim me Drejtorinë e Burimeve Njerëzore;
- rishikimin e vazhdueshëm (sa herë kryhen ndryshime në legjislacion lidhur me politikat kombëtare të sigurisë së Informacionit si dhe kur ka ndryshime të kontraktorëve) të

masave të sigurisë ndaj ofruesve të shërbimeve të jashtme, veçanërisht personelit që punon me kontratë në ambientet e DPT;

- rishikimin e rregullt (sa herë kryhen ndryshime në legjislacion lidhur me politikat kombëtare të sigurisë së Informacionit) të privilegjeve për aksesimin e sistemeve të kompjuterave;
- kontrollin për mbylljen e menjëhershme të llogarive të përdoruesve që japin dorëheqjen ose largohen nga puna për arsye të tjera,
- koordinimin e kontrolleve të sigurisë, përfshi këtu organizimin e rregullt të kontrolleve të jashtme;
- shqyrtimin e thyerjeve të sigurisë që raportohen apo dyshohen se kanë ndodhur;
- 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.

1.7 Politika dhe Procedura në funksion të Sigurisë së Informacionit

Departamenti i Teknologjisë dhe Informacionit përgatit politika dhe procedura, në zbatim të kësaj rregullore, për çështje të cilat janë të rëndësishme për ruajtjen e sigurisë së informacionit.

Nr.	Titulli
1.	Rregullorja e fjalëkalimeve
2	Rregullorja e përdorimit të Postës Elektronike
3	Rregullorja e përdorimit të përgjithshëm të pajisjeve TIK, pronësia dhe siguria
4	Rregullorja e kushteve të përdorimit të Pajisjeve dhe Sistemeve në Administratën Tatimore
5	Rregullore për lidhjen në distancë (*remote access*)

2. SIGURIA E INSTITUCIONIT DHE PËRGJEGJËSITË

2.1 Përgjegjësitë për sigurinë

Çdo përdorues/aksesues është përgjegjës për respektimin dhe për ruajtjen e nivelit të kërkuar të sigurisë gjatë kryerjes së detyrave. Ai vepron vazhdimisht në përputhje me këtë rregullore.

Në këtë rregullore, me përdorues/aksesues kuptojmë të gjithë ata persona të cilëve u lejohet aksesi në asetet e Drejtorisë së Përgjithshme të Tatimeve dhe në mënyrë të veçantë asetet e informacionit. Këtu përfshihen:

- punonjësit e DPT;

- kontraktorët e DPT, për sa është e nevojshme për të përmbushur detyrimet kontraktuese;

• nëpunësit e ofruesve të shërbimeve (*service providers*) e DPT, për sa është e nevojshme për të përmbushur detyrimet kontraktuese;

• konsulentët vetëm për informacionin teknik përkatës;

• palë të tjera me të drejtë aksesi;

Përpara ushtrimit të punës/shërbimit të fituar nga kontraktorët, Komiteti dhe drejtoria sipas fushës së përgjegjësisë i vendos në dispozicion dhe i bën me dije politikat e saj të sigurisë dhe Rregulloren për sigurinë e informacionit. Ndërkohë që trajnime mbi sigurinë e informacionit, organizohen për të gjithë punonjësit e DPT.

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 këtë rregullore, procedurat dhe standardet e publikuara për sigurinë e informacionit në DPT;

• 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 DPT (përfshi këtu kompjuterat, llogaritë e përdoruesve, çelësat dhe çdo gjë tjetër) të hiqen menjëherë, për çdo pjesëtar të personelit (i përhershëm ose me kontratë) që largohet nga DPT ose që kalon në një departament apo në një detyrë tjetër, duke siguruar një proces të rregullt dorëzimi detyre;

• 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, duke përdorur formularët e miratuar;

• 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, sipas Manualeve të punës për çdo Drejtori Specifike.

2.1 Aksesimi i të tretëve

Personat, të cilët nuk janë punonjës të DPT dhe institucionet (organizatat) të tjera, lejohen të aksesojnë asetet e informacionit të DPT vetëm në bazë të kushteve të përcaktuara në një marrëveshje zyrtare. 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 DPT, përfshirë këtu për aq sa është e mundur:

• rregulloren për sigurinë e informacionit të DPT;

• kufizimet në kopjimin dhe në shpërndarjen e informacionit;

• një përshkrim për sejcilin prej shërbimeve që do të ofrohet nga DPT;

• 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 DPT, si dhe të palëve të treta;

• metodat e lejuara të aksesimit dhe kontrolli i përdorimit të fjalëkalimit të përdoruesit;

• procesin e dhënies së të 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 kontraktuale;

• 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 DPT për administrimin e ndryshimeve mbi sistemet e informacionit;

• mbrojtjen nga programet keqdashëse;

• procedurat për raportimin, për njoftimin dhe për shqyrtimin e thyerjeve të sigurisë;

• detyrimin e palëve të treta për të kërkuar zbatimin e këtyre kushteve edhe nga nënkontraktorët e tyre.

3. KLASIFIKIMI DHE KONTROLLI i ASETEVE

3.1 Përgjegjësia për asetet

Të gjitha asetet kryesore për aktivitetin normal të DPT (programet; pajisjet kompjuterike përfshirë dhe tabletët; shërbimet, përfshirë: shërbimet kompjuterike/të komunikimit dhe shërbimet e përgjithshme; të gjitha asetet e tjera të informacionit, përfshirë: bazën e të dhënave dhe skedarët e të dhënave, kontratat dhe marrëveshjet, dokumentacionin e sistemeve, manualet e përdoruesve, materialin e trajnimeve, procedurat operative ose ndihmëse, planet e vazhdimësisë, dhe informacionin e arkivuar) përgatiten për çdo Drejtori nga Drejtori përkatës sipas formularit unik dhe përmblidhen nga Drejtoria e Administratës dhe Prokurimeve, në bashkëpunim me Drejtorinë TIK, për sa i përket programeve dhe Drejtoria e Financës dhe Buxhetit për asetet fizike. 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 "përgjegjësit" 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 i mbetet përgjegjësit të asetit. Për asetet në ngarkim sipas kartelës

personale janë përgjegjës personat/punonjësit që e kanë në ngarkim. Për asetet në nivel institucional caktohet një person përgjegjës nga Drejtoria e Administratës dhe Prokurimeve, që duhet të ushtrojë kontroll herë pas here.

3.2 Regjistri i aseteve të informacionit

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

• **asetet e informacionit**: bazat e të dhënave dhe skedarët e të dhënave, dokumentacionin e sistemeve, manualet e përdoruesit, materialet e trajnimit, procedurat operacionale, rregulloret, planet e vazhdueshmërisë së punës, rregullat dhe procedurat e rikuperimit të të dhënave të humbura, informacionin e arkivuar;

• **programet**: programet aplikative, programet e sistemit, mjetet për zhvillimin e mëtejshëm të tyre dhe mjetet ndihmëse;

• **asetet fizike**: pajisjet kompjuterike, pajisjet e komunikimit, shiritat magnetikë, pajisje të tjera teknike (për shembull. kabllot e energjisë elektrike, pajisjet e ajrit të kondicionuar), mobiljet;

• shërbimet: shërbimet kompjuterike, shërbimet e komunikimit dhe utilitetet e përgjithshme.

