REPUBLIKA E SHQIPËRISË

ZYRA E INSPEKTORIT TË LARTË TË DREJTËSISË
DREJTORIA E PËRGJITHSHME E ÇËSHTJEVE DHE SHËRBIMEVE JURIDIKE

Nr. 4436 prot. Tiranë, më 22.12.2021

U R D H Ë R

Nr. 163, datë 22.12.2021

"PËR
MIRATIMIN E RREGULLORES MBI PARIMET DHE RREGULLAT E PËRGJITHSHME TË SIGURISË SË INFORMACIONIT NË ZYRËN E INSPEKTORIT TË LARTË TË DREJTËSISË"

Në mbështetje të nenit 147/d të Kushtetutës, në zbatim të neneve 204, pika 1, shkronja "c", 216, të ligjit nr. 115/2016 "Për organet e qeverisjes së sistemit të drejtësisë", i ndryshuar,

U R D H Ë R O J:

1. Miratimin e "Rregullores mbi parimet dhe rregullat e përgjithshme të sigurisë së informacionit në Zyrën e Inspektorit të Lartë të Drejtësisë", sipas tekstit dhe lidhjeve bashkëlidhur, pjesë përbërëse e këtij urdhri.

2. Ngarkohen punonjësit e Zyrës së Inspektorit të Lartë të Drejtësisë për zbatimin e këtij urdhri.

3. Ngarkohet Drejtoria Ekonomike dhe Shërbimeve Mbështetëse për njoftimin dhe publikimin e këtij urdhri, në faqen zyrtare të Zyrës së Inspektorit të Lartë të Drejtësisë.

Ky urdhër hyn në fuqi menjëherë.

INSPEKTORI I LARTË I DREJTËSISË

Artur Metani

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www.ild.al info@ild.al

RREGULLORE
MBI
PARIMET DHE RREGULLAT E PËRGJITHSHME TË SIGURISË SË INFORMACIONIT NË ZYRËN E INSPEKTORIT TË LARTË TË DREJTËSISË

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti

1. Objekt i kësaj rregulloreje është përcaktimi i politikës dhe i rregullave të përgjithshme të sigurisë në mbrojtje të informacionit që administrohet nga të gjitha njësitë e Zyrës së Inspektorit të Lartë të Drejtësisë. Politika e sigurisë, detajon parimet, përgjegjësitë me qëllim ruajtjen e integritetit, disponueshmërisë dhe konfidencialitetit të aktiveve të teknologjisë, në zbatim të rregullave nga të gjitha njësitë përbërëse, të angazhuara në ndjekjen dhe zbatimin e masave teknike dhe organizative për të ruajtur sigurinë e aktiveve nga kërcënime reale apo potenciale, që prekin sistemet elektronike dhe ato të arkivimit të informacionit.

Neni 2
Qëllimi

1. Qëllimi i kësaj rregulloreje është:

a. Vendosja e rregullave të qarta, të drejtave, detyrimeve, si dhe bashkëpunimin e ndërsjellë ndërmjet njësive organizative, për të siguruar një mjedis të sigurt të aksesit në rrjetin elektronik që administrohet dhe zotërohet nga Zyra e Inspektorit të Lartë të Drejtësisë;
b. Vendosja e rregullave të qarta për sigurimin e vazhdimësisë dhe disponueshmërinë e sistemeve;
c. Përcaktimi i rregullave të përdorimit, administrimit, mbikëqyrjes dhe kontrollit të informacionit dhe aktiveve në dispozicion;
d. Marrja e masave organizative për të garantuar akses mbi bazë nevoje, identifikimi të përdoruesit dhe gjurmimit të aktivitetit;
e. Vendosja e rregullave për kontrollin, ndjekjen dhe raportimin e incidenteve apo keqfunksionimeve;
f. Masa kontrolli për sigurinë fizike të ambienteve dhe administrimit të dokumentacionit të ekspozuar;
g. Identifikimin, analizimin dhe në zbutjen e rreziqeve ndaj sigurisë së të dhënave personale në vlerësim të:
    i. Sistemeve të teknologjisë së informacionit të përdorur për përpunimin e të dhënave;
    ii. Formave manuale të përpunimit të të dhënave;

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

iii. Sigurisë fizike të ambienteve, sigurisë së personelit dhe pajisjeve elektronike ose të lëvizshme.

Neni 3
Baza ligjore

1. Rregullorja është hartuar në mbështetje të nenit 216 të ligjit nr. 115/2016, "Për organet e qeverisjes së sistemit të drejtësisë", i ndryshuar, ligjit nr. 9918 datë 19.05.2008 "Për komunikimet elektronike në Republikën e Shqipërisë", i ndryshuar, ligjit nr. 9887, datë 10.3.2008 "Për mbrojtjen e të dhënave personale", të ndryshuar, të ligjit nr. 9154, datë 06.11.2003 "Për arkivat", të ligjit nr. 8457, datë 11.02.1999, "Për informacionin e klasifikuar "sekret shtetëror"", të ligjit nr. 152/2013 "Për nëpunësin civil", i ndryshuar,

Neni 4
Fusha e zbatimit

1. Dispozitat e kësaj rregulloreje zbatohen nga funksionarët e kabinetit, inspektorët për aq sa nuk bie në kundërshtim me parashikimet e legjislacionit në fuqi për statusin e gjyqtarëve dhe prokurorëve në Republikën e Shqipërisë dhe legjislacionit në fuqi për organet e qeverisjes së sistemit të drejtësisë", si dhe nga nëpunësit civil dhe punonjësit administrativ, të cilët aksesojnë informacionin nga të gjitha burimet dhe sistemet e informacionit në pronësi ose në përdorim nga Zyra e Inspektorit të Lartë të Drejtësisë.
2. Për qëllime të kësaj rregulloreje, këtu e në vijimi termi "punonjës", nënkupton subjektet e përcaktuara në pikën 1 të këtij neni, të cilëve u lejohet aksesi në sistemet e informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë, në përputhje me funksionin dhe detyrat që ushtrojnë.
3. Në mënyrë të veçantë detyrohen të ruajnë sigurinë e informacionit:

a. Administratorët e sistemeve të brendshme ose të jashtme të teknologjisë së informacionit dhe komunikimit, të instaluar për këtë qëllim;
b. Punonjësit që përpunojnë të dhëna personale në përmbushje të detyrave funksionale pranë njësive organizative të Zyrës së Inspektorit të Lartë të Drejtësisë;
c. Përdoruesit e jashtëm, personat e tretë apo marrëveshjeve të lidhura sipas kësaj rregulloreje;
d. Të gjithë personat e caktuar nga Zyra e Inspektorit të Lartë të Drejtësisë për të përpunuar të dhënat në mënyrë manuale.

KREU II
PARIMET E SIGURISË, OBJEKTIVAT, TË DREJTAT E AKSESIT DHE PËRGJEGJËSITË

Neni 5
Parimi i sigurisë

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

1. Parimi i sigurisë së informacionit ka për qëllim garantimin e sigurisë së informacionit, në ruajte të integritetit, disponueshmërisë dhe konfidencialitetit të pajisjeve dhe programeve në përdorim apo në pronësi të Zyrës së Inspektorit të Lartë të Drejtësisë.

Neni 6
Parimi i integritetit

1. Sipas këtij parimi, informacioni i ofruar nga Zyra e Inspektorit të Lartë të Drejtësisë duhet të jetë i plotë, i saktë dhe i qëndrueshëm ndaj modifikimeve të paautorizuara ose ndaj dëmtimeve, në çdo kohë.

Neni 7
Parimi i disponueshmërisë

1. Informacioni bëhet i aksesueshëm sa herë që është e nevojshme, duke siguruar që të gjitha informacionet dhe të gjitha sistemet e informacionit janë të disponueshme dhe operacionale (të gatshme për punë) sa herë që nevojitet.

Neni 8
Parimi i konfidencialitetit

1. Parimi i konfidencialitetit siguron që të dhënat të jenë të aksesueshme vetëm për punonjësit dhe personat e autorizuar, të cilët kanë detyrimin ruajtjen e konfidencialitetit dhe të marrin masa lidhur me mbrojtjen, ruajtjen, dhe mospërhapje e tyre.

Neni 9
Parimi i përgjegjësisë

1. Inspektorët, personeli administrativ kontraktues, konsulentë ose përdorues të jashtëm, mbajnë përgjegjësi për pasojat qe rrjedhin direkt nga veprimet e tyre dhe që kanë të bëjnë me aktivet e teknologjisë së informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë. Çdo punonjësi i bëhen të qarta përgjegjësit e tij në lidhje me detyrën që kryhen.

Neni 10
Parimi i mbrojtjes fizike

1. Të gjitha aktivet e teknologjisë së informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë mbrohen duke vendosur masa dhe mjete në dispozicion për të mbrojtur sigurinë e informacionit në shkallën më të lartë nga dëmtimet fizike.

