VENDIM
Nr. 221, datë 22.4.2026

PËR MIRATIMIN E RREGULLAVE MBI MENAXHIMIN E INFRASTRUKTURËS DHE SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT NË GJYKATAT E REPUBLIKËS SË SHQIPËRISË

Në mbështetje të nenit 147, pika 1 të Kushtetutës së Republikës së Shqipërisë; të neneve 61, shkronja "ë", 92, pika 2, 97, pika 1, shkronja "c" dhe 98, pika 4, të ligjit nr. 115/2016, "Për organet e qeverisjes së sistemit të drejtësisë", të ndryshuar; të nenit 36, të ligjit nr. 98/2016, "Për organizmin e pushtetit gjyqësor në Republikën e Shqipërisë", të ndryshuar; të ligjit 25/2024, "Për sigurinë kibernetike", si dhe të VKM-së nr. 971, datë 2.12.2020, "Për miratimin e rregullave për politikat e përgjithshme shtetërore, për Sistemin e Teknologjisë së Informacionit, për Sistemin e Drejtësisë"; të VKM-së nr. 972, datë 2.12.2020, "Për organizimin, funksionimin e përcaktimin e kompetencave të Qendrës së Teknologjisë së Informacionit për Sistemin e Drejtësisë", me propozim të Komisionit të Planifikimit Strategjik, Administrimit dhe Buxhetit, Këshilli i Lartë Gjyqësor

VENDOSI:

1. Miratimin e rregullave mbi menaxhimin e infrastrukturës dhe sistemeve të teknologjisë së informacionit në gjykatat e Republikës së Shqipërisë, sipas tekstit dhe anekseve që i bashkëlidhen këtij vendimi dhe përbëjnë pjesë përbërëse të tij.
2. Ky vendim publikohet në faqen zyrtare të internetit të Këshillit të Lartë Gjyqësor dhe hyn në fuqi në datën e botimit në Fletoren Zyrtare.

PËR KËSHILLIN E LARTË GJYQËSOR
KRYETAR
Ilir Rusi

RREGULLAT MBI MENAXHIMIN E INFRASTRUKTURËS DHE SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT NË GJYKATAT E REPUBLIKËS SË SHQIPËRISË

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Qëllimi

1. Qëllimi i kësaj rregulloreje është përcaktimi i rregullave për administrimin, përdorimin, kontrollin dhe sigurimin e Sistemeve të Teknologjisë së Informacionit në sistemin gjyqësor të Republikës së Shqipërisë.
2. Rregullorja synon garantimin e konfidencialitetit, integritetit dhe disponueshmërisë së informacionit të përpunuar dhe të ruajtur në sistemet dhe bazat e të dhënave gjyqësore, në përputhje me legjislacionin në fuqi.

Neni 2
Fusha e zbatimit

1. Kjo rregullore zbatohet nga të gjithë përdoruesit e sistemeve TIK në gjykatat e të gjitha shkallëve të Republikës së Shqipërisë, si dhe në Këshillin e Lartë Gjyqësor.

2. Dispozitat e saj janë të detyrueshme për çdo person që, në bazë të funksionit, marrëdhënies së punës apo marrëdhënies kontraktore, përdor ose administron sistemet TIK.

Neni 3
Përkufizime

1. Në këtë rregullore termat e mëposhtëm kanë këto kuptime:

a) "Administrim gjyqësor" është tërësia e veprimtarive organizative dhe mbështetëse që sigurojnë funksionimin efektiv të sistemit gjyqësor;

b) "Administratori i sistemit" është personi ose grupi i personave të autorizuar për menaxhimin, mirëmbajtjen dhe garantimin e sigurisë së sistemit;

c) "Akses" është e drejta e një përdoruesi për të hyrë dhe përdorur një sistem, në përputhje me detyrat e tij ose me autorizimin e dhënë;

ç) "Aksesi i autorizuar nga zotëruesi i informacionit" nënkupton qasjen në të dhëna në përputhje me nivelin e miratuar të autorizimit, që mund të përfshijë shikimin, përpunimin, ndryshimin ose fshirjen e tyre;

d) "Aksesi i autorizuar në sistem" është procesi i krijimit dhe menaxhimit të profileve të përdoruesve dhe i të drejtave të tyre, në përputhje me politikat e sigurisë, për të garantuar akses vetëm për subjektet e autorizuara;

dh) "Autentifikim" është procesi i verifikimit të identitetit të përdoruesit përpara dhënies së aksesit në sistem;

e) "*Backup*" është infrastruktura teknike dhe proceset për krijimin dhe ruajtjen e kopjeve rezervë të të dhënave, për përdorim në raste emergjente;

ë) "*Backup* sistematik" është procesi automatik dhe periodik i kopjimit të të dhënave, me qëllim garantimin e mbrojtjes së tyre në rast humbjeje ose dëmtimi;

f) "Fjalëkalim" është kodi sekret personal që përdoret për autentifikimin e përdoruesit dhe që duhet të mbahet konfidencial;

g) "Fshirja e mediave të rishkrueshme përpara se të ripërdoren" është procesi i fshirjes ose asgjësimit të të dhënave të ruajtura në media të rishkrueshme, si disqe të ngurtë, CD ose DVD, përpara përdorimit të tyre për ruajtjen e të dhënave të reja;

gj) "Incident i sigurisë së informacionit" është çdo ngjarje që cenon ose rrezikon konfidencialitetin, integritetin ose disponueshmërinë e informacionit;

h) "Infrastrukturë e Sistemit" janë pajisjet fizike, programet, rrjetet dhe bazat e të dhënave që mbështesin funksionimin e Sistemit;

i) "Gjurmueshmëria" është procesi i kërkimit të gjurmëve/logeve, që përmbajnë informacion të nevojshëm për monitorimin dhe detektimin e veprimeve në Sistem, si dhe për zgjidhjen e problemeve të sigurisë;

j) "Hartimi i planit të vazhdimësisë së biznesit/*Disaster Recovery Plan*" është ndërmarrja e një analize për identifikimin e proceseve kryesore të punës dhe të informacionit nga i cili ato varen, me qëllim sigurimin e vazhdimësisë së funksionimit në situata emergjente;

k) "Integriteti i të dhënave" është garantimi i saktësisë, plotësisë dhe mbrojtjes së të dhënave nga ndryshimet e paautorizuara;

l) "Kredenciale" janë të dhënat identifikuese unike që mundësojnë autentifikimin dhe aksesin në sistem;

ll) "Konfidencialiteti i të dhënave" është parimi sipas të cilit informacioni është i aksesueshëm vetëm për persona ose sisteme të autorizuara;

m) "Klasifikimi dhe inventarizimi i informacionit" është procesi i identifikimit, organizimit dhe vlerësimit të informacionit sipas rëndësisë dhe nivelit të sigurisë së kërkuar;

n) “*Malware*” janë programe ose kode me qëllim të dëmshëm që instalohen ose ekzekutohen në sistem për të shkaktuar dëme ose ndërhyrje të paautorizuara;

nj) “Masat për mbrojtjen e mjedisit” përfshijnë pajisjet dhe mekanizmat mbrojtës si sistemet kundër zjarrit, furnizimi me energji të pandërprerë (UPS) dhe mbrojtja nga dëmtimet nga uji;

o) “Mbikëqyrje” është procesi i monitorimit dhe vlerësimit të vazhdueshëm të infrastrukturës dhe sistemeve TIK për garantimin e sigurisë, stabilitetit dhe performancës së tyre;

p) “Niveli i sigurisë së bazës së të dhënave të sistemit të menaxhimit” është niveli i sigurisë që aplikohet për një sistem kompjuterik të caktuar, për të garantuar mbrojtjen e tij sipas kritereve të përcaktuara nga legjislacioni në fuqi;

q) “*Off site backup*” është një metodë e sigurimit të të dhënave që përfshin kopjimin dhe ruajtjen e tyre jashtë vendndodhjes primare fizike, në një ambient të dytë;

r) “Përpunimi i të dhënave” çdo veprim i kryer mbi të dhënat, përfshirë grumbullimin, regjistrimin, ruajtjen, renditjen, përshtatjen, ndreqjen, këshillimin, shfrytëzimin, përdorimin, bllokimin, fshirjen, shkatërrimin ose çdo veprim tjetër, si dhe transmetimin e tyre;

rr) “Përdorues” çdo individ i identifikuar në mënyrë unike në sistem përmes një emërtimi ose kredencialeje;

s) “Përdorues i brendshëm” janë punonjësit e administratës gjyqësore dhe personat e autorizuar që aksesojnë sistemin në kuadër të funksioneve të tyre;

sh) “Përdorues i jashtëm” janë individët jashtë administratës gjyqësore që autorizohen për të aksesuar sistemin;

t) “Përditësimi automatik i të dhënave në formë elektronike” është procesi i përditësimit të të dhënave në mënyrë të automatizuar përmes mekanizmave elektronikë;

th) “Plan i Vazhdimësisë së Biznesit” – është dokumenti që përcakton procedurat për të garantuar vazhdimësinë e aktiviteteve kritike në raste emergjente;

u) “Privilegj” është parimi sipas të cilit çdo përdorues pajiset vetëm me të drejtat minimale të nevojshme për kryerjen e detyrave të tij. Zbatimi i këtij parimi kufizon dëmin që mund të rezultojë nga aksidentet, gabimet ose përdorimet e paautorizuara;

v) “Procedurat e *Backup*-it” janë procedurat e shkruara për rikuperimin e informacionit nga *backup*-i të cilat duhet të testohen periodikisht;

x) “Siguria e informacionit” është sigurimi i konfidencialitetit, integritetit dhe disponueshmërisë së informacionit;

xh) “Siguria kibernetike” – është tërësia e mjeteve ligjore, organizative, teknike dhe edukative, me qëllim mbrojtjen e hapësirës kibernetike;

y) “Sistemi i Menaxhimit të Çështjeve Gjyqësore” (Sistemi) janë sistemet elektronike të përdorura për administrimin e çështjeve gjyqësore, përfshirë ICMIS dhe ARKIT;

z) “Sisteme TIK” janë sistemet e teknologjisë së informacionit dhe infrastruktura përkatëse që përdoren nga gjykatat;

zh) “Teknologjia e Informacionit dhe Komunikimit” (TIK) janë pajisjet dhe programet elektronike që mundësojnë mbledhjen, ruajtjen, përpunimin dhe transmetimin e të dhënave.