Për çdo aset në regjistër mbahet:

• përshkrimi i tij

• përgjegjësi i tij

• niveli i rëndësisë: përcakton rëndësinë e aseteve të informacionit për DPT, në bazë të periudhës kohore maksimale gjatë të cilës DPT 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), në rastet kur lejohet;

• krijimi, mirëmbajtja dhe mbrojtja e regjistrit të aseteve të informacionit është përgjegjësi e Drejtorisë së Administratës dhe Prokurimeve, me kontributin e Drejtorisë TIK për sa i përket infrastrukturës IT, e cila konsultohet me përgjegjësit e aseteve. Regjistri duhet të rishikohet të paktën një herë në gjashtë muaj.

3.3 Klasifikimi i Informacionit

I gjithë Informacioni shkresor i trajtuar në DPT klasifikohet bazuar në parashikimet e ligjit nr. 8457, datë 11.02.1999 "Për informacionin e klasifikuar "sekret shtetëror", si dhe VKM nr. 189, datë 04.03.2015 "Për Sigurimin Fizik të Informacionit të Klasifikuar "Sekret Shtetëror", të NATO-s, BE-së, Shteteve dhe Organizatave të Tjera Ndërkombëtare". Bazuar në ligjin nr. 8457, informacioni klasifikohet si:

1. Tepër sekret

2. Sekret

3. Konfidencial

4. I kufizuar

Zyra e Protokollit është përgjegjëse për klasifikimin e shkresave hyrëse dhe për shpërndarjen e dokumentacionit të klasifikuar (konfidencial, sekret, etj.) sipas procedurave përkatëse.

3.4 Analiza e riskut

Regjistri i riskut bazohet në ligjin nr.10.296 datë 8.7.2020, i ndryshuar, Udhëzimin nr.7 datë 28.2.2018, si dhe Udhëzimin nr.21 datë 25.10.2016.
Komiteti dhe Nëpunësi Zbatues i institucionit kryejnë një analizë vjetore zyrtare të riskut për asetet e informacionit të DPT sipas procedurave që rekomandohen në standardet ndërkombëtare. Rezultatet e analizës së riskut do të përdoren për të përcaktuar strategjitë për zbutjen e çdo risku që identifikohet. Nga çdo drejtori do të rishikohet risku nëse risqet janë përshkallëzuar në nivele më të larta të menaxhimit dhe vendimet për risqet përdoren për të përmirësuar proceset operative dhe të sigurisë. Në momentin kur kemi një risk të ri potencial, së pari do të trajtohet tek plani operacional i cili ka frekuencë zbatueshmërie 1 herë në 3-muaj. Nëse risku do të vijojë pa gjetur zgjidhje dhe kthehet në risk potencial atëherë identifikohet tek regjistri i riskut i vitit që vjen, duke nxjerr në pah një risk të ri, i cili ndikon sipas peshës që ka në performancë.

Analiza e riskut të sigurisë së informacionit kryhet duke marrë parasysh **kërcënimet**, **dobësitë** dhe **impaktin**.

Për të kryer analizën e riskut të sigurisë së informacionit, ndiqen hapat si më poshtë:

- Identifikimi i aseteve

a) Dobësitë
b) Kërcënimet
c) Kontrollet

- Vlerësimi – sipas nivelit të riskut (Ulët, Mesëm, Lartë)
- Trajtimi:

a) Rregullimi (Implementimi i një kontrolli që pothuajse ose plotësisht i përgjigjet riskut themelor)
b) Zbutja e riskut (*mitigation*)
c) Transferimi i riskut
d) Pranimi i riskut në rastet kur risku është shumë i ulët dhe mund të pranohet
e) Shmangia e riskut

- Komunikimi brenda organizatës
- Monitorimi i vazhdueshëm

<u>Zotëruesi dhe përgjegjësia e procesit të analizës së riskut</u>

- Zotëruesit e procesit : Nëpunësi Zbatues i Institucionit dhe Komiteti
- Zotëruesit e riskut (Drejtori i Drejtorisë)

3.5 Administrimi i dokumenteve

Për të gjitha dokumentet ndiqet Procedura e Administrimit të Dokumenteve. Funksionimi dhe menaxhimi i ciklit të lëvizjes së dokumentacionit bazohet në Ligjin Nr. 9154 datë 06.11.2003 "Për arkivat", si dhe "Normat tekniko-profesionale dhe metodologjike të shërbimit arkivor në Republikën e Shqipërisë", dhe përcaktohet gjithashtu në nenin 44 dhe 45, të Rregullores së Brendshme "Për funksionimin e Administratës Tatimore Qëndrore". Për rëndësinë e zyrës që administrojnë punonjëset e protokollit dhe korrieri duhet të jenë të pajisur me certifikatë DSIK.

3.6. Procedurat e Arkivimit të Dokumenteve.

Kriteret dhe procedurat që ndiqen për arkivat e institucionit.
Arkiva e DPT funksionon dhe menaxhohet në respektim të ligjit nr.9154, datë 6.11.2003 "Për arkivat", VKM nr. 360, datë 26.04.2017 (germa b, pika 5) për "Organizimin dhe funksionimin e Drejtorisë së Përgjithshme të Arkivave" dhe në "Normat tekniko-profesionale dhe metodologjike të Shërbimit Arkivor në Republikën e Shqipërisë", si dhe në Vendimin nr.4 datë 19.06.2017, të Këshillit të Lartë të Arkivave për "Miratimin e Rregullores së Njehsuar të Punës me Dokumentet në Autoritet Publike të Republikës së Shqipërisë", (neni 5,6,8 pika m, neni 9).
Arkiva DPT është e vendosur në një ambient të veçantë, e siguruar me derë të përforcuar me hekur.
Dokumentet janë të sistemuara në kuti arkive dhe këto të fundit janë të vendosura në rafte metalike.

4. SIGURIA E PERSONELIT

4.1 Manualet e vendeve të punës dhe marrëdhënia e punësimit

Çdo punonjës ka përgjegjësitë e tij në lidhje me sigurinë, pas njohjes me rregullat e përgjithshme të institucionit në fushën e sigurisë së informacionit. Përgjegjësia për sigurinë përcaktohet që në fazën e marrjes në punë, ku çdo punonjës i Administratës Tatimore nënshkruan një dokument që quhet "Deklarata e Sigurisë dhe Konfidencialitetit". Në fazën e marrjes në punë në strukturat e Administratës Tatimore, nëpunësit/punonjësit kanë detyrimin të njohin Ligjin nr. 9920 datë 19.05.2008, "Për Procedurat Tatimore në Republikën e Shqipërisë" i ndryshuar.