Neni 11
Objektivat e sigurisë

1. Objektivat dhe niveli i kërkuar i sigurisë së informacionit përcaktohet nëpërmjet parametrave të integritetit, konfidencialitetit dhe disponueshmërisë, të cilat renditen si vijon:
    a. Kontrolli i aksesit të të gjitha sistemeve të informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë për të garantuar korrektësinë, plotshmërinë, përditësimin dhe

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

vërtetësinë e të dhënave, si dhe mungesën e ndryshimeve të paautorizuara.

b. Autorizimi i aksesit në të dhënat e sistemeve të informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë përmes identifikimit me anë të llogarisë unike të përdoruesit, emrit (*username*) dhe fjalëkalimit (*password).*
c. Dhënia e autorizimit për akses vetëm për qëllime të përmbushjes së detyrave funksionale, sipas pozicionit të punës.
d. Mbrojtja e sistemeve përmes përdorimit të të dhënave vetëm nga persona apo mjete teknike të autorizuara, duke ruajtur fshehtësinë e fjalëkalimit dhe ndryshimit në mënyrë periodike, sipas politikave të sigurisë, të specifikuara në Nenin 48 të kësaj rregulloreje.
e. Vendosja e kufizimeve për përdoruesit e sistemit mbi bazën e aksesimit unik, duke mos lejuar hyrjen e njëkohshme të më shumë se një përdoruesi me të njëjtin fjalëkalim.
f. Mbajtja dhe shqyrtimi i vazhdueshëm i *log*-eve, për të gjitha përdorimet e sistemeve me qëllim, identifikimin e shkeljeve.
g. Hartimi dhe miratimi i masave/procedurave të sigurisë, nga njësia përgjegjëse për Teknologjinë e Informacionit, përpara se të bëhen zhvillime/ndryshime aplikimesh, mjedisi të teknologjisë së informacionit (këtu përfshihen pajisjet në dhomën e serverëve, bazat e të dhënave dhe të gjitha pajisjet e rrjetit të brendshëm të Zyrës së ILD-së). Ato klasifikohen si konfidenciale dhe kopja origjinale e tyre do të ruhet në mënyrë të sigurt nga njësia përgjegjëse për Teknologjinë e Informacionit.
h. Mbrojtja nga të gjitha kërcënimet dhe nga dëmtimet fizike.
i. Marrja e masave për të siguruar përgjegjësi mbi përdoruesit për veprimet që kryejnë mbi aktivet e informacionit në përdorim dhe çaktivizimin e llogarisë së përdoruesit, pas largimit të punonjësit nga institucioni, me kërkesë të njësisë përgjegjëse për Burimet Njerëzore.

Neni 12

Aksesimi nga përdoruesit e brendshëm

1. Punonjësit e Zyrës së Inspektorit të Lartë të Drejtësisë, kanë akses si përdorues të brendshëm në sisteme dhe rrjetin e brendshëm, me qëllim kryerjen e detyrave që ata mbulojnë.
2. Dhënia e të drejtave të aksesit në sisteme bazohet në nevojat e institucionit, të përcaktuar në bazë të detyrave funksionale të miratuara sipas rregullores së brendshme të organizimit dhe funksionimit të Zyrës së Inspektorit të Lartë të Drejtësisë.
3. Kur një përdorues i sistemeve ndryshon detyrë, ai humbet të drejtat e aksesimit që lidheshin me detyrën e mëparshme.

Neni 13

Aksesimi nga përdoruesit e jashtëm

1. Për raste të veçanta, dhënia e aksesit për përdoruesit e jashtëm, autorizohet në çdo rast me shkrim nga Inspektori i Lartë i Drejtësisë.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

2. Përpara dhënies së të drejtës së aksesit, të gjithë përdoruesit e jashtëm të sistemeve të Zyrës së Inspektorit të Lartë të Drejtësisë duhet të nënshkruajnë një deklaratë konfidencialiteti, ku pranojnë të respektojnë të gjitha rregullat dhe procedurat e kësaj rregulloreje. Modeli dhe përmbajtja e deklaratës, janë sipas lidhjes nr. 1, bashkëlidhur kësaj rregulloreje.
3. Përdoruesit të jashtëm i jepet akses për përmbushjen e qëllimit, në përputhje me autorizimin e dhënë nga Inspektori i Lartë i Drejtësisë. Përdoruesi i jashtëm monitorohet gjatë gjithë procesit nga punonjësi i Teknologjisë së Informacionit.
4. Të gjithë përdoruesit e jashtëm identifikohen në mënyrë të qartë (log-in) para se t'u jepet e drejta e aksesit në sisteme.

Neni 14
Aksesimi i të tretëve

1. Personat, të cilët nuk janë punonjës të Zyrës së Inspektorit të Lartë të Drejtësisë dhe institucionet (organizatat) e tjera, lejohen të aksesojnë aktivet e informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë vetëm në bazë të kushteve të përcaktuara në marrëveshje. Përjashtim bëjnë rastet kur aksesi kërkohet nga organet ligj zbatuese për nevoja të hetimit dhe zbulimit të veprës penale.
2. Marrëveshja duhet të përmbajë përcaktime lidhur me të drejtat dhe detyrimet e të tretëve që janë të interesuara të aksesojnë sistemet e informacionit të Zyrës së ILD-së, përfshi këtu:
    a. Njohjen me dhe zbatimin e rregullores për sigurinë e informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë;
    b. Kufizimet në kopjimin dhe në shpërndarjen e informacionit;
    c. Një përshkrim për secilin prej shërbimeve që do të ofrohet nga Zyra e Inspektorit të Lartë të Drejtësisë;
    d. Nivelin e synuar dhe atë të papranueshëm të shërbimeve;
    e. Klauzolat për ndryshimin e personelit nëse është e nevojshme;
    f. Detyrimet respektive të palëve që bëjnë marrëveshjen;
    g. Përgjegjësitë për të respektuar përputhjen me ligjin dhe me rregulloret;
    h. Mbrojtjen e të drejtës së autorit të Zyrës së Inspektorit të Lartë të Drejtësisë , si dhe të palëve të treta;
    i. Metodat e lejuara të aksesit dhe kontrolli i përdorimit të fjalëkalimit të përdoruesit;
    j. Procesin e dhënies së të drejtës për akses;
    k. Një kërkesë për të mbajtur një listë të personave të autorizuar për të përdorur shërbimet e kërkuara dhe të të drejtave të tyre përkatëse;
    l. Përcaktimin e kritereve të verifikueshme të performancës, monitorimin e tyre dhe raportimin;
    m. Të drejtën për të monitoruar dhe për të ndërprerë aktivitetin e përdoruesit;
    n. Të drejtën për të kontrolluar/verifikuar zbatimin e përgjegjësive kontraktore;
    o. Përgjegjësitë që kanë të bëjnë me instalimin dhe me mirëmbajtjen e pajisjeve dhe të programeve;

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

p. Një strukturë të qartë raportimi dhe miratim të formateve të raportimit;
q. Kërkesën për të zbatuar procedurat e Zyrës së Inspektorit të Lartë të Drejtësisë për administrimin e ndryshimeve mbi sistemet e informacionit;
r. Mbrojtjen nga programet keqdashëse;
s. Procedurat për raportimin, për njoftimin dhe për shqyrtimin e shkeljeve të sigurisë;
t. Detyrimin e palëve të treta për të kërkuar zbatimin e këtyre kushteve edhe nga nënkontraktorët e tyre.

Neni 15

Përgjegjësitë e Njësisë Përgjegjëse për Teknologjinë e Informacionit

1. Misioni i njësisë përgjegjëse për Teknologjinë e Informacionit është zbatimi i politikave dhe standardeve të përgjithshme shtetërore për një funksionim efektiv të sistemeve të teknologjisë së përpunimit të informacionit dhe të të dhënave, përmes sigurimit të mirëfunksionimit të pajisjeve dhe programeve për të garantuar përmbushjen e nevojave të veprimtarisë së Inspektorit të Lartë të Drejtësisë.
2. Njësia përgjegjëse për Teknologjinë e Informacionit është strukturë organizativo-teknike, si njësi e veçantë brenda strukturës organizative të Zyrës së Inspektorit të Lartë të Drejtësisë, e cila ka një rol të rëndësishëm në menaxhimin, koordinimin, monitorimin dhe mbikëqyrjen e përdorimit të teknologjisë së informacionit.
3. Njësia përgjegjëse për Teknologjinë e Informacionit përgatit raporte dhe procedura , në zbatim të kësaj rregulloreje, për çështje të cilat janë të rëndësishme për ruajtjen e sigurisë së informacionit, si dhe është përgjegjëse për kryerjen e procedurave si më poshtë:
    a. Shqyrton këtë rregullore dhe merr masa për zbatimin e parashikimeve në të;
    b. Monitoron ndryshimet e rëndësishme që ekspozojnë aktivet ndaj kërcënimeve të mëdha;
    c. Menaxhon dhe mirëmban të dhënat që përmban *active directory*;
    d. Ndjek zbatimin e masave lidhur me sigurimin e një mjedisi të sigurt pune nëpërmjet instalimit dhe konfigurimit të *firewall* dhe *antivirus*;
    e. Merr masa për të parandaluar, shqyrtuar dhe monitoruar shkeljet ndaj sigurisë;
    f. Merr masa për sigurinë e sistemeve të teknologjisë së informacionit, duke analizuar periodikisht riskun për të gjitha sistemet kompjuterike, si dhe përmbushjen e nevojave të sigurisë teknike dhe operative, veçanërisht për sigurinë kibernetike, integritetin e paprekshmërinë në përputhje me rregullat dhe politikat e përgjithshme shtetërore;
    g. Merr masa që sistemet e teknologjisë të përmbushin standarde të posaçme, që garantojnë parimet ergonomike, shkëmbimin e dokumenteve (përputhshmërinë e sistemeve), njësinë e dokumenteve, certifikimin e dokumenteve, indeksimin e dokumenteve, mbrojtjen e të dhënave personale;
    h. Propozon dhe miraton projekte të rëndësishme për përmirësimin e mëtejshëm të sigurisë;
    i. Rishikon periodikisht funksionimin dhe zbatimin e kësaj rregulloreje.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

Neni 16

Përgjegjësitë e njësive

1. Siguria e informacionit është përgjegjësi e çdo njësie, e cila është përgjegjëse për:
    a. Njohjen e punonjësve me objektivat e sigurisë së informacionit dhe procedurat të përcaktuar në këtë rregullore;
    b. Vlerësimin e vazhdueshëm të riskut të sigurisë në funksion të mbrojtjes së informacionit;
    c. Sigurimin e të drejtës për akses në aktivet e Zyrës së Inspektorit të Lartë të Drejtësisë (përfshi këtu kompjuterët, llogaritë e përdoruesve, çelësat dhe çdo gjë tjetër), në përputhje me detyrat e ngarkuara;
    d. Informimin për punonjësit që largohet nga Zyra e Inspektorit të Lartë të Drejtësisë ose që kalon në një njësi apo në një detyrë tjetër;
    e. 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.