Neni 4

Parimet në përdorimin dhe sigurinë e infrastrukturës TIK

1. Përdorimi i infrastrukturës TIK bazohet në parimet e ligjshmërisë, efikasitetit, sigurisë, profesionalizmit, saktësisë, kontrollit, llogaridhënies, barazisë dhe transparencës.

2. Mbikëqyrja dhe siguria e infrastrukturës TIK dhe e Sistemit bazohet në parimet e ligjshmërisë, unitetit dhe gjurmueshmërisë, si dhe në përdorimin automatik të të dhënave në formë elektronike.

Neni 5

Ruajtja e konfidencialitetit dhe mbrojtja e të dhënave personale

1. Të gjithë përdoruesit e sistemeve TIK në gjykata dhe në Këshillin e Lartë Gjyqësor duhet të ruajnë konfidencialitetin e informacionit zyrtar dhe të mbrojnë të dhënat personale të palëve dhe pjesëmarrësve të tjerë, në përputhje me legjislacionin në fuqi dhe aktet nënligjore në zbatim të tij.

2. Gjatë procedimit të çështjeve përmes sistemit, zbatohen të gjitha përgjegjësitë ligjore për ruajtjen e konfidencialitetit.

3. Përdoruesit e sistemeve TIK kryejnë vetëm veprimet e nevojshme sipas autorizimeve dhe detyrave funksionale, pa tejkaluar përgjegjësitë e caktuara.

4. Çdo përdorim ose shpërndarje e paautorizuar e të dhënave konsiderohet shkelje sipas legjislacionit në fuqi.

KREU II
PËRDORUESIT, AKSESI DHE PROCEDIMI I DOSJES PËRMES SISTEMIT TË MENAXHIMIT TË ÇËSHTJEVE

Neni 6
Grupi i menaxhimit të çështjes gjyqësore (GMÇ)

1. Grupi i menaxhimit të çështjes gjyqësore përbëhet nga gjyqtari i çështjes dhe sekretari gjyqësor.

2. Grupi i menaxhimit të çështjes gjyqësore siguron përmbushjen e të gjitha hallkave të çështjes në sistem, duke përfshirë regjistrimin, përpunimin e çështjes, hedhjen e dispozitivit, pasqyrimin e vendimit dhe arkivimin elektronik të çështjes.

3. Ndihmës magjistratët dhe këshilltarët ligjorë kanë akses për hedhjen e relacioneve në Sistem.

4. Ndihmësit ligjorë kanë vetëm akses për informacion dhe vendimet e shkallëve më të ulëta.

5. Grupi i menaxhimit të çështjes gjyqësore, në zbatim të përgjegjësive të tij:

a) Siguron informacion dhe statistika për palët e interesuara, bazuar në të dhënat e ruajtura në Sistem;

b) Siguron plotësimin e të gjitha fushave të Sistemit me të dhëna të plota, të sakta dhe pa gabime. Çdo kopjim, transmetim, shpërndarje ose veprim tjetër i ngjashëm ndaj personave ose subjekteve jashtë GMÇ-së është i ndaluar;

c) Siguron mbrojtjen e të dhënave personale dhe ruajtjen e konfidencialitetit.

6. Në varësi të procesit të punës së gjykatës, një sekretar gjyqësor mund të jetë i konfiguruar në më shumë se një GMÇ.

7. Kur sekretari i caktuar në GMÇ nuk është prezent, kryhet zëvendësimi i tij në rubrikën përkatëse për të siguruar funksionimin e GMÇ-së. Zëvendësuesit i caktohen kredenciale të veçanta me të dhënat e tij.

8. Ndalohet përdorimi i kredencialeve të sekretarit që nuk është prezent.

Neni 7
Krijimi i llogarive për përdoruesit e Sistemit

1. Çdo përdoruesi i caktohet një llogari me fjalëkalim në Sistemin e Menaxhimit të Çështjeve. Të drejtat e qasjes në të dhëna përcaktohen sipas autorizimeve dhe detyrave funksionale të përdoruesit.

2. Krijimi i llogarive bëhet me kërkesë, bazuar në nevojat e gjykatave.

3. Llogaritë e përdoruesve administrohen nga strukturat IT të gjykatave dhe mbikëqyren nga

Këshilli i Lartë Gjyqësor, me qëllim garantimin e sigurisë ndaj hyrjeve të paautorizuara.

4. Fjalëkalimet duhet të përmbushin kriteret e sigurisë, sipas parashikimeve të përcaktuara në nenin 29 e vijues të kësaj rregulloreje.

Neni 8

Regjistrimi i çështjes përmes Sistemit të Menaxhimit të Çështjeve

1. Regjistrimi fillestar i çështjes në Sistem kryhet nga sekretaria regjistruese e gjykatës.

2. Sekretaria regjistruese regjistron çështjen sipas kohës së arritjes dhe me të dhënat përkatëse të çështjes, palëve, pjesëmarrësve të tjerë dhe të dhënat e tjera të kërkuara nga Sistemi.

3. Regjistrimi i çështjeve gjyqësore kryhet në ditën e pranimit të saj, me përjashtim të rrethanave të veçanta, ai kryhet në ditën e nesërme të punës.

4. Gjatë regjistrimit të çështjes, sekretaria regjistruese:

a) Kryen verifikimin paraprak për të identifikuar çështjet e njëjta ose të ngjashme, duke marrë si referencë identitetin e palëve, objektin e çështjes, akuzën ose numrin e procedimit për rastet penale;

b) Bën kategorizimin e natyrës së çështjes, në përputhje me regjistrat fizikë në përdorim nga gjykatat;

c) Pasqyron të dhënat e palëve ndërgjyqëse dhe vendimet e mëparshme nga të gjitha shkallët e gjyqësorit, sipas fushave të kërkuara nga Sistemi;

ç) Siguron plotësinë dhe saktësinë e të dhënave të çështjes gjyqësore që regjistron.

5. Çdo çështje merr numër unik identifikimi të gjeneruar nga Sistemi në secilën shkallë të gjykimit.

6. Numri i regjistrimit identifikon kategorinë e çështjes, numrin e radhës, kodin e gjykatës ku është regjistruar dhe vitin, përjashtuar Gjykatën e Shkallës së Parë të Juridiksionit të Përgjithshëm Tiranë dhe Gjykatën e Posaçme për Korrupsionin dhe Krimin e Organizuar, të cilat i referohen regjistrit fizik.

7. Numri unik i identifikimit jepet vetëm një herë gjatë regjistrimit fillestar të çështjes në çdo shkallë të gjyqësorit.

8. Pas regjistrimit, të dhënat e çështjes pasqyrohen në portalin e gjykatave përkatëse.

Neni 9

Shpërndarja/rishpërndarja e çështjes gjyqësore përmes Sistemit

1. Shortimi i çështjeve kryhet në përputhje me rregullat e përcaktuara nga Këshilli i Lartë Gjyqësor, në mbështetje të legjislacionit në fuqi.

2. Sistemi mundëson shpërndarjen e çështjeve për gjyqtarë në mënyrë automatike dhe manuale.

3. Shpërndarja e çështjes dhe ngarkesa me numër çështjesh kryhen në bazë të kritereve të përcaktuara në aktet ligjore.

4. Funksionaliteti i shortimit të çështjeve gjyqësore menaxhohet nga kryetari i gjykatës.

5. Për çdo veprim në Sistem, arsyeja e veprimit pasqyrohet në rubrikën përkatëse.

6. Kancelari mbikëqyr procesin e organizimit dhe dokumentimit të ndarjes së çështjeve me short, në përputhje me aktet ligjore në fuqi.

Neni 10

Detyrat dhe përgjegjësitë e sekretarit gjyqësor gjatë përdorimit të Sistemit

1. Sekretari gjyqësor planifikon seancën në Sistemin e Menaxhimit të Çështjeve sipas udhëzimeve të gjyqtarit, duke kryer të gjitha veprimet e nevojshme për njoftimin e palëve dhe

për gjenerimin e njoftimeve të seancës së planifikuar.

2. Ngarkon procesverbalin e seancës përgatitore, paraprake ose gjyqësore në Sistem.

3. Ngarkon menjëherë dispozitivin pas përfundimit të seancës në Sistem.

4. Kryen veprime të tjera në Sistem, sipas detyrave të deleguara dhe udhëzimeve të gjyqtarit përkatës, si dhe sipas akteve nënligjore të miratuara nga Këshilli i Lartë Gjyqësor.