Pas marrjes në punë nëpunësit/punonjësit njihen me detyrat dhe detyrimet gjatë ushtrimit të funksionit, të përcaktuara në Rregulloren e Brendshme të Administratës Tatimore Qendrore, të miratuar dhe Kodin e Etikës për punonjësit e Administratës Tatimore Qendrore, në të cilën përcaktohen qartë dhe parimet e Ruajtjes së Informacionit dhe Konfidencialitetit.

Në zbatim të Ligjit nr. 9367, datë 07.04.2005, "Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike", i ndryshuar, si dhe Rregullores së Brendshme nr.4 datë 21.01.2020, "Për parandalimin e Konfliktit të Interesave në Drejtorinë e Përgjithshme të Tatimeve", punonjësit e rinj plotësojnë autorizimin dhe deklaratën personale të konfliktit të interesit për personat e lidhur të cilët ushtrojnë aktivitet privat.

Plotësimi i formularit për konfliktin e interesit bëhet nga ana e gjithë punonjësve të emëruar rishtazi apo punonjës të cilët kanë pasur ndryshime nga deklarimi i mëparshëm.

Deklarata nënshkruhet pas njohjes të punonjësit me Rregulloren e Sigurisë së Informacionit, por jo më vonë se 15 ditë nga fillimi i marrëdhënieve financiare të tij me institucionin.

Detyrat specifike dhe mënyra e ushtrimit të tyre është pjesë e manualeve të punës së çdo strukture, rregullores së brendshme, formularëve të përshkrimit të punës dhe në çdo rast çdo dispozite ligjore në fuqi të përcaktuara në ligje të posaçme.

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.

Në çdo manual përcaktohet mënyra e dorëzimit të detyrës në rast largimi apo transferimi të punonjësit.

Në çdo rast përgjegjës për mbikëqyrjen dhe saktësinë e këtij procesi është eprori në linjë hierarkike, sipas radhës.

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 rastin kur punonjësi këto dokumente i depoziton për shqyrtim nga Institucioni, përveç rasteve që procedurat e rekrutimit menaxhohen nga Departamenti i Administratës Publike.

Në të gjitha kontratat e punës gjendet si pjesë përbërëse e saj, përveç përshkrimit të punës edhe deklarata ku punonjësit e rinj duhet të pranojnë me shkrim, që janë dakord me kërkesat e DPT mbi konfidencialitetin dhe sigurinë e informacionit.

Pas pranimit në punë dhe lidhjes së kontratës/zbatimit të akt-emërimit, punonjësit detyrohet të plotësojnë dosjen e tyre personale, për vërtetësinë e dokumentacionit të gjendur në të, mbajnë përgjegjësi personale dhe ligjore.

Pas largimit nga puna, zbatohen detyrimet e dorëzimit të detyrës, sipas legjislacionit në fuqi apo/dhe manualeve të punës, nëse ka procedura specifike të detajuara. Përgjegjësia për dorëzimin e detyrës i përket punonjësit që largohet dhe saktësia e procesit mbikëqyret nga eprori sipas shkallës hierarkike. Detyrohet çdo punonjës të ruajë konfidencialitetin e të dhënave të disponuara dhe njoftuara gjatë ushtrimit të detyrës publike.

PËRGJEGJËSIA E DREJTORËVE TË 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 përkatëse u është dhënë niveli i duhur i aksesimit ose jo në pajisjet dhe në sistemet e DPT, 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 drejtës së aksesimit në sistemet kompjuterike të DPT (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, para se të kryhen veprimet nga njësia *helpdesk*.

Çdo pjesëtari të ri, i cili i bashkohet personelit të DPT, 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 TIK (TI *helpdesk*);
- njohjen me këtë Rregullore 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 DPT.

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 drejtorie/sektori të sigurojë, që kur një pjesëtar i personelit pezullohet ose largohet nga puna, t'i hiqen të gjitha të drejtat e aksesimit dhe t'i kërkohet të dorëzojë të gjitha kartat e aksesimit, çelësat, shënimet, kompjuterat 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 DPT, duhet të bëhen para se pjesëtari i stafit të largohet fizikisht nga ambienti i punës. Është përgjegjësi e drejtorit të drejtorisë përkatëse, të sigurojë që kjo gjë të kryhet sa më parë.

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 korrektimin e të drejtave do të përfshijnë:

- Formularin për mbyllje të aksesit në sisteme

- Formularin për mbylljen e postes Elektronike në të cilën llogaria e tij e postës elektronike kalon në statusin *disable* për një periudhe 3 mujore dhe pas kësaj periudhe fshihet mailbox.
- një formë të kërkesës së mbylljes së kartës së aksesit në ambientet e DPT (për këtë nuk ka një formular specifik)

Është përgjegjësi e drejtorit të departamentit përkatës të kërkojë nivelin e duhur të korrektimit.

4.2 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, përfshirë këtu pamjaftueshmërinë, largimin dhe lëvizjet e planifikuara të personelit.

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

4.3 Trajnimi

Të gjithë punonjësit e rekrutuar rishtazi në Administratën Tatimore në bashkëpunim me QTATD dhe ASPA i nënshtrohen ciklit të trajnimeve për përfitimin e njohurive bazë për legjislacionin tatimor në tërësi si dhe për tema specifike të cilat trajtojnë parimet kryesore si: ruajtja e informacionit dhe konfidencialiteti, e drejta informimit dhe mbrojtja e të dhënave personale;

Punonjës/Nëpunës të Administratës Tatimore të cilët janë të pajisur me certifikatë sigurie për shkak të pozicionit të punës, i nënshtrohen trajnimeve për çështje të sigurisë së informacionit të klasifikuar, pranë Institucioneve të veçanta si DSIK, ILDKPKI,.

Personat që kanë akses në asetet e informacionit të DPT janë të detyruar të jenë të vetëdijshëm për rregullat dhe standardet e sigurisë në DPT, i gjithë personeli duhet të marrë trajnimin e nevojshëm për rregullat dhe për procedurat organizative dhe të sigurisë. Nevojat për trajnim përcaktohen menjëherë nga Drejtori i Drejtorisë, i cili ja përcjell zyrtarisht kërkesën Drejtorisë së Burimeve Njerëzore. 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 DPT;
- 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 TIK përgjigjet për zhvillimin dhe për shpërndarjen e materialeve të trajnimit.

Për çdo punonjës në periudhë prove, përcaktohet një punonjës mbikëqyrës i tij, gjatë ushtrimit të detyrave funksionale i cili raporton në vijueshmëri dhe jep opinion në fund të periudhës së provës. Kryesisht ky punonjës mbikëqyrës, është nëpunësi më i vjetër i strukturës ku është emëruar punonjësi.