Neni 17

Përgjegjësitë e punonjësit

1. Të gjithë punonjësit janë përgjegjës për respektimin dhe për ruajtjen e nivelit të kërkuar të sigurisë gjatë kryerjes së detyrave, të cilët veprojnë dhe i përdorin sistemet në përputhje me rolet e përdoruesve dhe të drejtave të aksesit, sipas kësaj rregulloreje.

KREU III
ADMINISTRIMI DHE PËRGJEGJËSIA PËR AKTIVET

Neni 18

Përgjegjësia për aktivet e teknologjisë së informacionit

1. Aktivet e informacionit në zotërim apo për përdorim me qëllim përpunimin, ruajtjen dhe mbrojtjen e të dhënave në ushtrim të veprimtarisë të Zyrës së Inspektorit të Lartë të Drejtësisë, janë:
    a. Serverët;
    b. Programet;
    c. Kompjuterët;
    d. Laptopët dhe tabletat;
    e. Bazat e të dhënave;
    f. Kontratat dhe marrëveshjet;
    g. Dokumentacionet e sistemeve;
    h. Manualet e përdoruesve dhe materialet e trajnimeve;
    i. Planet e vazhdimësisë;
    j. Rregullat dhe procedurat e rikuperimit;
    k. Informacioni i arkivuar.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

2. Përgjegjësia për aktivet është individuale për çdo punonjës që ka në ngarkim personal këto aktive sipas kartelës së regjistrit kontabël të aktiveve. Për aktivet që janë në përdorim të përbashkët dhe në ngarkim të njësisë, përgjegjësia është e të gjithë punonjësve të njësisë.

Neni 19
Regjistrimi i aktiveve të informacionit

1. Për sistemet e informacionit, hartohet dhe mbahet në mënyrë të vazhdueshme regjistri i aktiveve të informacionit, sipas formatit dhe përmbajtjes së përcaktuar në lidhjen nr. 2, që mbulon të gjitha aktivet kryesore për çdo sistem, duke përfshirë:
    a. *aktivet e informacionit*: bazat e të dhënave, dokumentacionin e sistemeve, manualet e përdoruesit, materialet e trajnimit, planet e vazhdueshmërisë së punës, rregullat dhe procedurat e rikuperimit të të dhënave të humbura, informacionin e arkivuar;
    b. *programet*: programet aplikative, programet e sistemit dhe mjetet për zhvillimin e mëtejshëm të tyre;
    c. *aktive fizike*: pajisjet kompjuterike, pajisjet e komunikimit, pajisje të tjera teknike (për shembull kabllot e energjisë elektrike, pajisjet e ajrit të kondicionuar), mobiljet;
    d. *shërbimet*: shërbimet kompjuterike, shërbimet e komunikimit dhe utilitetet e përgjithshme.
2. Për çdo aktiv, në regjistër mbahet informacion në lidhje me:
    a. përshkrimin e tij;
    b. personi i autorizuar për përdorim;
    c. nivelin e lejuar të aksesit (lexim, shkrim, kopjim, ndryshim, fshirje);
    d. klasifikimin, sipas përcaktimeve të nenit 20 të kësaj rregulloreje;
    e. nivelin e rëndësisë (L – i lartë; U – i ulët; M – i mesëm): përcakton rëndësinë e aktiveve të informacionit për Zyrën e Inspektorit të Lartë të Drejtësisë, në bazë të periudhës kohore maksimale gjatë të cilës Zyra e ILD-së mund të vazhdojë të punojë, pa i patur ato në dispozicion.
3. Regjistri i aktiveve, përgatitet për çdo përdorues dhe njësi nga njësia përgjegjëse për Teknologjinë e Informacionit, duke reflektuar ndryshimet sipas rastit.

Neni 20
Klasifikimi i informacionit

1. Informacionet elektronike që administron Zyra e Inspektorit të Lartë të Drejtësisë, i nënshtrohet klasifikimeve zyrtare të sigurisë së informacionit, siç përcaktohet në aktet në fuqi për informacionin e klasifikuar.

Neni 21
Analiza e riskut

1. Analiza e sigurisë së sistemit të arkivimit nënkupton një analizë të detajuar të gjendjes së sigurisë, duke përfshirë, në veçanti:

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

a. Analizën e riskut, në të cilën identifikohen kërcënimet që prekin pjesë individuale të sistemit të arkivimit, të afta të shkelin sigurinë apo funksionimin e tij; rezultati i analizës së riskut do të jetë një listë e kërcënimeve që mund të rrezikojnë konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave personale të përpunuara, ndërkohë që ajo do të deklarojë edhe shkallën e riskut të mundshëm, propozimet e masave për eliminimin apo minimizimin e ndikimit të riskut dhe një listë të rreziqeve të mbetura.
b. Përdorimin e standardeve të sigurisë dhe përcaktimin e metodave të tjera dhe mjeteve për mbrojtjen e të dhënave personale; vlerësimin e përshtatshmërisë së masave të sigurisë të propozuara nga standardet e sigurisë të aplikuara, metodat dhe mjetet do të përbëjnë një pjesë të analizës së sigurisë së sistemit të arkivimit.
c. Hartimin e raporteve të detajuara mbi sigurinë të cilat do të specifikojnë rezultatet që dalin nga zbatimi i rregullave të vendosura për sistemet e arkivimit, në veçanti:
    i. përshkrimin e masave teknike, organizative edhe në lidhje me personelin të përcaktuara në këtë rregullore dhe përdorimin e tyre në kushtet konkrete;
    ii. shtrirjen e kompetencave dhe përshkrimin e veprimtarive të lejuara të punonjësve që i gëzojnë ato të drejta, mënyrën e identifikimit të tyre dhe verifikimin gjatë aksesimit në sistemin e arkivimit;
    iii. objektin e përgjegjësisë së punonjësve të ngarkuar dhe të personit të kontaktit;
    iv. mënyrën, formën dhe periodicitetin e kryerjes së aktiviteteve të inspektimit të fokusuara në vëzhgimin e sigurisë së sistemit të arkivimit;

2. Procedurat gjatë avarive, dështimeve dhe situatave të tjera të jashtëzakonshme, duke përfshirë masat parandaluese për kufizimin e zhvillimit të situatave të jashtëzakonshme dhe mundësive për një restaurim efikas të gjendjes njësoj si përpara avarisë.Për të kryer analizën e riskut të sigurisë së informacionit, kryhet identifikimi i:
    a. Aktiveve;
    b. Dobësive;
    c. Kërcënimeve;
3. Vlerësimi i riskut përshkruhet sipas nivelit të riskut, i cili duhet të tregojë nivelin duke e përshkruar si “nivel i ulët”, “nivel i mesëm”, “nivel i lartë”.
4. Në vlerësimin dhe trajtimin e riskut, përfshihet:
    a. Rregullimi (implementimi i një kontrolli që pothuajse ose plotësisht i përgjigjet riskut themelor);
    b. Zbutja e riskut (mitigimi);
    c. Transferimi i riskut;
    d. Pranimi i riskut në rastet kur risku është shumë i ulët dhe mund të pranohet;
    e. Shmangia e riskut përmes komunikimit me njësitë dhe monitorimit të vazhdueshëm.
5. Zotëruesi dhe përgjegjësia e procesit të analizës së riskut:
    a. zotëruesit e procesit - sektori i teknologjisë së informacionit;
    b. zotëruesit e riskut - punonjësi ose titullari i njësisë.

Bulevardi “Dëshmorët e Kombit”, Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

6. Rezultatet e analizës së riskut përfshihen tek regjistri i riskut për aktivet e informacionit dhe përdoren për të përcaktuar strategjitë për zbutjen e çdo risku që identifikohet. Nëpunësi zbatues i institucionit kryen një analizë vjetore të riskut për aktivet e informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë, duke marrë parasysh kërcënimet dobësitë dhe impaktin, sipas procedurave që rekomandohen në standardet e miratuara për këtë qëllim.
7. Risku rishikohet nga çdo zotërues i tij nëse ka përshkallëzim 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 vit. Nëse risku do 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 rëndësisë që ka në performancë.

Neni 22
Administrimi i dokumenteve

1. Për aktet e dokumentet e krijuara apo të administruara, apo edhe ndryshimet në to, ndiqen rregullat dhe procedura e parashikuara në rregulloren e brendshme të organizimit dhe funksionimit të Zyrës së Inspektorit të Lartë të Drejtësisë.