Neni 11

Planifikimi i seancave përmes Sistemit

1. Menjëherë pas caktimit të datës së seancës nga gjyqtari i çështjes, sekretari gjyqësor kryen të gjitha veprimet e nevojshme në Sistem për planifikimin e seancës.

2. Përmes Sistemit, sekretari gjyqësor evidenton të dhënat e seancës gjyqësore, duke përfshirë: numrin e çështjes; tipin e seancës (pajtim, dhomë këshillimi etj.); sallën e gjykimit; si dhe kohën e fillimit dhe të mbarimit sipas udhëzimeve të kryetarit të seancës.

3. Çdo seancë e kryer pasqyrohet në kohë reale në Sistem.

4. Sekretari gjyqësor pasuron Sistemin me të dhëna shtesë, duke përfshirë:

a) statusin e gjykimit;

b) regjistrimin audio të seancës (po/jo);

c) zhvillimin e seancës me dyer të hapura ose të mbyllura;

ç) datën e seancës;

d) kohën e mbarimit;

dh) gjyqtarët prezent;

e) sallën e gjykimit;

ë) palët ndërgjyqëse;

f) palët e pranishme në sallë;

g) procesverbalin e seancës;

gj) arsyen e regjistrimit të vonuar (nëse ka);

h) arsyen e shtyrjes së seancës (nëse ka);

i) datën e re të planifikuar.

5. Pas regjistrimit të seancës, të dhënat e autorizuara pasqyrohen në portalin e gjykatave përkatëse sipas nivelit të tyre. Caktimi, shtyrja dhe anulimi i seancave kryhen përmes Sistemit, duke evidentuar arsyet e mosmbajtjes së seancës.

Neni 12

Regjistrimi i dispozitivit të vendimit në Sistem

1. Në përfundim të procesit gjyqësor, sekretari gjyqësor regjistron dispozitivin e çështjes në Sistem. Në ndërfaqen e regjistrimit ngarkohen të dhënat përkatëse, duke përfshirë:

a) emrin e gjyqtarit;

b) kohën e hedhjes së dispozitivit;

c) datën e dispozitivit të çështjes;

ç) palët e pranishme gjatë shpalljes së vendimit;

d) llojin e dispozitivit të vendimit;

dh) përshkrimin e dispozitivit.

2. Të dhënat e regjistruara në fushën e dispozitivit pasqyrohen në portalin e gjykatave përkatëse.

Neni 13

Regjistrimi i vendimit nga gjyqtari në Sistem

1. Të gjitha vendimet e marra nga gjyqtari rreth çështjes, qofshin vendime të ndërmjetme, përfundimtare apo jo përfundimtare, duhet të regjistrohen përmes Sistemit.

2. Hedhja e vendimeve jopërfundimtare kryhet vetëm nëse çështja ka pasur një seancë të mëparshme të regjistruar në Sistem; hedhja e vendimeve përfundimtare kryhet vetëm nëse sekretaria gjyqësore ka regjistruar dispozitivin përkatës.

3. Vendimi duhet të përmbajë të dhënat e gjeneraliteteve të palëve, objektin e çështjes apo akuzën, bazën ligjore, konkluzionet e palëve, si dhe përmbajtjen e vendimit të strukturuar sipas formatit të Sistemit.

4. Të dhënat e vendimit të regjistruara pasqyrohen në portalin e gjykatave përkatëse.

Neni 14

Fshirja dhe korrigjimi i çështjes në Sistem

1. Përdoruesi që ka kryer gabime gjatë plotësimit të të dhënave ose ka ndërmarrë veprime jo të sakta gjatë realizimit të detyrave të çështjes në Sistem, të cilat nuk mund të korrigjohen nga vetë ai, duhet të adresojë kërkesën për korrigjim në mënyrë zyrtare drejtuar administratorit të sistemit përmes sistemit të raportimit të problematikave, në https://helpdesk.klgj.al.

2. Administratori i sistemit, pasi administron kërkesën, për çdo veprim që kryen në sistemin e menaxhimit të çështjeve, përfshirë fshirje ose përditësime të të dhënave, mban procesverbal në rastin kur çështja është në fazën e regjistrimit.

3. Kur çështja është shortuar, çdo veprim i kryer në sistem, qoftë fshirje apo përditësim i të dhënave, realizohet vetëm me vendim të titullarit të institucionit.

Neni 15

Veçimi dhe bashkimi i çështjeve në Sistem

Veçimi dhe bashkimi i çështjeve gjyqësore kryhen përmes Sistemit, vetëm pasi gjyqtari i çështjes të ketë marrë vendim të ndërmjetëm përkatës.

Neni 16

Arkivimi i çështjes përmes Sistemit

1. Çështjet e përfunduara nga gjykata e nivelit përkatës, të zgjidhura me vendim të formës së prerë, arkivohen nga arkivisti, i cili ka detyrimin të regjistrojë veprimin e arkivimit në Sistem.

2. Pas arkivimit të çështjes ose të secilës dosje që i përket një numri unik, statusi i secilës dosje në atë numër unik ndryshohet në "Arkivuar". Në Sistem evidentohen vendi, data, ora dhe përdoruesi që ka kryer arkivimin e çështjes.

3. Pas përfundimit të procedurës së arkivimit, e drejta e aksesit në çështje i takon vetëm arkivistit, ndërsa për përdoruesit e tjerë të gjykatës aksesi mbyllet.

Neni 17

Aksesi në çështje sipas profilit të përdoruesit në Sistem

1. Profilet e përdoruesve në Sistem përfshijnë, por nuk kufizohen në:

a) Kryetarin e gjykatës;

b) Zëvendëskryetarin e gjykatës;

c) Gjyqtarin;

ç) Kancelarin e gjykatës;

d) Ndihmësmagjistratin;

dh) Këshilltarin ligjor;

e) Ndihmësin ligjor;
ë) Kryesekretarin;
f) Sekretarin gjyqësor;
g) Sekretarin regjistrues;
gj) Nëpunësin e financës dhe buxhetit;
h) Nëpunës të tjerë që ushtrojnë funksione në fushën e kërkimit ligjor dhe dokumentacionit, burimeve njerëzore, teknologjisë së informacionit, arkivit, si dhe marrëdhënieve me publikun dhe median;
i) Përdoruesin e gjykatës;
j) Administratorin, arkitektin ose zhvilluesin e Sistemit;
k) Inspektorin ose audituesin gjyqësor, si dhe analistin e proceseve të punës në Sistem;
l) Inspektorin e Lartë të Drejtësisë;
ll) Këshillin e Lartë Gjyqësor.
2. Aksesi në Sistem kategorizohet si më poshtë:
a) Akses i plotë, i jep përdoruesit të drejtën për të parë të gjitha të dhënat dhe veprimet e ndërmarra në dosje, si dhe për të krijuar detyra dhe për të ndërmarrë veprime mbi çështjen;
b) Akses për lexim, i jep përdoruesit të drejtën për të parë të gjitha të dhënat, dokumentet dhe veprimet e ndërmarra në dosje, pa të drejtë për të krijuar detyra apo për të ndërmarrë veprime mbi çështjen;
c) Akses i kufizuar, i jep përdoruesit të drejtën për të parë vetëm statusin e çështjes, të dhënat e përgjithshme të rastit dhe të dhënat e palëve;
ç) Akses në të dhënat për seanca gjyqësore, i jep përdoruesit të drejtën për të parë të dhënat mbi seancat e caktuara, si: numri i dosjes, lloji i çështjes, data, ora, lloji i seancës (e hapur ose e mbyllur) dhe vendi i zhvillimit të saj;
d) Akses në çështjet e zgjidhura, përdoruesi nuk ka akses në dosjet e çështjeve në procedim, por ka të drejtë leximi në dosjet e çështjeve me status "Përfunduar";
dh) Akses në statistika;
e) Akses në regjistra;
ë) Mohim i aksesit të çështjes.

Neni 18
Raportimi përmes Sistemit

1. Raportet statistikore mbi performancën e punës së gjykatave dhe gjyqtarëve gjenerohen, për aq sa është teknikisht e mundur, përmes Sistemit të Menaxhimit të Çështjeve.
2. Raportimi i problematikave që lidhen me funksionimin e Sistemit kryhet përmes platformës elektronike *Online Ticketing Service Desk*, e cila aksesohet nëpërmjet lidhjes https://helpdesk.klgj.al

KREU III
POLITIKAT DHE PROCEDURAT PËR MENAXHIMIN E SISTEMEVE TIK

Neni 19
Kërkesat për mbikëqyrjen e infrastrukturës TIK

1. Infrastruktura TIK në gjykatat e Republikës së Shqipërisë dhe në Këshillin e Lartë Gjyqësor, në përmbushje të detyrave funksionale, duhet të garantojë:
a) Monitorimin e rrjetit, i cili përfshin kontrollin e trafikut brenda dhe jashtë gjykatës, identifikimin e problemeve të rrjetit, si: ngadalësimi i shpejtësisë, humbja e paketave, konfliktet e adresave IP, si dhe evidentimin e përdoruesve të paautorizuar;

b) Monitorimin e serverave, që përfshin ndjekjen dhe vlerësimin e performancës së tyre, përfshirë funksionalitetin, përdorimin e burimeve, ngarkesën e CPU-së, memorien dhe ruajtjen e të dhënave;

c) Monitorimin e bazave të të dhënave, që përfshin kontrollin e performancës, vlerësimin e vonesave në kërkimin e informacionit, monitorimin e hapësirës së diskut dhe garantimin e sigurisë së tyre;

ç) Monitorimin e sigurisë, që përfshin identifikimin e aktiviteteve të paligjshme, tentativave për hyrje të paautorizuar në sistemet e gjykatës, si dhe kontrollin e aksesit të përdoruesve të autorizuar;

d) Monitorimin e pajisjeve fizike, që përfshin kontrollin e performancës së serverave, *switch*-eve, ruterëve dhe pajisjeve të tjera të rrjetit;

dh) Monitorimin e shërbimeve, duke garantuar funksionimin dhe disponueshmërinë e shërbimeve IT të ofruara për përdoruesit, si: posta elektronike, shërbimet e aksesit në rrjet, aplikacionet e specializuara, përfshirë regjistrimin e seancave dëgjimore dhe sistemet e hyrje-daljeve.