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

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 TË SIGURISË

Për të gjitha rastet e ngjarjeve që lidhen me sigurinë ndiqet një procedurë formale për raportimin e incidenteve. Të gjitha ngjarjet e dyshuara duhet të raportohen menjëherë nga Drejtori i Drejtorisë ku ndodh incidenti tek Komiteti, duke plotësuar formularin sipas Aneksit 1. Më pas Komiteti trajton këtë informacion duke marrë masat paraprake të nevojshme dhe duke njoftuar strukturat eprore dhe Titullarin e Institucionit.

Në rast incidentesh mbi sigurinë e të dhënave të marra nga shkëmbimi i informacionit me një Autoritet të huaj Tatimor, njoftohet menjëherë edhe ky i fundit mbi incidentin e ndodhur dhe masat përkatëse të ndërmarra.

Drejtori i Drejtorisë ku ndodh thyerja e sigurisë, duhet të raportojë të dhënat e mëposhtme:

- Emrin dhe të dhënat e personit që raportoi incidentin
- Tipin e të dhënave apo informacionit që është kompromentuar
- Dëmet apo riskun që shkakton incidenti
- Vendndodhjen e incidentit
- Numrin e inventarit të pajisjeve të prekura nga incidenti
- Datën dhe orën kur ka ndodhur incidenti
- Vendndodhjen e të dhënave apo pajisjes që ka pësuar dëmin/incidentin.
- Tipin dhe rrethanat e incidentit.

Komiteti duhet gjithashtu të jetë i mirë-informuar për ngjarjen në mënyrë që reagimi të jetë i duhur. Njëkohësisht të gjitha veprimet që kryhen pas incidentit duhet të ruhen dhe të pasqyrohen në raportin e analizës së vlerësimit të riskut.

Të gjithë punonjësit duhet të njohin dhe zbatojnë këtë rregullore. Përveç kësaj, ata inkurajohen për të raportuar çdo dobësi të sigurisë ose çdo kërcënim të vënë re në procedura, në sisteme dhe në shërbime.

Nëse ndonjëri nga punonjësit shkel politikat e sigurisë të përcaktuara në këtë rregullore, atëherë ndaj tij merren masa disiplinore të përcaktuara në ligjin nr. 153/2013 "Për nëpunësin civil", i ndryshuar.

Të gjithë përdoruesit/aksesuesit, të cilët shkaktojnë dëm ekonomik, përgjigjen sipas dispozitave të Kodit Civil të Republikës së Shqipërisë

RAPORTIMI I KEQFUNKSIONIMIT TË PROGRAMIT TEK DREJTORIA TIK

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 Drejtorisë TIK, 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 Komiteti gjykon se veprimtaria e një punonjësi nuk është në përputhje me rregullat dhe procedurat e sigurisë, për çfarëdolloj arsyeje. Komiteti organizon 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.

Në rast të pretendimit apo konstatimit të një shkelje disiplinore përsa i përket shkeljes së rregullave për ruajtjen e informacionit të klasifikuar, apo çështje të sigurisë dhe konfidencialitetit, ndaj nëpunësit përgjegjës Komisioni i Disiplinës fillon procedimin disiplinor sipas Ligjit nr. 152/2013 "Për nëpunësin Civil", i ndryshuar, neni 57 e në vijim dhe VKM nr. 115, datë 05.03.2014 "Për Përcaktimin e Procedurës Disiplinore dhe të Rregullave për Krijimin, përbërjen e Vendimmarrjen në Komisionin Disiplinor në Shërbimin Civil".

Për punonjësit të cilët trajtohen sipas dispozitave të Kodit të Punës, në rast të pretendimit apo konstatimit të një shkelje disiplinore, përsa i përket shkeljes së rregullave për ruajtjen e informacionit të klasifikuar, apo çështje të sigurisë, konfidencialitetit ndaj nëpunësit përgjegjës fillon procedimi disiplinor, sipas dispozitave të Kodit të Punës dhe Urdhrit nr. 10, datë 31.01.2020 Për miratimin e Rregullores "Për marrëdhëniet e punës të personelit jo nëpunës civil, në Administratën Tatimore Qendrore".

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. 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 përkatëse sipas ligjit.

4.7 Ndarja e përgjegjësive

Për të minimizuar mundësinë e mashtrimit ose të keqpërdorimit 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 dhe tek drejtuesi i strukturës.

5. SIGURIA FIZIKE DHE E MJEDISEVE

SIGURIA FIZIKE

Shpjegime për sigurinë fizike

Bazuar në VKM nr. 189, datë 04.03.2015 "Për Sigurimin Fizik të Informacionit të Klasifikuar "Sekret Shtetëror", të NATO-s, BE-së, Shteteve dhe Organizatave të tjera Ndërkombëtare", ambientet e DPT janë të ndara në 3 zona sigurie:

1. Klasi i parë;

2. Klasi i dytë;

3. Klasi administrativ.

Funksionimi i sigurisë fizike të objektit realizohet nëpërmjet shërbimit të ruajtjes fizike në respektim të akteve ligjore në fuqi.

Ky shërbim konsiston në këto element:

1. Perimetri i jashtëm i sigurisë se objektit, ky perimetër monitorohet nëpërmjet kamerave që rrethojnë objektin.
2. Sistem i ruajtjes me persona fizik 24 orë për 7 ditë të javës.
3. Monitorim 24 orë i sistemit të kamerave në zyrën qendrore të shoqërisë.
4. Kamera të jashtme të lidhura me sistem alarmi.

Institucioni ka në funksion zyrë informacioni.

Në institucion janë të instaluara fikse zjarri.

Dera hyrëse në institucion është e pajisur me sistem *chekimi* me kartë që monitorohet nga Drejtoria TIK.

Ne brendësi të institucionit është i instaluar sistemi i kamerave të brendshme i cili monitorohet nga Drejtoria TIK.

Dritaret e kateve në bodrum janë të pajisura me kangjella.

5.1 Siguria e ambienteve (ndërtesave)

Aksesimi i të gjitha ambienteve të sistemeve të informacionit në DPT 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.

Siguria fizike duhet të fillojë me vetë ndërtimin dhe duhet të kryhet një vlerësim i cënueshmërisë së sistemit. Ndërtimi duhet të ketë mekanizma të duhura kontrolli për llojin e informacionit dhe pajisjen që ruhet. Kjo mund të përfshijë, por nuk kufizohet si më poshtë:

• Alarme të vendosura dhe aktivizuara jashtë orëve të punës.

• Kangjella për dritaret në kate të ulëta.

• Mekanizma të kontrollit të aksesit të vendosura në të gjitha dyert e aksesueshme (aty ku përdoren kode duhet të ndryshohen rregullisht dhe duhet t'u tregohen njerëzve të autorizuar për të hyrë në ndërtesë apo në zonë).