Neni 23
Arkivimi i dokumenteve

1. I gjithë dokumentacioni i krijuar, përpunuar, administruar dhe ruajtur, pranë Zyrës së Inspektorit të Lartë të Drejtësisë krijohet dhe përpunohet në respektim dhe zbatim të parashikimeve të ligjit nr. 9154, datë 6.11.2003 "Për arkivat" dhe akteve nënligjore në zbatim të tij.

KREU V
MARRËDHËNIA E PUNËS DHE SIGURIA

Neni 24
Përshkrimet e punës dhe punësimi

1. Detyrimi për sigurinë përcaktohet që në fazën e fillimit të marrëdhënies së punës, ku çdo punonjës i Zyrës së Inspektorit të Lartë të Drejtësisë nënshkruan deklaratën e konfidencialitetit, sipas formatit të përcaktuar në lidhjen nr. 3. Çdo punonjës ka përgjegjësitë e tij në lidhje me sigurinë, pas njohjes me rregullat e përgjithshme të Zyrës së Inspektorit të Lartë të Drejtësisë, në fushën e sigurisë së informacionit.
2. Me fillimin e detyrës punonjësit njihen me detyrat dhe detyrimet gjatë ushtrimit të funksionit, të përcaktuara në aktet e Inspektorit të Lartë të Drejtësisë, si edhe me këtë rregullore, duke përcaktuar qartë edhe detyrimet për ruajtjen e informacionit dhe konfidencialitetit.
3. Punonjësit e rinj plotësojnë autorizimin dhe deklaratën personale të konfliktit të interesit për personat e lidhur të cilët ushtrojnë aktivitet privat, në përputhje me kushtet, afatet dhe procedurat e parashikuara nga legjislacioni në fuqi për konfliktin e interesit.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

4. 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 përcaktuar në ligje të posaçme.
5. Titullarët e njësive sigurojnë që në përshkrimin e pozicionit të punës, të përfshihen në përmbajtje çështje të sigurisë që lidhen me të:
    a. Rolet dhe përgjegjësitë që lidhen me sigurinë, duhet të përfshihen në përshkrimet e pozicioneve të punës, në mënyrë të veçantë për pozicionet drejtuese, duke siguruar përgjegjësinë e të gjithë punonjësve. Përshkrimet e 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 aktiveve të veçanta ose për ekzekutimin e proceseve të veçanta.
    b. Punonjësit që largohen apo transferohen, dorëzojnë detyrën, sipas përcaktimeve të bëra në nenin 96, të rregullores së brendshme të organizimit dhe funksionimit të Zyrës së Inspektorit të Lartë të Drejtësisë dhe mbikëqyrja e këtij procesi është nën përgjegjësinë e eprorit në linjë hierarkike.
    c. Përgjegjësia për dorëzimin e detyrës i përket punonjësit që largohet dhe saktësia e procesit mbikëqyret nga eprori sipas shkallës hierarkike. Çdo punonjës që largohet ka detyrimin të ruaje konfidencialitetin e të dhënave që administron dhe merr dijeni gjatë ushtrimit të detyrës publike.
6. Të gjitha aplikimet për punësim shqyrtohen me kujdes nga pikëpamja e sigurisë, duke dokumentuar të gjitha hapat e ndjekur dhe duke garantuar mbrojtjen e të dhënave dhe konfidencialitetin.

Neni 25

Procedurat e fillimit dhe të largimit nga puna

1. Njësia përgjegjëse për Burimet Njerëzore është përgjegjëse për njoftimet e rekrutimeve të reja duke kërkuar, që sipas kërkesave të pozicionit të punës, punonjësit e rinj:
    a. të furnizohen me bazën materiale të nevojshme;
    b. t'u hapet llogaria e përdoruesit;
    c. t'u jepet niveli i duhur i aksesit në pajisjet dhe në sistemet e Zyrës së Inspektorit të Lartë të Drejtësisë, përfshi këtu llogaritë e përdoruesve për kompjuterët, miratimin e lejes së aksesit të sistemeve, të dhomave të serverëve, të nyjeve të rrjetit, mjediseve të punës përmes sistemeve dhe pajisjeve të implementuara (karta aksesi, *chip-a*), etj.
2. Të gjitha kërkesat për dhënien e të drejtës së aksesit në sistemet kompjuterike të Zyrës së Inspektorit të Lartë të Drejtësisë (përfshi këtu llogarinë personale fillestare për punonjësit e rinj dhe çdo ndryshim në vazhdim në të drejtat për aksesin në sisteme) bëhen me shkrim, sipas formularit të menaxhimit të postës elektronike dhe sistemeve, për pajisjen me llogarinë përkatëse, të përcaktuar në lidhjen nr. 4, bashkëlidhur kësaj rregulloreje. Kërkesat miratohen nga Përgjegjësi i Teknologjisë së Informacionit para se të kryhen veprimet nga njësia *helpdesk.*

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

3. Çdo punonjës i ri i cili i bashkohet personelit të Zyrës së Inspektorit të Lartë të Drejtësisë, merr në dorëzim të gjitha pajisjet e aksesimit, duke pranuar njëkohësisht rregullat e vendosura për përdorimit të tyre, përpara se të hapet llogaria e përdoruesit ose t'ju jepen privilegje për të aksesuar sistemet e Zyrës së Inspektorit të Lartë të Drejtësisë.
4. Të gjithë punonjësve të rinj u jepen udhëzime të plota për procedurat e teknologjisë së informacionit dhe në veçanti për kërkesat në lidhje me çështjet e sigurisë. Këto udhëzime duhet të përfshijnë të paktën:
    a. përdorimin e përgjithshëm të mjeteve të teknologjisë së informacionit;
    b. ndihmën e kualifikuar nga Njësia përgjegjëse për Teknologjinë e Informacionit,;
    c. familjarizimin me objektivat e sigurisë së Zyrës së ILD-së, rregullat dhe procedurat e sigurisë;
    d. trajtimin e informacioneve konfidenciale;
    e. politikën e përdorimit të internetit, të email-it etj.;
    f. rregullat për fjalëkalimet;
    g. rregullat për përdorimit të postës elektronike.
5. Njësia përgjegjëse për Burimet Njerëzore është përgjegjëse për të garantuar zbatimin e procedurave të sigurisë në rastet kur ndonjë prej punonjësve largohet nga puna, duke kërkuar:
    a. heqjen e të gjitha të drejtave të aksesimit;
    b. dorëzimin e mjeteve të aksesit, çelësat, shënimet, kompjuterët apo çdo aktiv tjetër në përdorim.
6. Procedurat teknike për mbylljen e llogarisë së përdoruesit dhe për heqjen e të drejtave të aksesit të sistemeve të Zyrës së Inspektorit të Lartë të Drejtësisë, bëhen para se punonjësi të largohet fizikisht nga ambienti i punës.
7. Njësia përgjegjëse për Burimet Njerëzore, njofton menjëherë personin përgjegjës të Njësia përgjegjëse për Teknologjinë e Informacionit, kur ndonjë punonjësi i përfundon marrëdhënia e punës.
8. Njësia përgjegjëse për Teknologjinë e Informacionit sigurohet që njoftimi për ndërprerjen e marrëdhënies së punës, të trajtohet sa më parë, për rastet e largimit nga puna të një punonjësi të caktuar, dhe kryen procedurat e nevojshme për ndryshimin e të drejtave të përdoruesit të personit që do të largohet. Ndryshimi i të drejtave përfshin:
    a. Fshirjen e menjëhershme të llogarisë së përdoruesit;
    b. Heqjen e disa privilegjeve të aksesit;
    c. Mbajtjen e nivelit aktual të privilegjeve të aksesit që ka përdoruesi, por duke rritur nivelin e auditimit për këtë përdorues.

Neni 26
Trajnimi

1. Të gjithë punonjësit trajnohen për përdorimin korrekt të sistemeve kompjuterike dhe udhëzohen rast pas rasti për përdorimin e aktiveve të teknologjisë së informacionit. Trajnimi bëhet përpara se t'u jepet e drejta për akses në sisteme.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

2. Punonjësit që kanë akses në aktivet e teknologjisë së informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë janë të detyruar të ndjekin dhe zbatojnë rregullat dhe standardet e sigurisë në Zyrën e Inspektorit të Lartë të Drejtësisë. Të gjithë punonjësit marrin trajnimet e nevojshme për rregullat dhe për procedurat organizative dhe të sigurisë. Trajnimi fillestar kryhet sa më shpejtë që të jetë e mundur për punonjësit e rinj.
3. Objektivat e trajnimeve në lidhje me sigurinë janë:
    a. krijimi i kulturës së sigurisë në të gjithë Zyrën e Inspektorit të Lartë të Drejtësisë;
    b. edukimi i punonjësve mbi pasojat e veprimeve të tyre mbi sigurinë e informacionit;
    c. udhëzimi i punonjësve për rregullat dhe procedurat e sigurisë sipas pozicioneve përkatëse;
    d. përcaktimi i përgjegjësive që mban çdo punonjës mbi sigurinë dhe detyra e secilit për të raportuar çdo shkelje të rregullave të sigurisë.
4. Të gjithë specialistët e teknologjisë së informacionit duhet të marrin rregullisht trajnime përmirësuese në fushat e tyre të specializimit dhe të ndjekin seminare / workshop-e / trajnime periodike në fushat e interesit të përgjithshëm, veçanërisht në ato që lidhen me sigurinë.