Neni 20

Procedura për mbikëqyrjen e infrastrukturës TIK

1. Çdo strukturë IT në gjykatat e Republikës së Shqipërisë ka detyrimin të zbatojë procedurat e mëposhtme për mbikëqyrjen e infrastrukturës TIK:

a) Identifikimi i burimeve kritike të informacionit, duke evidentuar komponentët thelbësorë për funksionimin e përditshëm të gjykatës, si: serverat, rrjeti, bazat e të dhënave, pajisjet e sigurisë fizike dhe elemente të tjera të infrastrukturës;

b) Përcaktimi i roleve dhe përgjegjësive, duke caktuar personat përgjegjës për verifikimin e infrastrukturës së Sistemit, si dhe një person përgjegjës për koordinimin e mbikëqyrjes dhe reagimin ndaj incidenteve të sigurisë;

c) Vlerësimi i rrezikut, përmes identifikimit të vulnerabiliteteve dhe rreziqeve të mundshme për infrastrukturën e Sistemit që cenojnë sigurinë fizike dhe sigurinë e informacionit, nëpërmjet kontrolleve periodike;

ç) Zbatimi i politikave dhe standardeve të sigurisë, duke respektuar aktet e dokumentuara për sigurinë e informacionit dhe mbikëqyrjen e infrastrukturës së Sistemit, përfshirë politikat e aksesit, kontrollin e hyrje-daljeve, menaxhimin e privilegjeve dhe aksesin në ambientet e serverave;

d) Menaxhimi i gjurmëve (*log*-eve) dhe monitorimi i sistemeve, duke verifikuar dhe monitoruar aktivitetin e rrjetit dhe të Sistemit, duke ruajtur *log*-et përkatëse dhe duke përdorur mjete automatike për identifikimin e tentativave të paautorizuara, ndryshimeve të papritura të konfigurimit apo shkeljeve të politikave të sigurisë, me miratimin paraprak të Këshillit të Lartë Gjyqësor;

dh) *Backup*-i dhe rikthimi i të dhënave, përmes zbatimit të një strategjie të dokumentuar për *backup*-in dhe rikuperimin e të dhënave në rast humbjeje ose dështimi të Sistemit, si dhe testimit periodik të procedurave të rikthimit;

e) Menaxhimi i incidenteve të sigurisë, duke ndjekur procedurat për raportimin, verifikimin dhe trajtimin e incidenteve, në përputhje me legjislacionin në fuqi.

Neni 21

Platforma *Online Ticketing Service Desk*

1. Platforma elektronike ka për qëllim monitorimin dhe menaxhimin e kërkesave për suport teknik, në lidhje me problematikat e raportuara nga gjykatat për sistemet TIK.

2. Të gjithë nëpunësit IT të gjykatave pajisen me llogari individuale, me qëllim raportimin e problematikave në platformën https://helpdesk.klgj.al.

3. Struktura TIK në Këshill krijon llogarinë e përdoruesit pas marrjes së kërkesës zyrtare nga gjykata për emërimin e nëpunësit IT, së cilës i bashkëlidhet urdhri i emërimit, dhe mbi këtë bazë mundëson aksesin në platformën.

4. Struktura TIK në Këshill mbyll llogarinë e përdoruesit pas marrjes së kërkesës zyrtare me *email* nga gjykata për ndërprerjen e marrëdhënieve të punës së nëpunësit IT, së cilës i bashkëlidhet urdhri për përfundimin e marrëdhënieve financiare.

5. Në përshkrimin e problematikës, nëpunësi IT i gjykatës përcakton shkallën e prioritetit, tipin e problemit dhe mund të bashkëngjisë materiale ndihmëse për të lehtësuar trajtimin e çështjes nga Këshilli.

6. Çdo komunikim që lidhet me detyrën dokumentohet përmes komenteve përkatëse, të cilat përfshihen në raportin mujor të shërbimit. Komentet nuk mund të modifikohen pas kalimit të pesë minutave nga momenti i publikimit të tyre në platformë.

7. Platforma mundëson vënien në dijeni të eprorëve të gjykatave përmes funksionit "*tag*", të cilët njoftohen automatikisht nëpërmjet *email*-it.

8. Çdo nëpunës IT i gjykatës ka akses për të krijuar, korrigjuar dhe parë detyra vetëm për gjykatën ku ushtron detyrën.

9. Platforma mundëson përcaktimin e statusit të detyrës dhe arkivimin e të gjitha kërkesave për suport IT.

10. Platforma mundëson gjenerimin e raporteve në formatet *PDF* dhe *Excel*.

Neni 22

Periodiciteti i raportimit mbi gjendjen e infrastrukturës TIK

1. Kërkesat për mbikëqyrjen e infrastrukturës TIK në gjykata monitorohen çdo ditë nga struktura përgjegjëse e IT-së pranë gjykatës.

2. Rastet e mosfunksionimit vërtetohen me procesverbal, duke përfshirë datën, orën, burimet e të dhënave të konstatuara, llojin e aktivitetit dhe konkluzionet për mosfunksionimin.

3. Çdo tre muaj, struktura përgjegjëse e IT-së përgatit një raport monitorimi me gjetje dhe konkluzione, i cili protokollohet në zyrën e protokollit të institucionit ku është emëruar. Raporti përfshin seksione të veçanta për çdo aktivitet të monitoruar, rezultatet e arritura dhe rekomandimet për veprimet e ardhshme.

4. Në fund të çdo viti, struktura përgjegjëse e IT-së në gjykata përgatit një raport përmbledhës monitorimi mbi gjendjen aktuale të infrastrukturës TIK dhe informon Këshillin.

5. Raporti vjetor mbi zbatimin e kësaj rregulloreje, si dhe çdo problematikë që lidhet me sigurinë e bazës së të dhënave, i dërgohet Departamentit të Administrimit të Gjykatave dhe Teknologjisë së Informacionit.

6. Pas vlerësimit të raporteve të gjykatave, Këshilli ka detyrimin çdo vit të analizojë gjendjen aktuale të infrastrukturës së gjykatave dhe të propozojë masa për zgjidhjen e problematikave të raportuara.

7. Të dhënat e raportuara duhet të ruhen dhe mbrohen në mënyrë të sigurt për të garantuar konfidencialitetin dhe integritetin e tyre.

8. Këshilli merr masat e nevojshme për të siguruar zbatimin e detyrave të pikës 6, në përputhje me aktet ligjore në fuqi.

9. Këshilli ka të drejtën të verifikojë edhe nga afër infrastrukturën TIK të gjykatave dhe të Sistemit të Menaxhimit të Çështjeve.

10. Këshilli monitoron dhe mbikëqyr përdorimin e Sistemit të Menaxhimit të Çështjeve në gjykata për të siguruar saktësinë dhe sigurinë e të dhënave, si dhe mbrojtjen e të dhënave personale.

11. Këshilli ofron asistencë teknike për gjykatat, lidhur me përdorimin e sistemit elektronik.

12. Monitorimi i infrastrukturave TIK dhe i Sistemit të Menaxhimit të Çështjeve mund të kryhet në distancë ose *onsite*.

13. Këshilli organizon trajnime të rregullta për stafin e gjykatës mbi praktikat e sigurisë së informacionit dhe mbikëqyrjen e infrastrukturës së sistemit, për të rritur ndërgjegjësimin mbi rreziqet dhe rolin e tyre në mbrojtjen e informacionit të gjykatës.

KREU IV
POLITIKAT DHE PROCEDURAT PËR SIGURINË E INFRASTRUKTURËS TIK

Neni 23
Menaxhimi i aseteve

1. Gjykatat kanë detyrimin të identifikojnë asetet dhe të përcaktojnë nivelin e duhur të mbrojtjes për secilin prej tyre. Çdo aset dokumentohet dhe mirëmbahet përmes një inventari të përditësuar rregullisht, në varësi të rëndësisë dhe vlerës së asetit.

2. Të gjitha asetet duhet të kenë një zotërues të përcaktuar, i cili është përgjegjës për kontrollin, zhvillimin, përdorimin, mirëmbajtjen dhe sigurinë e aseteve brenda juridiksionit të tij.