• Kamera CCTV.

• Zona e recepsionit.

• Mbrojtje ndaj dëmtimit – p.sh. zjarr, përmbytje, vandalizëm.

Vëmendje e veçantë do t'i kushtohet qëndrave të të dhënave dhe dhomave të pajisjeve të telekomunikacionit.

ZONAT BAZË TË SIGURISË

Çdo ndërtesë apo zyrë brenda DPT-së që nuk janë zakonisht të hapura për publikun konsiderohen si minimum zona bazë të sigurisë.

Të gjitha ndërtesat dhe zyrat brenda DPT-së konsiderohen ndonjëherë si minimum zona bazë të sigurisë, kur nuk janë të hapura për publikun.

Brenda zonave bazë të sigurisë:

• Çdo departament duhet të sigurojë që dyert dhe dritaret janë mbyllur mirë.

• Mjetet/lejëkalimet e identifikimit dhe aksesit (p.sh. kartat, çelësat, kodet e hyrjes etj.) duhet të ruhen nga punonjës të autorizuar për të aksesuar ato zona dhe nuk duhet t'i jepen askujt tjetër.

KARTAT E AKSESIMIT

Të gjitha ambientet kritike sigurohen me sisteme aksesimi dhe karta elektronike, çdo punonjës i autorizuar për një ambient specifik pajiset me një kartë individuale aksesi. Drejtoria e Burimeve Njerëzore në bashkëpunim me Drejtorinë TIK, janë përgjegjëse 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 DPT nuk duhet t'u lejohet lëvizja e lirë, e pakontrolluar në ambientet kritike. Identitet i vizitorëve të 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 DPT. 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 TIK, 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. Të gjitha pajisjet e përgjithshme kompjuterike duhet të vendosen në vendndodhje të përshtatshme fizike që:

• Të kufizojnë rreziqet mjedisore – p.sh. ngrohjen, zjarrin, tymin, ujin, pluhurin dhe dridhjen.

• Të kufizojnë rrezikun e vjedhjes – p.sh. nëse është e nevojshme sende të tilla si laptopët duhet të jenë fizikisht në tavolinë.

• Të lejojnë kompjuterët që janë të pozicionuar në atë mënyrë që të trajtojnë të dhëna të ndjeshme në mënyrë që të eliminojnë rrezikun që të dhënat të shihen nga njerëz të paautorizuar.

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 me karte aksesi dhe mundësinë qe loget e secilit akses të ruhen.

Të gjitha aksesimet në dhomat e të kompjuterave 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 DPT 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 trajnuar dhe i autorizuar nga Drejtori i Drejtorisë TIK.

NXJERRJA JASHTË GODINAVE

Ky seksion zbatohet për kompjuterat personalë apo çdo formë tjetër mjetesh që mbajnë ose që përpunojnë informacione. Të gjitha pajisjet e DPT, 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 godinës së DPT. 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 DPT, 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.

Për procedurën e asgjësimit të aktiveve në magazinat e DPT. (kompjutera +printera)

Ky proces kryhet në respektim të ligjit Nr. 10296 , datë 08.07.2014 "Për menaxhimin financiar dhe kontrollin", Udhëzimit të Ministrisë të Financave Nr. 30 , date 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik" kreu IV pika 107 deri 120 si dhe bazuar në VKM Nr. 957 , datë 19.12.2012 "Për mbetjet për pajisjet elektrike dhe elektronike"

Çdo vit kalendarik me urdhër të Drejtorit të Përgjithshëm ngrihet komisioni i inventarizimit të vlerave materiale për punonjësit dhe për magazinën e DPT-së. Ky komision në inventarizimin që i bën mallit të magazinës bënë dhe një vlerësim paraprak për gjendjen fizike të artikujve. Pas përfundimit të punës së këtij komisioni ngrihet komisioni i vlerësimit të aktiveve. Ky komision miratohet nga titullari i institucionit dhe ka në përbërje të tij specialistë të fushës. Në respektim të neneve 95-101 të Udhëzimit Nr. 30 të Ministrit të Financave bën vlerësimin e aktiveve dhe evidenton aktivet për jashtë përdorimi. Në përfundim të procedurës informohet titullari i institucionit.
Në respektim të VKM-së Nr.957, datë 19.12.2017, asetet kompjuterike të evidentuara nga komisioni i vlerësimit kalojnë në një procedurë ankandi. Për të gjitha këto procedura në fund informohet titullari i institucionit.

5.3 Siguria e aseteve

Çdo përdorues/aksesues 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 të 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 dhe sipas parashikimeve të ligjit nr. 8457, datë 11.02.1999, "Për informacion e klasifikuar "Sekret Shtetëror". Në zbatim të këtij ligji në DPT janë ngritur Urdhri nr. 10 datë 26.02.2019 "Për caktimin e strukturës së sigurisë" dhe Urdhri nr. 9 datë 26.02.2019 "Për ndarjen e zonave të sigurisë në Drejtorinë e Përgjithshme të Tatimeve".

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 DPT. Këtu përfshihen edhe pajisjet që nxirren jashtë DPT për t'u riparuar. Tape-t magnetikë të nxjerrë përfundimisht jashtë DPT duhet të shkatërrohen dhe të digjen.

HEDHJA OSE RIPËRDORIMI I SIGURTË I PAJISJEVE

Kur një kompjuter ose pajisje portabël duhet të ripërdoret jashtë personelit të cilit i ishte caktuar në fillim, të gjitha të dhënat në pajisje duhet të fshihen në mënyrë të sigurtë përpara se të ripërdoret.

Kur një kompjuter ose pajisje portabël ka arritur në fund të ciklit të përdorimit të tij, të gjitha të dhënat në pajisje do të fshihen në mënyrë të sigurtë dhe më pas të hidhen në një mënyrë miqësore për mjedisin.

Kur hedhja lidhet me një pajisje portabël, duhet t'i referohemi Politikës së Pajisjeve Portabël.

Kur pajisja i jepet një organizate tjetër (p.sh. kthehet në bazë të një marrëveshjeje *leasing*) do të kryhet heqja në mënyrë e sigurtë e të dhënave përpara transferimit të pajisjeve.

Praktikat e fshirjes së sigurtë të të dhënave do t'i nënshtrohen verifikimit periodik nga një palë e tretë e pavarur.

Për këtë procedurë mirëmbahet një procesverbal për të gjithë materialin që është ruajtur dhe gjithçka që është shkatërruar.

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 të 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 TË INFORMACIONIT

6.1 Procedurat e operimit

APLIKIMET

Përgjegjësitë dhe procedurat e administrimit 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 TIK.