KREU VI
DENONCIMI RAPORTIMI DHE MASAT E MARRA NDAJ INCIDENTEVE TË SIGURISË

Neni 27
Incidentet e sigurisë

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

Neni 28
Raportimi i incidenteve të sigurisë

1. Për të gjitha rastet e ngjarjeve që lidhen me sigurinë, ndiqet procedura për raportimin e incidenteve. Të gjitha ngjarjet duhet të raportohen menjëherë nga punonjësi që konstaton incidentin e sigurisë, duke plotësuar formuarin për raportimin e incidenteve, sipas lidhjes nr. 5 dhe përcjellë atë tek Njësia përgjegjëse për Teknologjinë e Informacionit,.
2. Njësia përgjegjëse për Teknologjinë e Informacionit trajton informacionin duke marrë masat paraprake të nevojshme dhe njofton Sekretarin e Përgjithshëm. Për raste të veçanta e serioze, njoftohet Inspektori i Lartë i Drejtësisë.
3. Njësia përgjegjëse për Teknologjinë e Informacionit, pasi ka marrë formularin e raportimit të incidentit, merr të gjitha masat për të riparuar incidentin dhe njofton Sekretarin e Përgjithshëm me të dhënat e mëposhtme:
    a. Emrin dhe të dhënat e personit që raportoi incidentin;

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

b. Tipin e të dhënave apo informacionit që është kompromentuar;
c. Dëmet apo riskun që shkakton incidenti;
d. Vendndodhjen e incidentit;
e. Numrin e inventarit të aktiveve të prekura nga incidenti;
f. Datën dhe orën kur ka ndodhur incidenti;
g. Vendndodhjen e të dhënave apo pajisjes që ka pësuar dëmin/incidentin;
h. Tipin dhe rrethanat e incidentit.

4. Të gjitha veprimet që kryhen pas incidentit duhet të ruhen dhe të pasqyrohen në raportin e analizës së vlerësimit të riskut.
5. Shkelja e parashikimeve të këtij neni nga punonjësit përbën shkak për fillimin e ecurisë disiplinore dhe marrjen e masave përkatëse disiplinore në përputhje me rregullat e legjislacionit në fuqi, për çdo punonjës.
6. Të gjithë përdoruesit/aksesuesit, të cilët shkaktojnë dëm ekonomik, përgjigjen sipas dispozitave te Kodit Civil të Republikës së Shqipërisë.

Neni 29

Raportimi i keqfunksionimit të programit

1. Për të minimizuar çdo ndërprerje të shërbimeve apo çdo dëmtim të të dhënave, është e nevojshme që keqfunksionimi i programeve të korrektohet sa më shpejt që të jetë e mundur. Keqfunksionimet e dukshme të programeve i raportohen njësisë përgjegjëse për Teknologjinë e Informacionit, e cila përgjigjet menjëherë dhe udhëzon në lidhje me mënyrën e veprimit në raste të tilla.

Neni 30

Siguria e faqes zyrtare të internetit (*web*)

1. Mbikëqyrja e faqes zyrtare realizohet nga njësia përgjegjëse për teknologjinë e informacionit, e cila siguron shërbimin *online* të informacionit të publikuar në faqe dhe kryen aktivitetet e mëposhtme në funksion të ruajtjes së sigurisë:
   a. Përcaktimit të privilegjeve të administrimit të faqes zyrtare të internetit nga nivele të ndryshëm përdoruesish, të thjeshtë apo administrator, me të drejta editimi ose jo;
   b. Sigurimit të një ambienti steril, duke fshirë shërbime të panevojshme apo skedarë të ekzekutueshëm;
   c. Monitorimit të vazhdueshëm të log-eve;
   d. Përdorimit të certifikatave të sigurisë "SSL/TLS", me qëllim krijimin e një kanali të koduar ndërmjet klientit dhe serverit
   e. Kryerjes së *backup*-it të faqes zyrtare çdo javë;
   f. Vënies në funksion të mekanizmave të kontrollit për *malware.*
2. Për të të gjitha rastet e ngjarjeve që lidhen me cenimin e sigurisë do të raportohet duke plotësuar formuarin, sipas lidhjes nr. 5.

Neni 31

Shkelja e rregullave dhe procedurave të sigurisë

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

1. Kur njësia përgjegjëse për Teknologjinë e Informacionit, gjykon se veprimtaria e një punonjësi nuk është në përputhje me rregullat dhe procedurat e sigurisë, për çfarëdolloj arsyeje, takon dhe udhëzon punonjësin për të diskutuar çështjen dhe për të planifikuar veprimet korrigjuese.
2. Njësia përgjegjëse për Teknologjinë e Informacionit njofton sa më shpejt të jetë e mundur dhe siguron dokumentacion të plotë për titullarin e njësisë nga varet punonjësi. Në çdo rast dyshimi për shkelje të rregullave dhe procedurës së sigurisë, ndiqet një proces disiplinor. Shkeljet dhe përgjegjësia mbi to, përcaktohet nga legjislacioni në fuqi, në varësi të statusit të punonjësit dhe rregullave disiplinore të parashikuara për atë kategori punonjësi.
3. Në rrethana të veçanta tepër serioze, shkelja mund të raportohet në organet përkatëse sipas ligjit.

KREU V
SIGURIA FIZIKE DHE E MJEDISEVE

Neni 32
Siguria e ambienteve (ndërtesës)

1. Aksesimi i të gjitha ambienteve të sistemeve të informacionit kontrollohet rreptësishtë dhe në çdo kohë, në mënyrë që të parandalohen humbjet ose kompromet imet e aktiveve të teknologjisë së informacionit dhe të aktiveve të tjera.

Neni 33
Sistemi i aksesit

1. Të gjitha ambientet kritike sigurohen me sisteme aksesi dhe çdo punonjës i autorizuar për të hyrë një ambient specifik, pajiset me një mjet individual aksesi.
2. Njësia përgjegjëse për Teknologjinë e Informacionit është përgjegjëse për mbajtjen e të dhënave në lidhje me të gjitha aksesimet e autorizuara, ku përfshihen detaje si: emri i punonjësit, njësia ku ushtron funksionin ose detyrën, data kur është aktivizuar aksesi, ora dhe dita deri kur i lejohet aksesi.
3. Për të gjitha aktivitetet e aksesimit, mbajtja e *log*-eve është e detyrueshme kur sistemet e aksesimit të ambienteve e lejojnë një gjë të tillë.

Neni 34
Vizitorët

1. Vizitorëve nuk u lejohet lëvizja e lirë dhe e pakontrolluar në ambientet e Zyrës së Inspektorit të Lartë të Drejtësisë. Çdo vizitor pajiset me një mjet identifikimi të përkohshëm para se të lejohet të hyjë. Vizitorët, punonjësit e mirëmbajtjes dhe persona të tjerë të huaj, shoqërohen gjatë gjithë kohës nga punonjës të autorizuar të Zyrës së Inspektorit të Lartë të Drejtësisë.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

2. Në veçanti, vizitorëve nuk duhet t'u lejohet të aksesojnë ambientet me akses të kufizuar, sidomos në vendndodhjet e serverëve, të pashoqëruar nga një person i autorizuar nga njësia përgjegjëse për Teknologjinë e Informacionit,.

Neni 35
Siguria e aktiveve

1. Të gjitha aktivet e teknologjisë së informacionit mbrohen fizikisht nga kërcënimet e sigurisë dhe nga rreziqet e mjedisit.

Neni 36
Dhomat e serverëve

1. Të gjithë serverët dhe pajisjet e komunikimit (*router*-at, *switch*-et, *firewall*-et, etj.) duhet të vendosen në dhoma apo në ambiente të mbyllura e të sigurta. Aksesi në këto dhoma duhet të lejohet vetëm për punonjësin e autorizuar nga Përgjegjësi i Teknologjisë së Informacionit.
2. Aksesi në dhomat e serverit dhe në nyjet e rrjetit duhet të jetë i kontrolluar dhe të mbahen *log*-e ku të shënohet emri i personit ose i personave, arsyet e hyrjes, data/ora dhe veprimet e kryera. Përjashtohen nga mbajtja e shënimeve për arsyet e hyrjes dhe veprimet e kryera, punonjësit e teknologjisë së informacionit pranë Zyrë së Inspektorit të Lartë të Drejtësisë.
3. Dhoma e serverit pajiset me sistem aksesi, ajër të kondicionuar, me kamera, me UPS, detektorë dhe me fikës zjarri.

Neni 37
Kompjuterët personal

1. Kompjuterët personal (PC) vendosen në vende të përshtatshme për përdorimin e tyre dhe instalohen vetëm nga punonjës të njësisë përgjegjëse për Teknologjinë e Informacionit, në përputhje me rregullat e përcaktuara në rregulloren e brendshme për përdorimin e rrjetit dhe pajisjeve kompjuterike.
2. Instalimi i programeve realizohet bazuar në nevojën e përmbushjes së detyrës dhe programet duhet të jenë pjesë e listës së programeve të lejuara për instalim, që miratohet dhe mirëmbahet nga njësia përgjegjëse për Teknologjinë e Informacionit,.