3. Punonjësit janë të detyruar të kthejnë asetet që kanë përdorur pas përfundimit të marrëdhënies së punës ose ndryshimit të pozicionit të tyre.

4. Asetet e informacionit përfshijnë, por nuk kufizohen në:

a) *Software*;

b) *Hardware*, përfshirë pajisjet e lëvizshme (laptop, tablet, etj.);

c) Të gjitha asetet e tjera të informacionit, si bazat e të dhënave, kontratat dhe marrëveshjet, dokumentacioni i sistemit, manualet e përdoruesit, materialet e trajnimit, procedurat operative dhe mbështetëse, planet për vazhdimësinë e punës dhe informacionet e arkivuara.

5. Kthimi i aseteve pas përfundimit të punësimit të punonjësve duhet të dokumentohet sipas procedurave standarde, të cilat sigurojnë:

a) Kthimin e dokumenteve, të dhënave dhe manualeve në çdo format, përfshirë edhe asetet e informacionit të zhvilluara ose të përgatitura nga punonjësi, ose kontraktuesi gjatë kryerjes së detyrave;

b) Kthimin e pajisjeve kompjuterike, *software*-ve dhe pajisjeve të lëvizshme si loptop, tablet etj.;

c) Verifikimin e aseteve të kthyera kundrejt inventarëve të aseteve;

ç) Kompensimin për asetet që nuk janë kthyer, bazuar në kriteret për amortizimin dhe vlerën e zëvendësimit të llojit të asetit të humbur;

d) Identifikimin e pajisjeve të aksesit, kartave dhe çelësave të pakthyer, për të parandaluar aksesin e paautorizuar dhe për të siguruar mbrojtjen e të dhënave.

Neni 24
Klasifikimi i informacionit

1. Klasifikimi i informacionit përfshin:

a) Sigurimin që informacioni të ketë nivelin e duhur të mbrojtjes;

b) Ofrimin e mundësisë për punonjësit që të identifikojnë dhe të zbatojnë kërkesat ligjore, lidhur me trajtimin dhe shpërndarjen e informacionit në një mënyrë të thjeshtë, të standardizuar dhe të sigurt ligjërisht.

Neni 25

Autentifikimi dhe autorizimi

1. Kontrolli i aksesit dhe krijimi i llogarive të përdoruesve kryhet duke u caktuar privilegjet përkatëse.

2. Përdoruesve në gjykata dhe në Këshill u sigurohet akses vetëm në infrastrukturat që shërbejnë sistemin e menaxhimit të çështjeve dhe për të cilat ata janë autorizuar në mënyrë specifike.

3. Aksesi në këto infrastruktura kontrollohet në të gjitha nivelet: perimetri i rrjetit, kompjuterat individualë, ruterë, porta, *workstation*-et dhe serverat.

Neni 26

Procedura e regjistrimit dhe çregjistrimit të përdoruesit

1. Platforma e Sistemit të Menaxhimit të Çështjeve është e bazuar në *web* dhe përdor minimalisht mekanizmat standard të hyrjes me emër përdoruesi dhe fjalëkalim.

2. Përdoruesit kategorizohen sipas roleve dhe grupet e përdoruesve përcaktohen në përputhje me rolet e tyre.

3. Platforma mund të integrohet me Direktorinë Aktive (DA) për identifikimin e përdoruesve të brendshëm të gjykatave dhe zbatimin e rregullave të DA-së. Kjo përfshin informacionin:

a) emër dhe mbiemër i përdoruesit;

b) fjalëkalim fillestar, i cili më pas personalizohet nga përdoruesi;

c) roli i përdoruesit në sistem.

4. Grupet e përdoruesve dhe rolet e tyre janë të përcaktuara në aneksin I të kësaj rregulloreje.

5. Përdoruesit e jashtëm që kërkojnë vetëm informacion nuk kanë nevojë për llogari, pasi mund të aksesojnë informacionin e shfaqur në portalet përkatëse sipas nivelit të gjykatës.

6. Regjistrimi dhe çregjistrimi i përdoruesve për gjykatat bëhet me miratimin e kryetarit të gjykatës.

7. Struktura TIK është përgjegjëse për menaxhimin e aksesit në rrjet dhe bazën e të dhënave dhe zbaton procedurat e mëposhtme.

a) Regjistrimi:

i. miratimi për hapjen e llogarisë së përdoruesit;

ii. sigurimi i kërkesës për akses në rrjetin e gjykatave;

iii. verifikimi që kërkesat për akses përputhen me përgjegjësitë e punës së përdoruesit;

iv. informimi i përdoruesit mbi kushtet e aksesit;

v. kufizimi i aksesit sipas privilegjeve të roleve.

b) Çregjistrimi:

i. shqyrtimi i të drejtave të aksesit kur një përdorues largohet ose ndryshon detyrën ose përgjegjësitë, në përputhje me vendimet e Këshillit të Gjykatës;

ii. shqyrtimi i të drejtave të aksesit në rast ristrukturimi të institucionit.

8. Dhënia dhe revokimi i kredencialeve të autentifikimit kontrollohet sipas procedurave të përcaktuara në aneksin III.

9. Struktura TIK ka autoritetin për lëshimin dhe rivendosjen e fjalëkalimeve:

a) Kredencialet e përdoruesve të rinj jepen vetëm pas miratimit të Kryetarit të Gjykatës;

b) Fjalëkalimet nuk ruhen në formë të pambrojtur;

c) Fjalëkalimet fillestare të sistemeve që vendosen në gjykata duhet të ndryshohen sipas standardeve;

ç) Revokimi i kredencialeve të autentifikimit bëhet sipas procedurave të miratuara.

10. Fjalëkalimet duhet të jenë komplekse dhe të përputhen me standardet e sigurisë të cituara më poshtë.

11. Përdoruesit janë përgjegjës të ruajnë konfidencialitetin e informacionit të autentifikimit,

të mos e ndajnë me të tjerët, të shmangin regjistrimin e tij dhe përdorimin e të njëjtit fjalëkalim për llogari të tjera.

Neni 27

Standardi mbi krijimin e llogarive të përdoruesve

1. Emri i përdoruesit dhe fjalëkalimi për përdoruesit e thjeshtë:

a) Kërkesat e sigurisë për identifikimin e përdoruesve:

i. çdo përdorues pajiset me një identifikues personal, i cili përbëhet nga emri_mbiemri i përdoruesit;

ii. përdoruesi është përgjegjës për përdorimin dhe keqpërdorimin e identifikuesit të tij, në përputhje me rolin përkatës;

iii. identifikuesi dhe roli i përdoruesit përcaktohen nga eprori përkatës, i cili mund të delegojë këtë përgjegjësi për krijimin e përdoruesve të rinj në sistem;

iv. njësia e burimeve njerëzore informon menjëherë administratorin e sistemit dhe Drejtorinë e IT për çdo përdorues të ri, ndryshim pozicioni ose largim përdoruesi, së bashku me rolin përkatës në sistem;

v. çdo përdorues pajiset me një fjalëkalim unik për të aksesuar sistemin sipas rolit të tij. Përdoruesi është përgjegjës për përdorimin dhe keqpërdorimin e fjalëkalimit të tij;

vi. me pajisjen e përdoruesit me fjalëkalim, ai është përgjegjës për çdo veprim që kryhet në sistem nga llogaria e tij.

b) Kërkesat e sigurisë për fjalëkalimin e përdoruesve:

i. fjalëkalimi duhet të ketë të paktën 10 karaktere dhe të përmbajë kombinim germash kapitale dhe të vogla, një numër (0–9) dhe një simbol (p.sh. *, $, %, #, &);

ii. fjalëkalimi nuk duhet të përmbajë emrin e përdoruesit ose pjesë të tij më shumë se 3 karaktere;

iii. fjalëkalimet ndryshohen çdo 90 ditë. Çdo fjalëkalim i dyshuar për kompromet im duhet të raportuar dhe ndryshuar menjëherë;

iv. nuk mund të përdoren dhjetë fjalëkalimet e fundit;

v. fjalëkalimet nuk duhet të komunikohen tek të tjerët, të shkruhen në letër ose të ruhen në skedarë, ose bazë të dhënash në kompjuter;

vi. fjalëkalimet duhet të jenë të maskuara dhe nuk printohen ose përfshihen në raporte ose log-e.

Neni 28

Emri i përdoruesit dhe fjalëkalimi për administratorin e sistemeve TIK në gjykata

1. Emri i përdoruesit dhe fjalëkalimi i administratorit të sistemeve TIK i komunikohet vetëm këtij personi nga administratorët e sistemit. Pas marrjes së fjalëkalimit, përdoruesi duhet ta ndryshojë menjëherë. Në rast leje vjetore, sëmundjeje apo arsye të tjera madhore, emri i përdoruesit dhe fjalëkalimi dorëzohet tek administratorët e sistemit me anë të një procesverbali.

2. Në rast largimi nga detyra, administratorët e sistemeve plotësojnë formularin e miratuar mbi dorëzimin e detyrës sipas aneksit II, bashkëlidhur kësaj rregulloreje.