OPERACIONET E TEKNOLOGJISË SË INFORMACIONIT

Të gjitha procedurat që lidhen me teknologjinë e informacionit dokumentohen. Këto përfshijnë në mënyrë të veçantë: procedurat e hapjes dhe të mbylljes së llogarive në sisteme apo pajisje, *backup*-et dhe mirëmbajtjen rutinë për të gjitha elementet e mjedisit të teknologjisë së informacionit të DPT. 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 afruesve të jashtëm të shërbimeve ose të partnerëve në biznes (*business partner*), sulmet keqdashëse dhe thyerjet e konfidencialitetit.

KONTRAKTORËT E BURIMEVE TË JASHTME

Dokumentit me politikat e sigurisë së DPT 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 DPT.

6.2 Kontrolli i ndryshimeve

Të gjitha ndryshimet në pajisjet dhe në sistemet që përpunojnë informacionin, i nënshtrohen procedurave zyrtare të administrimit të ndryshimeve.

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 DPT instalohet dhe vihet në funksionim një program i licensuar antivirus ose protokolle të tjera për manaxhimin e

viruseve, *malware* etj. Ai duhet të përditësohet automatikisht, në mënyrë të vazhdueshme, nën kontrollin e punonjësve të teknologjisë së informacionit. Çinstalimi ose çaktivizimi i programeve antivirus trajtohet si shkelje serioze.

6.4 *Backup* i të dhënave

BAZAT E TË DHËNAVE TË DPT

Drejtoria TIK është përgjegjës për të siguruar që të gjitha të dhënat sensitive të mbajtura në serverat e DPT t'u bëhet *backup* (kopje) i rregullt në përputhje me procedurat e përcaktuara, për çdo sistem (përfshi këtu edhe *file/print servers*). Kopjet 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 DPT, për të gjithë përdoruesit e brendshëm e të jashtëm.

6.6 Politika e përdorimit të Internetit dhe të Postës Elektronike

I gjithë personeli i DPT (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.

7. KONTROLLI I AKSESIT

Për çdo burim informacioni të DPT, 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/aksesues identifikohet në mënyrë individuale nëpërmjet një llogarie unike përdoruesi, e cila do të caktohet vetëm nëpërmjet një autorizimi me shkrim i cili miratohet nga Drejtori i Drejtorisë TIK. 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 përcaktimin e përgjegjësisë 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 aktivitetin e tyre. Në të gjitha rastet, ndiqen procedura të dokumentuara për:

• regjistrimin e përdoruesve të rinj;

• ndryshimin e statusit për një përdorues ekzistues (për shembull ndërprerjen e llogarisë së përdoruesit kur ai largohet nga puna ose ndryshimin e privilegjeve të aksesit të tij);

• mbylljen përfundimtare të një llogarie përdoruesi (mbyllja përfundimtare nuk fshin historikun e logeve të këtij përdoruesi.

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

7.1. Përdoruesit e brendshëm

Përdoruesit e brendshëm përfshijnë punonjësit e DPT, kontraktorët, dhe nënkontraktorët e shërbimeve të DPT. Aksesi për përdoruesit e brendshëm në sistemet e DPT 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. Për përdoruesit si Kontraktorët dhe nënkontraktorët e shërbimeve të DPT nënshkruhet një marrëveshje konfidencialiteti dhe mos-zbulimi, si pjesë e kushteve të tyre fillestare të angazhimit.

LLOGARITË E PËRDORUESVE

Llogaritë e përdoruesve krijohen dhe administrohen nga punonjësit e Drejtorisë TIK. Ata përdoren për aksesimin e të gjitha shërbimeve të teknologjisë së informacionit të DPT, përfshi këtu rrjetin e brendshëm, adresën elektronike, pajisjet dhe sistemet e DPT. Modifikimi ose heqja e një llogarie bëhet me anë të një kërkesë zyrtare nga DBNJ, nëpërmjet plotësimit të një formulari të miratuar për këtë qëllim nga drejtorët e drejtorive. Kjo kërkesë mund të bëhet edhe nga drejtori i drejtorisë nën përgjegjësinë e të cilit është përdoruesi, por do aprovohet nga DBNJ dhe miratohet nga Drejtori TIK. Procedura për administrimin e llogarive të përdoruesve të DPT dokumentohet sipas një rregullore të veçantë. Kjo procedurë zbatohet në të gjitha rastet kur:

• nevojitet një llogari e re (për shembull për një punonjës të ri);

• llogaria e një punonjësi duhet të pezullohet për një periudhë kohe ose kur duhet të riaktivizohet mbas pezullimit në rastin e politikave të sigurisë se postes elektronike;

• do të ndryshohen privilegjet e aksesimit (për shembull kur kalohet në një rol me përgjegjësi më të madhe);

• nevojitet mbyllja e një llogari kur një nëpunës, pjesëtar i personelit të DPT, largohet nga puna (fshirja e përhershme e llogarisë).

ADMINISTRIMI I FJALËKALIMEVE

Të gjithë përdoruesit e DPT instruktohen në lidhje me mënyrat e administrimit të fjalëkalimeve. 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 (e-mail).

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 DPT.

MONITORIMI I PROFILEVE TË PËRDORUESVE

Është e rëndësishme të garantohet që:

• vetëm përdoruesve të duhur u është lejuar akses në sistemet e DPT (janë eliminuar të gjitha llogaritë të përdoruesve që janë larguar ose kanë ndryshuar pozicion dhe të drejtat);

• 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 Drejtoria TIK.

7.2. 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 DPT.

LLOGARITË E PËRDORUESVE

Caktimi i llogarive të përdoruesve është përgjegjësi e drejtorive përkatëse të DPT. Përdoruesit e jashtëm instruktohen që të ruajnë konfidencialitetin e llogarisë së tyre, gjatë procesit të trajnimit 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 DPT. 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 TIK.

AUTENTIFIKIMI

Të gjithë përdoruesit e jashtëm, para se t'u jepet akses në sistemet e informacionit të DPT, 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.

Sistemi i AT është i ekspozuar vetëm në rrjetin *Goverment Gateway* që është një rrjeti i sigurt dhe vetëm për institucionet qeveritare. Forma e autentifikimit është e njëjtë me përdoruesit e brendshëm nëpërmjet *username* dhe *password.*

MONITORIMI i PROFILEVE TË PËRDORUESVE

Është e rëndësishme të garantohet që:

• vetëm përdoruesve të duhur u është lejuar akses në sistemet e DPT (janë eliminuar të gjitha llogaritë fiktive);

• 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 Drejtoria TIK.

MARRËVESHJET ME KONTRATË

Kërkesat e sigurisë përfshihen në të gjitha kontratat ndërmjet DPT dhe përdoruesve të jashtëm për të administruar aksesin e tyre direkt (online) në sistemet e DPT. 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 DPT, në të gjithë kompjuterat që mund të lidhen me sistemet e DPT, 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 DPT.