Neni 38
Nxjerrja jashtë godinës

1. Të gjitha pajisjet, të cilat për arsye të nevojshme pune duhet të nxirren jashtë godinës së Zyrës së Inspektorit të Lartë të Drejtësisë, duhet të jenë po aq të sigurta sa edhe pajisjet që ndodhen brenda tyre, duke marrë parasysh riskun e të punuarit jashtë ambienteve punës të Zyrës së Inspektorit të Lartë të Drejtësisë.
2. Pajisjet dhe mediat që nxirren jashtë godinës së Zyrës së Inspektorit të Lartë të Drejtësisë, nuk duhet të lihen në vende publike (përfshi këtu makinat) të pambrojtur. Ato shkatërrohen në mënyrë të parikuperueshme kur nxirren përfundimisht jashtë pune.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

3. Informacioni i klasifikuar në letër ose në trajtë elektronike, nxirret jashtë vetëm në përputhje me aktet në fuqi për informacionin e klasifikuar

KREU VII
ADMINISTRIMI I SISTEMEVE TË INFORMACIONIT

Neni 39
Aplikimet

1. Përgjegjësitë dhe procedurat e administrimit dhe të aktivitetit, mbi të gjitha aplikimet kompjuterike, dokumentohen si pjesë përbërëse e procesit të zhvillimit të tyre. Procedurat e aktivitetit testohen nga përdoruesi në bashkëpunim me Njësinë përgjegjëse për Teknologjinë e Informacionit.

Neni 40
Kontraktorët e burimeve të jashtme

1. Kërkesat e sigurisë së Zyrës së Inspektorit të Lartë të Drejtësisë duhet t'i bashkëlidhen të gjitha kontratave që bëhen me ofruesit e shërbimeve, për të garantuar sigurinë mbi veprimet e punonjësve të tyre gjatë lidhjeve me rrjetin e Zyrës së Inspektorit të Lartë të Drejtësisë.

Neni 41
Programet keqdashëse

1. Të gjitha pajisjet e teknologjisë së informacionit mbrohen nga programet keqdashëse, (ku përfshihen viruset e kompjuterëve si dhe çdo tip tjetër i njohur dhe i klasifikuar si kërcënim informatik).
2. Në funksion të mbrojtjes dhe parandalimit të veprimeve keqdashëse, instalohet dhe vihet në funksion një program i licencuar antivirus, i cili duhet të përditësohet automatikisht, në mënyrë të vazhdueshme, nën kujdesin e punonjësve të teknologjisë së informacionit.
3. Ndalohet çinstalimi ose çaktivizimi i programeve antivirus, të cilat trajtohen si shkelje serioze.

Neni 42
Bazat e të dhënave të Zyrës së ILD-së

1. Njësia përgjegjëse për Teknologjinë e Informacionit është përgjegjëse për të siguruar që bazat e të dhënave të mbajtura në serverët e Zyrës së Inspektorit të Lartë të Drejtësisë t'u bëhet kopje (*backup*) e rregullt në përputhje me procedurat e përcaktuara, për çdo sistem.
2. Kopjet (*backup*) e të dhënave duhet të testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme.
3. Procedurat e rikrijimit (*restore*) të të dhënave duhet të testohen rregullisht për t'u siguruar që ato janë të efektshme dhe mund të ekzekutohen brenda kohës së lejuar.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

Neni 43

Të dhënat që ndodhen në kompjuterët personal të përdoruesve

1. Çdo punonjës është përgjegjës personalisht për mbrojtjen nga humbjet e të dhënave të ruajtura në kompjuterin personal, si dhe ruajtjen e një kopje të dytë (*backup*), sipas nevojës.

Neni 44

Përdorimi i internetit dhe postës elektronike

1. Të gjithë punonjësve të Zyrës së Inspektorit të Lartë të Drejtësisë të cilëve u është dhënë akses në internet dhe në shërbim email-i, zbatojnë politikën e përdorimit të internetit si dhe rregullat e zbatueshme në rregulloren e brendshme të organizimit dhe funksionimit të Zyrës së Inspektorit të Lartë të Drejtësisë.

KREU VII
KONTROLLI I AKSESIT

Neni 45

Kontrolli i aksesit

1. Përdoruesit e sistemeve të Zyrës së Inspektorit të Lartë të Drejtësisë krijohen me kërkesë të njësia përgjegjëse për Burimet Njerëzore, drejtuar njësisë përgjegjëse për Teknologjinë e Informacionit, për ndjekjen e procedurave të nevojshme për krijimin e tyre ose për krijimin e përdoruesit përkatës të llogarisë së postës elektronike zyrtare, pranë Agjencisë së Shoqërisë së Informacionit.
2. Përdoruesit i jepet akses në sistemet elektronike vetëm në përputhje me funksionet e tij për kryerjen e detyrave, përmes krijimit të llogarisë unike të përdoruesit. Aksesi jepet bazuar në rolin e punonjësit të Zyrës së Inspektorit të Lartë të Drejtësisë, i cili përcaktohet nga rrjedha e proceseve të punës e nevojat operative të punës për të përmbushur detyrën e tij.
3. Çdo përdorues i sistemeve, si punonjës i Zyrës së Inspektorit të Lartë të Drejtësisë, 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, të krijuar nga njësia përgjegjëse për Teknologjinë e Informacionit.
4. Kontrolli i aksesit zbatohet për të gjithë personat, pavarësisht roleve të tyre dhe shërben për ruajtjen e integritetit dhe sigurinë e aktivitetit, duke ndaluar aksesin e paautorizuar.
5. Ndalohet rreptësisht shpërndarja e të dhënave të llogarisë personale në persona të tjerë, apo dy ose më shumë aksese të njëkohshme me të njëjtën llogari përdoruesi. Shkelja e këtij rregulli do të trajtohet si një shkelje e rëndë dhe pas sjell përgjegjësi disiplinore.
6. Në funksion të kontrollit të aksesit, ndiqen procedura të dokumentuara për:
    a. Regjistrimin e përdoruesve të rinj;

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

b. 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);
c. Çaktivizimin ose mbylljen përfundimtare të një llogarie përdoruesi.

7. Natyra e këtyre procedurave dhe përgjegjësitë për administrimin e tyre mund të ndryshojnë në varësi të kategorisë së përdoruesit.
8. Llogaria e përdoruesit çaktivizohet, me përfundimin e marrëdhënies së punës ose kontratës që ka krijuar llogarinë.
9. Të gjitha llogaritë e përdoruesve dhe caktimi i profileve të tyre rishikohen çdo 6 (gjashtë) muaj nga njësia përgjegjëse për Teknologjinë e Informacionit, në bashkëpunim me titullarin e njësisë përkatëse.
10. Në bazë të rishikimit, hartohet lista e emrave të të gjithë përdoruesve të brendshëm aktivë, me profilet e tyre përkatëse. Kjo listë do të mbahet dhe do të kontrollohet nga njësia përgjegjëse për Teknologjinë e Informacionit.

Neni 46
Administrimi i fjalëkalimeve

1. Punonjësi i njësisë përgjegjëse për Teknologjinë e Informacionit ndjek këto rregulla në lidhje me mënyrat e administrimit të fjalëkalimeve, ku përfshihen:
   a. Zgjedhja e fjalëkalimit fillestar;
   b. Udhëzimi i punonjësve për procedurën e ndryshimit të fjalëkalimit dhe këshillat e njohura për sigurinë në zgjedhjen e tij;
   c. Udhëzimi i punonjësve për mbrojtjen e fjalëkalimit si dhe ndalimin e dhënies së fjalëkalimit midis përdoruesve;
   d. Mbivendosja e fjalëkalimit (në qoftë se një llogari përdoruesi është mbyllur ose në qoftë se përdoruesi ka harruar fjalëkalimin).
2. Kërkesat e sigurisë për fjalëkalimet e përdoruesve përfshijnë:
   a. Fjalëkalimi duhet të jetë minimumi 8 karaktere;
   b. Fjalëkalimi duhet të përmbajë një kombinim të germave kapitale dhe të vogla, numrave dhe karaktereve speciale (si !, @, #, etj);
   c. Fjalëkalimi duhet të ndryshojë çdo 90 ditë. Në rast kompromentimi të fjalëkalimit ai duhet të ndryshohet menjëherë;
   d. 10(dhjetë) fjalëkalimet e mëparshme nuk mund të përdoren;
   e. Fjalëkalimi nuk mund t'u komunikohet të tjerëve, të shkruhet në letër, ose të ruhet në ndonjë *file* ose bazë të dhënash në kompjuter;
   f. Fjalëkalimi duhet të jetë i maskuar dhe nuk printohet ose përfshihet kurrë në raporte ose *log*-e;
   g. Fjalëkalimi nuk duhet të përmbajë të dhëna personale apo emrin e institucionit;
3. Kërkesat e sigurisë për fjalëkalime të tjera, si fjalëkalimet e bazës së të dhënave, *server*-ave, *router*-ave, *firewall*-eve, pajisje të tjera të rrjetit, etj, përfshijnë:
   a. Fjalëkalimi duhet të jetë minimumi 10 karaktere;

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

b. Fjalëkalimi duhet të përmbajë një kombinim të germave kapitale dhe të vogla, numrave dhe karaktereve special (si !, @, #, etj);
c. Fjalëkalimi duhet të ndryshojnë çdo 30 ditë, por mund ketë përjashtime. Në rast kompromet imi të fjalëkalimit ai duhet të ndryshohet menjëherë;
d. 15 (pesëmbëdhjetë) fjalëkalimet e mëparshme nuk mund të përdoren;
e. Fjalëkalimi duhet të jetë i maskuar dhe nuk printohet ose përfshihet kurrë në raporte ose *log-e*;
f. Fjalëkalimi nuk duhet të përmbajë të dhëna personale apo emrin e institucionit;
g. Nuk duhet të përdoren karakteret si :(\ , ~ , <)
h. Nuk duhet të përdorën hapësira.
i. Administratori i sistemit duhet të sigurojë mbrojtje ndaj tentativave të dyshimta të sulmeve me fjalëkalim "*brute force*".
j. Administratori duhet të konfigurojë sistemin në mënyrë që pas një kohe të caktuar pa aktivitet, aksesi në sistem kyçet. Për riaksesim, përdoruesi rivendos fjalëkalimin.