3. Kërkesat e sigurisë për fjalëkalimin e administratorit të bazës së të dhënave:

i. fjalëkalimi duhet të ketë të paktën 10 karaktere;

ii. fjalëkalimi duhet të përmbajë një kombinim të germave kapitale dhe të vogla, numrave dhe karaktereve speciale si ($!, @, # etj.);

iii. fjalëkalimet ndryshohen çdo 30 ditë. Në rast kompromet imi, ato duhet të ndryshohen menjëherë;

iv. fjalëkalimi nuk mund t'u komunikohet të tjerëve, të shkruhet në letër ose të ruhet në skedarë, ose baza të dhënash;

v. fjalëkalimi duhet të jetë i maskuar dhe nuk printohet ose përfshihet në raporte ose log-e;

vi. fjalëkalimi nuk duhet të përmbajë të dhëna personale ose emrin e institucionit/gjykatës;

vii. nuk lejohen karakteret: \, ~ ose <;

viii. nuk lejohen hapësira ("*space*") ose tabela ("*tab*");

ix. administratorët e sistemit duhet të forcojnë sistemet për të penguar tentativa të dyshimta, duke përdorur metoda për të zbutur sulmet me fjalëkalim "forcë brutale";

x. sistemet nuk duhet të lejojnë hyrjen e përdoruesit pa një fjalëkalim;

xi. administratorët e sistemit duhet të rivendosin fjalëkalimet për llogaritë e përdoruesve ose të kërkojnë nga përdoruesit ndryshimin e tyre kur përdorimi i një fjalëkalimi të njëjtë rrezikon akses të paautorizuar.

Neni 29

Emri i përdoruesit dhe fjalëkalimi për administratorin e infrastrukturave fizike TIK në gjykata

1. Infrastruktura fizike TIK përbën komponentin kryesor ku ruhen dhe përpunohen të dhënat e sistemit. Performanca dhe siguria e sistemit mund të ndikohen në mënyrë të konsiderueshme nga administrimi dhe optimizimi i serverave të bazës së të dhënave, ndaj këta duhet të mirëmbahen dhe monitorohen rregullisht.

2. Emri i përdoruesit dhe fjalëkalimi përkatës i komunikohen vetëm administratorit të autorizuar nga administratorët e sistemit.

3. Kërkesat e sigurisë për fjalëkalimin e administratorit të sistemit të menaxhimit të bazës së të dhënave përfshijnë:

i. fjalëkalimi duhet të përmbajë minimumi 10 karaktere;

ii. fjalëkalimi duhet të përmbajë kombinim të germave të mëdha dhe të vogla, numrave dhe karaktereve speciale (si !, @, #, etj.);

iii. fjalëkalimi duhet të ndryshohet çdo 30 ditë. Në rast të kompromet imit të fjalëkalimit, ai duhet të ndryshohet menjëherë;

iv. fjalëkalimi nuk duhet t'u komunikohet personave të tjerë, të shkruhet në letër ose të ruhet në skedarë apo baza të dhënash në kompjuter;

v. fjalëkalimi duhet të jetë i maskuar dhe nuk duhet të printohet apo të përfshihet në raporte ose në log-e të sistemit.

Neni 30

Autentifikimi

1. Autentifikimi përbën një mekanizëm thelbësor për garantimin e sigurisë së sistemeve të teknologjisë së informacionit dhe komunikimit (TIK), me qëllim parandalimin e aksesit të paautorizuar në sistemet dhe të dhënat e institucionit. Administrimi i informacionit dhe kredencialeve të llogarive të administratorëve duhet të kryhet me masa më të rrepta sigurie në krahasim me llogaritë e përdoruesve të zakonshëm.

2. Në kuadër të menaxhimit të autentifikimit duhet të zbatohen këto rregulla:

a) Të krijohen vetëm llogaritë e përdoruesve që janë të domosdoshme për funksionimin e sistemeve;

b) Për çdo llogari përdoruesi të përcaktohen qartë të drejtat e aksesit, në përputhje me funksionin dhe përgjegjësitë përkatëse;

c) Të krijohen llogari të veçanta për përdoruesit dhe për administratorët e sistemeve, me nivele të ndryshme të drejtash aksesi sipas rolit;

ç) Llogaritë që nuk përdoren të çaktivizohen (*disable*) ose të fshihen në mënyrë të menjëhershme;

d) Llogaritë e paracaktuara, të krijuara gjatë instalimit të sistemeve të fshihen ose të çaktivizohen në rast se nuk janë të nevojshme për funksionimin e sistemit.

Neni 31
Kontrolli i aksesit

1. Të përdoret *firewall* (mur zjarri) për mbrojtjen e serverave të bazës së të dhënave nga aksesi i paautorizuar.
2. Aksesi në serverat e bazës së të dhënave të kufizohet vetëm për terminalet e autorizuara ose për terminalet që i përkasin të njëjtit segment rrjeti.
3. Aksesi në skedarët e konfigurimit të bazës së të dhënave lejohet vetëm për administratorët e sistemit.
4. Aksesi në skedarët e shkrimeve (*script*-eve) të kufizohet vetëm për administratorët.
5. Të kryhet kontroll i rregullt i të drejtave të aksesit në skedarët e konfigurimit të bazës së të dhënave.

Neni 32
Përdorimi i memorieve të jashtme

1. Lidhja e memorieve të jashtme me serverin e bazës së të dhënave të kufizohet vetëm në rastet e nevojshme dhe të kontrollohet aksesi ndaj tyre.
2. Të ruhen *log*-et për çdo lidhje dhe akses në memoriet e jashtme.
3. Të kryhen rishikime periodike, lidhur me përdorimin e memorieve të jashtme. Këto rishikime duhet të realizohen veçanërisht para implementimit të sistemeve, aplikacioneve ose shërbimeve të reja, si dhe në rastet e ndryshimeve të konsiderueshme.

Neni 33
Siguria operacionale, auditimi dhe regjistrimi

1. Monitorimi dhe regjistrimi i veprimeve të përdoruesve, ndryshimet e konfiguracionit dhe aksese të tjera të ndjekura, si dhe identifikimin e veprimeve të dyshimta ose të paautorizuara, duke mundësuar hetimin e incidenteve të sigurisë.
2. Të zbatohen kontrolle për të kufizuar mundësitë për rrjedhje të informacionit, duke:
a) Analizuar kodet e dëmshme (*malicious code*);
b) Monitoruar përdorimin e burimeve në sistemet e informacionit;
c) Përdorur *software* që konsiderohen të një integriteti të lartë;
ç) Monitoruar në mënyrë të rregullt sistemet e informacionit;
d) Ndarë ambientet e testimit nga ambientet operacionale.

Neni 34
Mbrojta nga programet keqdashëse

1. Të gjitha pajisjet e teknologjisë duhet të jenë të mbrojtura nga programet keqdashëse, përfshirë viruset e kompjuterave.
2. Struktura TIK në gjykata dhe Këshill duhet të mbrojnë rrjetin dhe bazën e të dhënave nga kërcënimet, duke ndërmarrë aktivitete të tilla; si:
a) Përdorimi i *software*-ve për skanimin, zbulimin dhe mbrojtjen nga kërcënimet ndaj rrjetit dhe bazës së të dhënave;
b) Ndalimi i përdorimit të *software*-ve të paautorizuar;
c) Kontrolli i dokumenteve, përfshirë bashkëlidhjet e postës elektronike dhe shkarkimet e

skedarëve nga interneti, për *malware* përpara përdorimit.

Neni 35
Ruajtja dytësore e të dhënave (*Backup*)

1. I gjithë informacioni në bazën e të dhënave duhet të ruhet në një ambient dytësor, në mënyrë që të garantohet rikthimi i të dhënave në gjendjen e mëparshme në rast humbjeje ose shkatërrimi. Struktura TIK në gjykata dhe Këshill duhet të përcaktojë dhe dokumentojë procesin e *backup*-it dhe *recovery*-it.

2. Dokumentimi i proceseve të *backup*-it dhe *recovery*-it përfshin:

a) Llojin e informacionit që do të përfshihet në procesin e *backup*-it;

b) Frekuencën në të cilën do të kryhet *backup*-i;

c) Menaxhimin e medias së *backup*-it (periudha e mbajtjes dhe modeli i cikleve);

ç) Metodat për kryerjen dhe vlerësimin e *backup*-it;

d) Metodat për *recovery* të informacionit.

3. Procedurat e *backup*-it dhe *recovery*-it duhet të testohen rregullisht për të verifikuar funksionimin e tyre. Procedura e *backup*-it duhet të rishikohet çdo vit.

Neni 36
Kryerja e *backup*-it

1. *Backup*-i i të dhënave në sistem kryhet sipas frekuencës së përcaktuar, si më poshtë:

a) Kryhet *backup* çdo ditë nga e hëna në të premte në orën 17:30;

b) Kryhet *full backup* çdo javë, ditën e premte në orën 20:00;

c) Kryhet *full backup* çdo muaj, ditën e fundit të muajit në orën 20:00. Pas kryerjes së *backup*-it mujor fshihen manualisht *backup*-et javore;

ç) Kryhet *full backup* në fund të çdo viti;

d) Pas kryerjes së *backup*-it vjetor ruhen 12 *backup*-et e fundit mujore dhe fshihen manualisht *backup*-et mujore të vitit të kaluar;

dh) Në çdo moment duhet të ekzistojnë *backup*-et vjetore dhe 12 *backup*-et e fundit mujore.

Neni 37
Emërtimi i *backup*-it

1. Të gjitha *backup*-et emërtohen duke përfshirë informacionin e mëposhtëm:

a) emërtimi i sistemit;

b) data: dita, muaji dhe viti.