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 privilegjet e përdoruesve vendos dhe të firmos drejtori i drejtorisë përgjegjëse të sistemit, duke marrë në konsideratë mendimin e specialistëve të Drejtorisë TIK. 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 TIK.

ENKRIPTIMI

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

8. ZHVILLIMI DHE MIRËMBAJTJA E SISTEMEVE

8.1. 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 TIK, përpara fillimit të punës për zhvillimin e aplikimit. Masat e sigurisë përcaktohen qartë në dokumentacionin e programeve/aplikimeve, përfshi këtu procedurat operacionale.

8.2. 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 DPT.

MJEDISI i ZHVILLIMIT

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

MJEDISI i TESTIMIT

Mjedisi i Testimit është nën kontrollin e Drejtorisë TIK. Të gjitha profilet e sigurisë dhe lejet e aksesimit përcaktohen dhe jepen me miratimin e Drejtorisë TIK. 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:

1. Zhvilluesit (krijuesit) përgjegjës të shkruajnë një dokumentacion të plotë, që mbulon instalimin, testimin dhe funksionimin e programit të ri;
2. Drejtoria TIK duhet të përcaktojë se kush do ta instalojë, do ta testojë dhe do ta ekzekutojë programin, në përputhje me dokumentacionin;
3. Në qoftë se konstatohet ndonjë problem ose gabim, ai do të dokumentohet nga Drejtoria TIK dhe do të kthehet për korrigjim;
4. Kjo procedurë të përsëritet sa herë që është e nevojshme derisa të dyja palët të jenë të kënaqura me rezultatet e testimit;
5. 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 Drejtoria TIK. Të gjitha profilet e sigurisë dhe lejet e aksesimit përcaktohen me miratimin e Drejtorisë TIK 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.

8.3. 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 pjesëtar 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 TIK.

• 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 TIK. 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 Drejtorisë TIK.

• 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.

9. MENAXHIMI i VAZHDUESHMËRISË SË AKTIVITETIT

Mbështetur në Rregulloren për rastet e emergjencave civile në DPT, është hartuar Manuali i procedurave të rasteve të emergjencës civile. Në këtë Rregullore është përcaktuar ngritja e një komisioni për Menaxhimin e Emergjencave Civile. Komisioni i ngritur në konsultim me drejtorët e të gjitha drejtorive zhvillon dhe përditëson plane për rikrijimin e të gjitha proceseve dhe shërbimeve kritike të aktivitetit, në rastet e ndërprerjeve serioze apo masive. Ndërprerje të tilla mund të shkaktohen nga shkaqe natyrore, nga aksidente, nga difekte të pajisjeve, nga veprime të qëllimshme ose nga difekte të shërbimeve. Ky dokument miratohet nga Komiteti Operacional i DPT.

9.1. 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 DPT. 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;
- Sigurimin e procedurave dhe burimeve që nevojiten për rikthimin në gjendjen normale;
- Identifikimin e palëve të treta të cilët duhen njoftuar në rast të një katastrofe;
- Edukimin e personelit në ekzekutimin e procedurave;
- Identifikimin e burimeve alternative për furnizime, burime dhe vendndodhje
- 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 DPT. Drejtorët e drejtorive janë përgjegjës për zbatimin e planeve të 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, për të siguruar disponueshmërinë e tij në çdo kohë.

9.2. 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 zëvendësimit të të dhënave të humbura dhe për planet e vazhdueshmërisë, është e departamenteve që janë pronarë të tyre.

9.3 Testimi

Plani i vazhdueshmërisë duhet të testohet në praktike me një periodicitet të caktuar të paktën një herë në vit. Rezultatet e testimit të fundit duhet të reflektohen në planin e vazhdueshmërisë dhe të përdoren për përmirësimin e këtij plani.

9.4. 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 fillestar dhe për të garantuar efektshmërinë e 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.

10. UDHËZIMET PËR STAFIN

Të gjithë punonjësit e DPT-së duhet t'i përmbahen udhëzimeve të mëposhtme:

10.1 UDHËZIME TË PËRGJITHSHME

a) Të vetmit persona të cilët mund të aksesojnë të dhënat e mbuluara nga kjo politikë duhet të jenë ata të cilëve u nevojiten për punë.
b) Të dhënat nuk duhet të shpërndahen në mënyrë jo zyrtare. Kur kërkohet hyrja në informacionet konfidenciale, punonjësit mund ta kërkojnë nga menaxherët e tyre drejtues.
c) DPT-ja do të trajnojë të gjithë punonjësit për t'i ndihmuar të kuptojnë përgjegjësitë e tyre kur trajtojnë të dhënat.
d) Punonjësit duhet t'i mbajnë të gjitha të dhënat e sigurta, duke marrë masa paraprake dhe duke ndjekur udhëzimet e mëposhtme.
e) Punonjësit duhet të sigurohen qe kompjuterat duhet të mbyllen plotësisht në fund të ditës së punës.
f) Në përfundim të procesit të punës, çdo punonjës i institucionit duhet të ketë tavolinën e pastër, në asnjë rast nuk duhet të ketë shkresa dhe dosje të hapura.
g) Në largimet e përkohshme nga vendi i punës nuk duhet lënë asnjë shënim, axhendë, bllok shënimesh ose tablet.
h) Punonjësit duhet të sigurohen që ekranët e kompjuterave të tyre të jenë të kyçur (*lock*) kur lihen të pambikqyrura.
i) Punonjësit duhet të sigurohen që mbyllin çdo pajisje kompjuterike portative, siç janë laptopët dhe tabletët.
j) Punonjësit duhet të sigurohen që çelësat e përdorur për të hyrë në informacion të kufizuar ose të sensitiv nuk duhet të lihen në një tavolinë të pa mbikëqyrur.
k) Duhet të përdoren fjalëkalime të sigurta dhe nuk duhet të shpërndahen.
l) Fjalëkalimet nuk mund të lihen në shënime ngjitëse të postuara nën një kompjuter dhe nuk mund të lihen të shkruara në një vend të arritshëm.

m) Printimet që përmbajnë informacion të kufizuar ose sensitiv duhet të hiqen menjëherë nga printeri.
n) Të dhënat personale nuk duhet t'i jepen personave të paautorizuar, si brenda administratës ashtu edhe jashtë saj.
o) Të dhënat duhet të rishikohen rregullisht dhe përditësohen nëse janë të vjetëruara.
p) Punonjësit duhet të kërkojnë ndihmë nga menaxherët drejtues ose nga punonjësi i mbrojtjes së të dhënave nëse nuk janë të sigurtë për ndonjë aspekt të mbrojtjes së të dhënave.

10.2 RUAJTJA E TË DHËNAVE

Këto rregulla përshkruajnë se si dhe ku mund të ruhen të dhënat në mënyrë të sigurtë. Pyetje mbi ruajtjen e sigurtë të të dhënave mund t'i bëhen menaxherëve të TIK ose kontrolluesve të të dhënave.