Neni 47

Kontrollet për përdoruesit

1. Njësia përgjegjëse për Teknologjinë e Informacionit, kontrollon aktivitetin e përdoruesve për sipas roleve të përdoruesve për të minimizuar rrezikun e aktiviteteve mashtruese ose keqdashëse,. Kur një përdorues ndryshon detyrë, rol apo funksion , ai humbet të drejtat e aksesit që lidheshin me detyrën e mëparshme.
2. Akumulimi në kohë i privilegjeve evitohet dhe të monitorohet vazhdimisht nga njësia përgjegjëse për Teknologjinë e Informacionit.
3. Përdoruesit udhëzohen që të ruajnë konfidencialitetin e llogarisë së tyre dhe informacionin që aksesohet, gjatë gjithë periudhës që kanë autorizim për përdorimin e sistemeve apo llogarive të tyre.
4. Formati i llogarive të përdoruesve standardizohet, aq sa është e mundur, për të gjithë përdoruesit, me anë të një bashkëpunimi midis njësisë përgjegjëse për Teknologjinë e Informacionit dhe njësive të Zyrës së Inspektorit të Lartë të Drejtësisë. Ky format do të jetë pjesë e dokumentacionit të sistemeve. Lista e të gjithë përdoruesve të jashtëm të autorizuar, bashkë me llogaritë e tyre, mbahet nga njësia përgjegjëse për Teknologjinë e Informacionit.

Neni 48

Autentifikimi i përdoruesve të jashtëm

1. Të gjithë përdoruesit e jashtëm, para se t'u jepet akses në sistemet e informacionit të Zyrës së Inspektorit të Lartë të Drejtësisë, identifikohen në mënyrë të vetme. Niveli i aksesit në të dhënat e sistemit 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 kompromet ohen.
2. Mënyrat e autentifikimit që përdor Zyra e Inspektorit të Lartë të Drejtësisë janë:
   a. kombinimi i emrit të përdoruesit dhe fjalëkalimit, e identifikuar me emrin *llogari;*
   b. përdorimi i *smart cards* ose i formave të tjera *hardware* të autentikimit.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

Neni 49
Marrëveshjet me kontratë

1. Kërkesat e sigurisë përfshihen në të gjitha kontratat ndërmjet ILD-së dhe përdoruesve të jashtëm për të administruar aksesin e tyre direkt (*online*) në sistemet e Zyrës së Inspektorit të Lartë të Drejtësisë. Këtu mund të përfshihet:
    a. Një deklaratë për pranimin dhe për respektimin e të drejtave të aksesit, sipas modelit të përcaktuar në lidhjen nr. 1;
    b. Të marrin përsipër përmbushjen e kërkesave të sigurisë sa i takon krijimit dhe menaxhimit të fjalëkalimeve, sipas nenit 46 të kësaj rregulloreje;
    c. Të marrin përsipër përdorimin e programeve antivirus të miratuara nga Zyra e Inspektorit të Lartë të Drejtësisë, në të gjithë kompjuterët që mund të lidhen me sistemet e Zyrës së Inspektorit të Lartë të Drejtësisë dhe të garantojnë që programet antivirus rinovohen (*update*) të paktën një herë në ditë;
    d. Të marrin përsipër ruajtjen e konfidencialitetit të plotë për të gjitha të dhënat dhe informacionet që ata mund të marrin nga sistemet e Zyrës së Inspektorit të Lartë të Drejtësisë.

Neni 50
Dhënia e privilegjeve

1. Në rastet e përdoruesve të jashtëm, privilegjet caktohen në bazë të profileve të sigurisë. Këto profile zbatohen dhe testohen, përpara dhënies së tyre tek përdoruesit.
2. Inspektori i Lartë i Drejtësisë miraton dhënien apo ndryshimin e privilegjeve të përdoruesve, duke marrë në konsideratë mendimin e njësisë përgjegjëse për Teknologjinë e Informacionit.
3. Privilegjet përcaktohen në dokumentacionin e aplikimeve dhe ruhen të sigurta sipas përcaktimeve në këtë rregullore, nga njësia përgjegjëse për Teknologjinë e Informacionit.

KREU VIII
ADMINISTRIMI I VAZHDUESHMËRISË SË AKTIVITETIT

Neni 51
Vazhdueshmëria

1. Njësia përgjegjëse për Teknologjinë e Informacionit zhvillon dhe mban plane për rikrijimin e të gjitha proceseve dhe shërbimeve kritike, me qëllim sigurimin e vazhdueshmërisë së aktivitetit në Zyrën e Inspektorit të Lartë të Drejtësisë, në rastet e ndërprerjeve serioze. Ndërprerje të tilla mund të shkaktohen nga shkaqe natyrore, nga aksidente, nga defekte, nga veprime të qëllimshme.

Neni 52
Planet e vazhdueshmërisë së aktivitetit

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

1. 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.
2. Planet e vazhdueshmërisë duhet të mundësojnë funksionimin në vazhdimësi të aktiviteteve në raste dëmtimesh, defektesh ose humbjesh të shërbimeve apo të pajisjeve. Ato përfshijnë:
    a. Identifikimin dhe vendosjen e prioriteteve për proceset kritike;
    b. Identifikimin e kërcënimeve të mundshme që mund të kenë efekt në këto procese;
    c. Përcaktimin e ndikimit të mundshëm të katastrofave të ndryshme;
    d. Identifikimin dhe realizimin e marrëveshjeve për çdo përgjegjësi, në rast gjendjeje të jashtëzakonshme;
    e. Dokumentacionin për procedurat dhe proceset për të cilat është rënë dakord;
    f. Edukimin e personelit në ekzekutimin e procedurave;
    g. Testimin e planeve;
    h. Përmirësimin e vazhdueshëm të planeve.

Neni 53
Rikrijimi i informacionit në rast katastrofash

1. Për të rindërtuar (rikrijuar) sistemet dhe shërbimet prioritare kompjuterike në raste katastrofash është i domosdoshëm krijimi dhe ruajtja e planeve për këtë qëllim. Rifillimi i këtyre sistemeve duhet të bëhet në një interval kohe sa më të shkurtër.
2. Për çdo sistem dhe shërbim krijohet një plan rindërtimi (*recovery*), i cili mbahet nga njësia përgjegjëse për Teknologjinë e Informacionit, duke përfshirë edhe shërbimet që sigurohen nga ofertuesit e jashtëm.

Neni 54
Përmirësimi

1. Të gjitha planet për vazhdueshmërinë e aktivitetit dhe planet e rikrijimit rishikohen e përmirësohen të paktën një herë në vit. Planet të cilat vjetërsohen shpejt, si rezultat i ndryshimeve që ndodhin brenda ose jashtë institucionit, përmirësohen (*update*) në mënyrë të vazhdueshme me qëllim mbrojtjen e investimit mbi planin fillestar dhe për të garantuar efektshmërinë e vazhdueshmërisë.

KREU IX
DISPOZITA TË FUNDIT

Neni 55
Rregulla të përgjithshme

1. Të gjitha informacionet që vendosen, hartohen, dërgohen dhe/ose merren në sistemet elektronike të institucionit janë pronë e Zyrës së Inspektorit të Lartë të Drejtësisë dhe i nënshtrohen rregullave për mbrojtjen dhe ruajtjen e tyre në mënyrë të sigurt sipas

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

legjislacionin në fuqi. Punonjësit e Zyrës në funksion të mbrojtjes dhe ruajtjes së informacionit zbatojnë këto rregulla të përgjithshme:

a. Aksesimin e të dhënave sipas roleve dhe përgjegjësive të përdoruesve të sistemit, të përcaktuar nga Inspektori i Lartë i Drejtësisë
b. Përdorimin e informacionit të marrë vetëm për nevoja të punës dhe mos përhapjen e tij;
c. Mbajtjen e të gjitha të dhënave të sigurta duke marrë masa paraprake dhe duke ndjekur udhëzimet e mëposhtme:
    i. Punonjësit ruajnë fshehtësinë e fjalëkalimeve personale *(username / password)* të cilat nuk duhet t'i shpërdorojnë, shpërndajnë apo të bëjnë të shumëfishta dhe të njëkohshme me të njëjtën llogari, e cila duhet mbyllur në përfundim të punës;
    ii. 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;
    iii. Punonjësit sigurohen që kompjuterët duhet të fiken plotësisht në fund të ditës së punës;
    iv. Punonjësit duhet të sigurohen që kompjuterat e tyre të jenë të kyçur (*lock*) kur lihen të pambikëqyrura;
    v. Punonjësit duhet të sigurohen që të mbyllin çdo pajisje kompjuterike portative siç janë laptop-ët dhe tablet-et;
    vi. Punonjësit janë përgjegjës për raportimin, nëse janë në dijeni të shkeljeve dhe rreziqeve potenciale rreth sigurisë, si dhe të aktiviteteve joetike që shkelin rregullat e institucionit.