Neni 38
Gjurma/*log*-et dhe monitorimi

1. Struktura TIK në Këshill siguron gjenerimin, ruajtjen dhe menaxhimin e *log*-eve për të monitoruar aktivitetin e sistemeve.

2. Sektori përgjegjës përcakton nivelin e detajimit të *log*-eve bazuar në vlerën dhe ndjeshmërinë e aseteve të informacionit, rëndësinë kritike të sistemit dhe burimet e nevojshme për të shqyrtuar dhe analizuar.

3. *Log*-et përfshijnë informacionin e mëposhtëm:

a) përshkrimin e ngjarjes së ndodhur;

b) kohën e ngjarjes;

c) rëndësinë e ngjarjes.

4. Nevojitet sinkronizimi i orës në të gjitha sistemet përkatëse të përpunimit të informacionit

brenda gjykatës dhe në Këshill, ose në *domain* sigurie, me një burim të vetëm kohe referimi.

Neni 39
Kontrollet e sigurisë detektuese dhe evidentuese

1. Veprimet që lenë gjurmë në sistemin e menaxhimit të çështjeve janë:
a) Krijimi, leximi, modifikimi ose fshirja e informacionit konfidencial, duke përfshirë informacionin konfidencial mbi autentifikimin;
b) Krijimi, ndryshimi ose fshirja e informacionit që nuk përfshihet në pikën "a".

Neni 40
Kufizimi i instalimit të *software*-ve

1. Instalimi i pakontrolluar i *software*-ve në pajisjet kompjuterike mund të shkaktojë dobësi që sjellin rrjedhje të informacionit, humbje të integritetit, incidente sigurie ose shkelje të të drejtave të pronësisë intelektuale. Përdoruesit duhet të komunikojnë me strukturën TIK për autorizimin e çdo instalimi.
2. Struktura TIK krijon një listë të *software*-ve të lejuara për instalim, e cila miratohet nga Departamenti i Administrimit të Gjykatave dhe Teknologjisë së Informacionit. Çdo *software* jashtë listës duhet të kalojë proces rishikimi dhe miratimi, dhe instalimi bëhet vetëm nga personi IT i autorizuar.

Neni 41
Siguria dhe mbrojtja e pajisjeve

1. Të gjitha pajisjet e gjykatave duhet të mbrohen fizikisht nga kërcënimet e sigurisë dhe rreziqet e ambientit.
2. Masat mbrojtëse për pajisjet kompjuterike përfshijnë:
a) Ambienti i përdorimit të pajisjeve të ketë temperaturën dhe lagështinë e duhur;
b) Sigurimi i mbrojtjes nga rrufetë dhe rreziqet mjedisore, si: uji, pluhuri dhe rrezet e diellit;
c) Informimi i punonjësve mbi praktikat e sigurisë në vendin e punës;
ç) Ruajtja e pajisjeve që nuk përdoren në vende të sigurta dhe të mbyllura për të parandaluar aksesin e paautorizuar.
3. Pajisjet duhet të mbrohen nga ndërprerjet e furnizimit me energji elektrike dhe nga dështimet e shërbimeve mbështetëse, dhe të mirëmbahen në mënyrë të vazhdueshme për të garantuar disponueshmërinë dhe integritetin e tyre.
4. Kompjuterat personalë (PC) nuk duhet të vendosen në vende ku personat e paautorizuar mund të shohin informacionet; instalimi ose transferimi i tyre bëhet vetëm nga personel i trajnuar dhe i autorizuar.
5. Pajisjet që mirëmbahen ose riparohen nga kontraktues duhet të mbrohen sipas ndjeshmërisë së informacionit dhe vlerës së pajisjes. Struktura TIK përcakton nëse riparimi ose mirëmbajtja mund të kryhet jashtë ambienteve të institucionit.
6. Para asgjësimit ose ripërdorimit të pajisjeve elektronike që përmbajnë të dhëna, struktura IT duhet të verifikojë që çdo të dhënë sensitive dhe program i licencuar të fshihet ose mbishkruhet në mënyrë të sigurt, duke dokumentuar procesin me një procesverbal.

Neni 42
Siguria e ambienteve të punës

1. Përdoruesit duhet të mbrojnë hapësirën e tyre të punës dhe pajisjet sa herë nuk janë

prezent, duke:

a) Siguruar dokumentet dhe pajisjet e lëvizshme në një vend të kyçur;

b) Bllokuar PC-në me fjalëkalim;

c) Fikur kompjuterat në fund të ditës;

ç) Mbyllur dyert dhe dritaret;

d) Kontrolluar printerët për të siguruar që nuk ka informacione sensitive të lëna në pritje.

Neni 43

Siguria e dhomës së serverave

1. Çdo strukturë TIK duhet të zbatojë vendimin nr. 14, datë 19.12.2022, "Për standardet e ndërtimit dhe administrimit të dhomës së serverave për sistemin e drejtësisë", miratuar nga Bordi drejtues i QTI-së.

2. Çdo strukturë TIK duhet të zbatojë VKM-në nr. 538, datë 8.7.2020, "Për përcaktimin e kritereve dhe të procedurave për garantimin e rregullit e të sigurisë në gjykata dhe prokurori".

Neni 44

Kontrolli dhe menaxhimi i rrjetit

1. Struktura TIK në gjykata implementon kontrolle të sigurisë për infrastrukturën e rrjetit dhe sistemet e menaxhimit të sigurisë në rrjetin e brendshëm të gjykatës, me qëllim sigurimin e mbrojtjes së informacionit. Kontrollet përfshijnë asetet e rrjetit që kanë nevojë për mbrojtje, duke përfshirë:

a) Informacionin e ruajtur, si përmbajtja në *cache* dhe skedarët e përkohshëm;

b) Infrastrukturën e rrjetit;

c) Informacionin mbi konfigurimet e rrjetit, përfshirë konfigurimin e pajisjeve, kontrollet e aksesit, rutimin dhe fjalëkalimet;

ç) Informacionin mbi menaxhimin e rrjetit.

Neni 45

Kontrolli i konfigurimeve

1. Për të ruajtur integritetin e rrjetit të brendshëm të gjykatës, Struktura TIK në gjykata është përgjegjëse për menaxhimin dhe kontrollin e ndryshimeve në informacionin e konfigurimeve të pajisjeve të rrjetit, duke përfshirë:

a) Të dhënat e konfigurimit;

b) Kontrollin e aksesit;

c) Afatet dhe parametrat e fjalëkalimeve.

Neni 46

Menaxhimi i incidenteve të sigurisë së informacionit

1. Një incident i sigurisë së informacionit është një ngjarje ose një seri ngjarjesh të padëshiruara apo të papritura që kërcënojnë privatësinë ose sigurinë e informacionit. Këto incidente përfshijnë çdo përdorim, zbulim, akses, ruajtje ose asgjësim të informacionit, qoftë aksidentale ose të qëllimshme, pa autorizimin e personit përgjegjës.

2. Për të garantuar një përgjigje të shpejtë, efektive dhe të rregullt ndaj incidenteve, përgjegjësitë për menaxhimin e tyre ndahen dhe krijohen procedura të qarta.

3. Llojet e mundshme të incidenteve të sigurisë që raportohen përfshijnë:

a) Përpjekjet e përsëritura të aksesit të paautorizuar;

b) Mohimi i shërbimit;
c) Zbulimi i kodeve të dëmshme;
ç) Defektet e sistemeve;
d) Shpërndarja e kredencialeve të përdoruesve.

4. Dyshimet për incidente të sigurisë së informacionit raportohen menjëherë te Struktura TIK në gjykatën përkatëse dhe në Këshill. Struktura vlerëson çdo ngjarje të sigurisë së informacionit dhe vendos nëse duhet të klasifikohet si incident i sigurisë.

5. Njohuritë e fituara nga analiza dhe zgjidhja e incidenteve duhet të përdoren për të minimizuar gjasat dhe ndikimin e incidenteve të ardhshme.

Neni 47
Incidentet e sigurisë në Teknologjinë e Informacionit (TI)

1. Incidentet e sigurisë TIK shkaktohen nga *malware*, të cilat janë programe ose sekuenca kodi që vetëinstalohen në aplikacione të tjera dhe mund të dëmtojnë sistemin. Këto mund të shkaktojnë ndryshime të paautorizuara në të dhëna ose dëmtime të hard diskut. Shenjat e infektimit përfshijnë, veprime të kompjuterit pa komandën e përdoruesit, ndryshime në ekran, zhdukjen ose lëvizjen e karaktereve dhe të tjera.

2. Veprimet e përdoruesit në rast dyshimi për *malware*:
a) Ndërprerja menjëherë e punës në kompjuter;
b) Shkëputja e kabullit të rrjetit nga kompjuteri;
c) Sigurimi që kompjuteri dhe *software*-i nuk përdoren nga persona të tjerë;
ç) Raportimi i incidentit tek struktura TIK e institucionit, e cila mban një procesverbal për çdo veprim të dyshuar si pjesë e incidentit.

3. Pas raportimit, incidenti duhet të trajtohet në mënyrë efikase dhe të shpejtë deri në zgjidhjen e tij. Kategorizimi i incidenteve kibernetike ndihmon në planifikimin e veprimeve, duke siguruar respektimin e afateve të raportimit në bazë të rëndësisë së infrastrukturës së informacionit.