Kur të dhënat ruhen në letër, duhet të mbahen në një vend të sigurtë ku personat e paautorizuar nuk mund t'i shikojnë.

Këto udhëzime aplikohen edhe për të dhënat e ruajtura elektronikisht por që janë printuar për disa arsye:

a) Kur nuk kërkohet, letrat ose dosjet duhet të ruhen në një sirtar ose dollap të kyçur.
b) Punonjësit duhet të sigurohen që letrat ose shkresat e printuara nuk lihen në vende të dukshme për njerëzit e paautorizuar, si p.sh. në printer.
c) Të gjithë printerët dhe makinat e faksit duhet të pastrohen nga letrat sapo të shtypen; kjo ndihmon për të siguruar që dokumentet me përmbajtje sensitive/konfidenciale të mos lihen në printer për t'u kapur nga personi i gabuar.
d) Të dhënat e printuara duhet të grisen dhe hidhen në mënyrë të sigurtë kur nuk duhen më.
e) Pas shkatërrimit të Dokumenteve me përmbajtje sensitive/konfidenciale duhet të copëtohen në kosha dhe të vendosen në kosha adekuate për shkatërrimet konfidenciale.
f) Të dhënat e ruajtura elektronikisht, duhet të ruhen nga aksesi i paautorizuar, fshirja aksidentale dhe përpjekjet dashakeqe të piraterisë.
g) Të dhënat duhet të ruhen me fjalëkalime të sigurta të cilat ndërrohen rregullisht dhe nuk shpërndahen asnjëherë me punonjësit.
h) Nëse të dhënat ruhen në media të lëvizshme (si një CD ose DVD), duhet të mbahen të mbyllura në mënyrë të sigurtë kur nuk përdoren.
i) Të dhënat duhet të ruhen vetëm në *drive* dhe servera të caktuar dhe duhet të shkarkohen vetëm në një shërbim kompjuterik *cloud* të aprovuar.

j) Serverat që përmbajnë të dhëna personale duhet të vendosen në një vendndodhje të sigurt larg hapësirave të zyrës së përgjithshme.

k) Duhet të ruhen kopje të të dhënave. Këto kopje duhet të testohen rregullisht në përputhje me standardet e procedurave të backup-eve.

l) Të dhënat nuk duhet të ruhen menjëherë në laptop ose pajisje të tjera të lëvizshme si tabletat apo telefonat smart.

m) Të gjitha serverat dhe kompjuterat që përmbajnë të dhëna duhet të mbrohen nga *software* të sigurisë dhe *firewall* të aprovuar.

11. PËRPUTHJSHMËRIA ME LIGJIN

11.1. Kërkesat ligjore

LEGJISLACIONI

Të gjithë punonjësve u kërkohet të njohin kërkesat e legjislacionit dhe akteve nënligjore, në të cilat DPT mbështet veprimtarinë e saj, si dhe të sigurohen që veprojnë 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 DPT 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 DPT, për t'u përdorur në kompjuterat që nuk i përkasin DPT, për çfarëdo lloj qëllimi të ndryshëm nga aktivitetet e autorizuara, përbën thyerje të të drejtës së autorit dhe do të trajtohet si shkelje serioze.

11.2. Politika e Sigurisë

KONTROLLET

Të gjitha departamentet janë subjekt i një kontrolli zyrtar vjetor për të siguruar zbatimin e rregullave dhe standardeve të sigurisë. Përgjegjësit e aseteve të informacionit mbështesin rregullisht auditime për përputhjen e sistemeve të tyre me këtë rregullore. Të gjitha pajisjet kompjuterike kontrollohen nga Drejtoria TIK, për përputhshmërinë me standardet e

implementimit të sigurisë. Këto kontrolle përfshijnë ekzaminimin e sistemeve operacionale për t'u siguruar që kontrollet e sigurisë të pajisjeve dhe të programeve janë implementuar me korrektësi.

Kuadri Ligjor:

- Ligji nr.9920, datë 19.5.2008 "Për Procedurat Tatimore në Republikën e Shqipërisë, i ndryshuar",
- Ligji nr. 9154 datë 06.11.2003 "Për arkivat",
- Ligji nr. 8457, datë 11.02.1999 "Për informacionin e klasifikuar "sekret shtetëror",
- Ligji nr. 152/2013 "Për Nëpunësin Civil", i ndryshuar,
- Ligji nr. 9367, datë 07.04.2005 "Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike", i ndryshuar,
- Ligji nr. 10296 ,date 08.07.2014 "Për menaxhimin financiar dhe kontrollin" ,
- VKM nr. 189, datë 04.03.2015 "Për Sigurimin Fizik të Informacionit të Klasifikuar "Sekret Shtetëror",
- VKM nr. 360, datë 26.04.2017 "Për Organizimin dhe funksionimin e Drejtorisë së Përgjithshme të Arkivave" ,
- VKM Nr. 957, datë 19.12.2012 "Për mbetjet për pajisjet elektrike dhe elektronike",
- VKM nr. 115, datë 05.03.2014 "Për Përcaktimin e Procedurës Disiplinore dhe të Rregullave për Krijimin, përbërjen e Vendimmarrjen në Komisionin Disiplinor në Shërbimin Civil",
- Rregullorja e Brendshme nr.4 date 21.01.2020 "Për parandalimin e Konfliktit të Interesave në Drejtorinë e Përgjithshme të Tatimeve",
- Urdhri nr. 10, datë 31.01.2020 Për miratimin e Rregullores "Për marrëdhëniet e punës të personelit jo nëpunës civil, në Administratën Tatimore Qendrore",
- Udhëzimit të Ministrit të Financave nr. 30, datë 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik",
- Urdhri nr.38 datë 22.5.2020 "Për ndarjen e zonave të sigurisë në Drejtorinë e Përgjithshme të Tatimeve",
- Urdhri nr. 46 datë 3.7.2020 "Për caktimin e strukturës së sigurisë", në Drejtorinë e Përgjithshme të Tatimeve".

DREJTOR I PËRGJITHSHËM

Delina IBRAHIMAJ

Aneksi 1.

Raporti i Incidentit të Sigurisë

PJESA I -Përshkrimi i Incidentit

Tipi i incidentit			
Emri i personit që raportoi incidentin		**Tel.** **Email** **Departamenti/Sektori**	
Vendndodhja		**Data**	
		Ora	
Niveli i klasifikimit të informacioni i cenuar			
Lloji i informacionit të dëmtuar/cenuar			
Pajisja e dëmtuar			
Nr. i përdoruesve të cenuar		**Departamenti/Sektori i cenuar**	
Arsyet e ndodhjes së incidentit			
Hapat e ndërmarrë			
Risku i mbetur			