Neni 56

Pronësia e programeve

1. Pronësia e programeve përcaktohet nëpërmjet licencës, e cila kufizon përdorimin e produktit në kompjuter të caktuar. Të gjitha programet e vëna në dispozicion, për përdorim, punonjësve apo përdoruesve të jashtëm, janë pronë e Zyrë së Inspektorit të Lartë të Drejtësisë.
2. Programet nuk lejohet të kopjohen nga një kompjuter në një tjetër, pa patur të drejtën e kopjimit nga pronari i tij.
3. Kopjimi i programeve që janë në pronësi të Zyrës së Inspektorit të Lartë të Drejtësisë, për t'u përdorur në kompjuterët që nuk i përkasin Zyrës së ILD-së, për çfarëdo lloj qëllimi të ndryshëm nga aktivitetet e autorizuara, përbën shkelje dhe do të trajtohet në përputhje me rregullat disiplinore në fuqi, për cilindo punonjës që përdor programet në pronësi të Zyrës, për qëllime të paautorizuara.

Neni 57

Kontrollet e politikës së sigurisë

1. Të gjitha njësitë janë subjekt i një kontrolli zyrtar vjetor për të siguruar zbatimin e rregullave dhe standardeve të sigurisë. Përdoruesit e aktiveve të informacionit ofrojnë

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

bashkëpunim për auditimin e aktivitetit të përdorimit të sistemeve sipas rregullave të përcaktuara në këtë rregullore.

2. Njësia përgjegjëse për Teknologjinë e Informacionit kontrollon të gjitha pajisjet kompjuterike për përputhjen me standardet e sigurisë. Këto kontrolle përfshijnë ekzaminimin e sistemeve për t'u siguruar që kontrollet e sigurisë të pajisjeve dhe të programeve janë zbatuar me korrektësi.

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

1. **Lidhja nr.1 -** "**Deklaratë e konfidencialitetit përdoruesit - sipas nenit 13**
2. **Lidhja nr. 2 – "Formati i regjistrit të aktiveve të informacionit" – sipas nenit 19**
3. **Lidhja nr.3 -** "**Deklaratë e konfidencialitetit dhe përgjegjshmërisë për përdoruesit e brendshëm"- sipas nenit 24**
4. **Lidhja nr.4 "Formularin e menaxhimit të postës elektronike dhe sistemeve", sipas nenit 25.**
5. **Lidhja nr. 5 - "Formuari i raportimit të incidenteve" - sipas neni 28**

Bulevardi "Dëshmorët e Kombit", Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

Lidhja nr.1 “Deklaratë Konfidencialiteti për përdoruesit e jashtëm”

Unë i/e nënshkruari/a _____ me cilësinë e personit të autorizuar nga Inspektori i Lartë i Drejtësisë, për _____, në zbatim të ligjit nr. 9887, datë 10.03.2008, "Për Mbrojtjen e të Dhënave Personale", i ndryshuar, të Ligjit nr. 115/2016 "Për organet e qeverisjes së sistemit të drejtësisë", i ndryshuar, si dhe akteve nënligjore, deklaroj se do të zbatoj të gjitha rregullat dhe procedurat për të mbrojtur të dhënat personale dhe përmbajtjen e informacionit, i cili do të administrohet gjatë autorizimit të dhënë për akses në sistem.

Nuk do të përdor dhe nuk do të transmetoj te persona të paautorizuar të dhëna personale apo informacione konfidenciale në lidhje me ose të marra dhe pranoj me përgjegjësinë time të plotë të respektoj dhe ruaj konfidencialitetin dhe besueshmërinë në lidhje me informacionet/arkivat/sistemet elektronik në të cilat kam akses duke respektuar palët e treta, të mos kopjoj asnjë të dhënë apo informacion pa leje të shkruar të titullarit, të mos nxjerr përmbajtjen e këtyre të dhënave personave të tjerë, si dhe të ndjek procedurat e punës në mënyrë të tillë që të mbroj privatësinë dhe të veproj në mënyrë profesionale, në përputhje me rregulloret në fuqi për mbrojtjen e të dhënave personale dhe sigurisë së informacionit për sistemet elektronike.

Deklaruesi: _____

Datë ___/___/202_

Bulevardi “Dëshmorët e Kombit”, Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

Lidhja nr. 2 “Formati i Regjistrit të Aktiveve të Informacionit”

Regjistri i Aktiveve të Informacionit					
Nr.	Përshkrimi i aktivit	Përdoruesi i autorizuar	Klasifikimi	Niveli i rëndësisë	Niveli i lejuar i aksesit

Bulevardi “Dëshmorët e Kombit”, Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

Lidhja nr. 3 “Deklaratë Konfidencialiteti”

Unë _____si punonjës i Zyrës së Inspektorit të Lartë të Drejtësisë, kam dijeni të plotë që për shkak të detyrës do të kem akses në informacione/arkiva të cilat janë të konsideruara si konfidenciale.

Me anë të kësaj deklarate marr përsipër të mos përdor dhe të mos i transmetoj personave të paautorizuar të dhëna personale apo informacione konfidenciale në lidhje me ose të marra nga Inspektori i Lartë i Drejtësisë, përveç nëse autorizohem shprehimisht, ose kërkohet me ligj. Unë e kuptoj se ky detyrim vlen gjatë afatit të punësimit si dhe pas përfundimit të tij.

Unë e kuptoj se përdorimi dhe zbulimi i të dhënave personale në lidhje me individët, trajtohet nga ligji nr.9987, datë 10.03.2008 për “Mbrojtjen e të Dhënave Personale”, i ndryshuar dhe pranoj me përgjegjësinë time të plotë të respektoj dhe ruaj konfidencialitetin dhe besueshmërinë në lidhje me informacionet/arkivat në të cilat kam akses duke respektuar palët e treta, të mos kopjoj asnjë të dhënë apo informacion pa leje të shkruar të titullarit, të mos nxjerr përmbajtjen e këtyre të dhënave personave të tjerë, si dhe të ndjek procedurat e punës në mënyrë të tillë që të mbroj privatësinë dhe të veproj në mënyrë profesionale, në përputhje me rregulloret në fuqi për mbrojtjen e të dhënave personale dhe sigurisë së informacionit për sistemet elektronike.
Unë nuk do të përdor ose përhap asnjë të dhënë personale që marr dijeni gjatë punës time për ndonjë qëllim që është në kundërshtim me qëllimet e kësaj pune.

Unë e kuptoj se jam i detyruar të ruaj konfidencialitetin për të dhënat personale dhe t’i mbaj ato të sigurta, duke marrë të gjitha masat organizative dhe teknike të përshtatshme.

Marr përgjegjësinë e plotë që në qoftë se konstatohet që kam vepruar në kundërshtim me udhëzimet në lidhje me konfidencialitetin e të dhënave personale apo në rast të mosruajtjes së tyre, dhe jam i ndërgjegjshëm që ndaj meje mund të merren masa të menjëhershme. Unë e kuptoj këtë veprim si një nevojë për të mbajtur standarde të larta profesionale pranë Zyrë së Inspektorit të Lartë të Drejtësisë.

Deklaruesi: _____

Data ___/___/202_

Bulevardi “Dëshmorët e Kombit”, Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

Lidhja nr. 4 “Formulari i Menaxhimit të Postës Elektronike dhe Sistemeve”

I. HAPJE E NJË LLOGARIE TË RE (datë ___.___.202__)

Emër Mbiemër	
Pozicioni i punës	
Sektori	
Drejtoria	
Lloji i aktit të emërimit (nr. prot./datë)	
Nr. Tel.	

II. NDRYSHIM / PEZULLIM / MBYLLJE LLOGARIE (datë ___.___.202__)

Emër Mbiemër	
Pozicioni i punës	
Sektori	
Drejtoria	
Lloji i aktit të emërimit (nr. prot./datë)	
Lloji i aktit të largimit (nr. prot./ datë)	
Nr. Tel.	
Pezullim llogarie (shkaku dhe afati)	
Mbyllje llogarie	

Bulevardi “Dëshmorët e Kombit”, Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al

Lidhja nr. 5 “Formulari i Raportimit të Incidenteve”

FORMULAR I RAPORTIMIT TË INCIDENTEVE

<table>
<tr><td>Tipi i incidentit</td><td colspan="3"></td></tr>
<tr><td rowspan="3">Emri i personit që raportoi incidentin</td><td rowspan="3"></td><td>Tel.</td><td></td></tr>
<tr><td>Email</td><td></td></tr>
<tr><td>Sektori</td><td></td></tr>
<tr><td rowspan="2">Vendndodhja</td><td rowspan="2"></td><td>Data</td><td></td></tr>
<tr><td>Ora</td><td></td></tr>
<tr><td>Niveli i klasifikimit të informacionit i cënuar</td><td colspan="3"></td></tr>
<tr><td>Lloji i informacionit të dëmtuar/cënuar</td><td colspan="3"></td></tr>
<tr><td>Pajisja e dëmtuar</td><td colspan="3"></td></tr>
<tr><td>Nr. i përdoruesve të cënuar</td><td></td><td>Sektori i cënuar</td><td></td></tr>
<tr><td colspan="4">Arsyet e ndodhjes së incidentit</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Hapat e ndërmarra</td></tr>
<tr><td colspan="4"></td></tr>
</table>

Bulevardi “Dëshmorët e Kombit”, Godina nr. 13, Tiranë Tel: + 355 4 2217217 http://www. ild.al info@ild.al