4. Çdo strukturë TIK në gjykata zbaton rregulloren për kategoritë e incidenteve kibernetike dhe formatin e elementeve të raportit, sipas udhëzimeve të miratuara nga AKSK-ja.

5. Çdo çështje që lidhet me privatësinë ose sigurinë e informacionit i drejtohet Departamentit të Administrimit të Gjykatave dhe Teknologjisë së Informacionit.

Neni 48
Privatësia dhe përmbajtja e të dhënave

1. Siguria e mjeteve të monitorimit duhet të garantojë mbrojtjen e privatësisë dhe integritetin e të dhënave.

2. Kjo përfshin mbrojtjen e të dhënave personale të përdoruesve, të dhënave të transmetuara në rrjet dhe të dhënave të ruajtura në mjetet e monitorimit, në përputhje me aktet ligjore për mbrojtjen e të dhënave personale, dokumentin elektronik dhe komunikimet elektronike në Republikën e Shqipërisë.

KREU V
DISPOZITA E FUNDIT

Neni 49
Hyrja në fuqi

Kjo rregullore publikohet në faqen zyrtare të internetit të Këshillit të Lartë Gjyqësor dhe hyn

në fuqi në datën e botimit në Fletoren Zyrtare.

ANEKS I
TË DREJTAT E PËRDORUESVE TË SISTEMIT TË MENAXHIMIT TË ÇËSHTJEVE

Tabela 1: Hierarkia e roleve sipas modelit RBAC

Nivel	Roli	Funksioni kryesor	Statusi
1	KLGJ	Pronari i sistemit dhe përcaktimi i politikave	Pronari i Sistemit
2	Kryetari i gjykatës	Administrim institucional	Administrator institucional
3	Zëvendëskryetari	Mbështetje drejtimi	Administrator delegues
4	Administratori /arkitekti/zhvilluesi i sistemit (IT)	Administrim teknik	Administrator teknik
5	Gjyqtari	Administrim i çështjes	Administrator i çështjes
6	Kancelari i gjykatës	Administrim administrativ	Administrator administrativ
7	Kryesekretari	Koordinim administrativ	Mbikëqyrje operative
8	Sekretari gjyqësor	Mbështetje procedurale	Mbështetje operative
9	Sekretari regjistrues	Regjistrim dosjesh	Regjistrim
10	Ndihmësmagjistrati	Mbështetje juridike	Mbështetje
11	Këshilltari ligjor	Mbështetje juridike	Mbështetje
12	Ndihmësi ligjor	Mbështetje juridike	Mbështetje
13	Nëpunësi i financë/buxhetit	Funksione financiare	Akses i kufizuar
14	Stafi administrativ (HR, arkiv, media etj.)	Mbështetje institucionale	Akses i kufizuar
15	Përdoruesi i gjykatës	Përdorim i kufizuar	Përdorues
16	Inspektori/audituesi	Monitorim	Kontroll
17	ILD	Auditim dhe mbikëqyrje	Kontroll

Tabela 2: Të drejtat sipas roleve (RBAC)

Roli	Administrim sistemi	Administrim çështje	Konfigurim teknik	Monitorim	Akses në dokumente
KLGJ	✔	✖	✖	✔	sipas rolit
Kryetari i gjykatës	✔	✔	✖	✔	✔
Zëvendëskryetari	✔	✔	✖	✔	✔
IT (admin/arkitekt/zhvillues)	✔	✖	✔	✔	i kufizuar
Gjyqtari	✖	✔	✖	✖	✔ i plotë
Kancelari	✔	✔	✖	✔	✔
Kryesekretari	✔	✔	✖	✔	✔
Sekretari gjyqësor	✖	✔	✖	✖	✔
Sekretari regjistrues	✖	regjistrim	✖	✖	i kufizuar
Ndihmësmagjistrati	✖	✔	✖	✖	✔ sipas autorizimit
Këshilltari ligjor	✖	✔	✖	✖	✔
Ndihmësi ligjor	✖	✔	✖	✖	i kufizuar
Financë/buxheti	✖	✖	✖	✖	sipas modulit
Stafi administrativ	✖	✖	✖	✖	minimal
Përdoruesi i gjykatës	✖	✖	✖	✖	minimal
Inspektori/Audituesi	✖	✖	✖	✔	vetëm lexim
ILD	✖	✖	✖	✔	Akses i pa

					kufizuar vetëm lexim

Tabela 3: Matrica sipas modelit RACI

Aktiviteti	R (përgjegjës për zbatim)	A (përgjegjës për vendimmarrje)	C (konsultohet)	I (informohet)
Politikat dhe rregullat IT	KLGJ	KLGJ	IT / Gjykatat	Përdoruesit
Administrimi teknik i sistemit	IT i gjykatës	Kryetari i gjykatës	KLGJ	Administrata
Menaxhimi i çështjeve	Gjyqtari	Kryetari i gjykatës	Kancelari	IT
Administrimi administrativ	Kancelari/kryesekretar	Kryetari	IT	KLGJ
Regjistrimi i çështjeve	Sekretar regjistrues	Kryetari	Gjyqtari	IT
Monitorimi dhe auditimi	ILD/audites	KLGJ	IT	Gjykata

RBAC: *Role-Based Access Control* – Kontrolli i aksesit bazuar në role (p.sh. gjyqtari sheh vetëm dosjet e veta).

RACI: *Responsible* (Përgjegjës), *Accountable* (Përgjegjës final), *Consulted* (Këshilluar), *Informed* (Informuar).

Matrica RACI: Tabelë që tregon kush bën çfarë në një proces/projekt (R/A/C/I për çdo detyrë).

**** Administratori teknik i sistemit në gjykatë dokumenton çdo ndërhyrje ose veprim teknik të kryer mbi sistemet dhe infrastrukturën TIK. Çdo ndryshim që ndikon në konfigurimin, sigurinë ose funksionimin e sistemit realizohet vetëm pas konfirmimit paraprak nga titullari i institucionit ose autoriteti i deleguar prej tij.*

ANEKSI II
Formulari i miratuar mbi dorëzimin e detyrës

REPUBLIKA E SHQIPËRISË

FORMULAR DORËZIMI NË PËRFUNDIM TË MARRËDHËNIES SË PUNËS SË NËPUNËSIT IT

Gjykata _____

_____.____.202X

1. **Serveri ICMIS/ ARKIT**
   - IP
   - Computer name:
   - Username i serverit Administrator:
   - Password i serverit:
   - A ka të tjerë usera me profil Administrator?
   - Nëse ka të citohen në material.
   - Listo të gjithë userat aktive që përdorin sistemin ICMIS/ ARKIT (kryegjyqtar, gjyqtare, kancelarë, kryesekretarë, sekretare regjistruese, sekretare gjyqësore, arkiviste) .

   Ku realizohet back-up i sistemit, përcakto HDD dhe Cloud (google drive nëse ka).
   - Username i SQL Server:
   - Passwordi:

   Lidhja VPN (Nëse ka)
   - (Për çfarë shërben dhe përdoren apo jo pajisjet shtesë fizike për lidhjen e VPN)
   - Username:
   - Passwordi:

2. **Servera të tjerë (nëse ka):**
   - IP :
   - Computer name:
   - Username i serverit Administrator:
   - Password i serverit:

- A ka të tjerë usera me profil Administrator?
- Nëse ka të shkruhen.
- Listo të gjithë userat aktivë që përdorin sistemin ICMIS/ ARKIT (kryegjyqtar, gjyqtare, kancelare, kryesekretare, sekretare regjistruese, sekretare gjyqësore, arkiviste) .

3. **Sistemi Audio i instaluar në Gjykatë:**
   - Si realizohet back-upi, çfarë lidhje përdoren për back-upin, përcakto vendndodhjen e ruajtjes së regjistrimeve audio që nga viti 2012 e deri më tani. Në cilin vend ruhet tjetër back-upi i regjistrimeve audio?
   - Në kompjuterët e secilës salle a gjenden regjistrimet të kryera lokalisht në secilën prej sallave që nga 2012 e deri më tani?
   - Po në serverin e ICMIS a gjenden regjistrimet audio të gjithë sallave? Nëse po përcakto periudhën që nga 2012 e deri më tani.
   - Në cilin vend ruhet tjetër back-upi i regjistrimeve audio, të tilla si HDD të jashtëm apo vendndodhje tjetër jashtë gjykate?
   - Cilat janë pajisjet shtesë nëpërmjet se cilave realizohet ruajtja e të dhënave (Laptop, dhe HDD) programi përkatës, kush janë kredencialet e njësisë kompjuterike (computer name, IP, user, password etj), të programit nëpërmjet së cilës raportohen, bëhet back-upi?
   - Cilat janë raportet e audios që raportohen në KLGJ apo USAID apo vende të tjera?
   - Përcakto konktaktet përkatëse për KLGJ:

Programi i regjistrimit të mbledhjeve të gjyqtarëve i instaluar (nëse ka)
   - Çfarë pajisje përdoret? A është në funksionim ky program? Sa mikrofona ka? Përfshin edhe regjistrim video?
   - A janë të ruajtura diku në program apo në kompjuter mbledhjet e mëparshme të bëra që nga instalimi e deri më tani?

4. **Serveri i kamerave**
   - IP:
   - Computer name:
   - User name i serverit :
   - Password:

Programi i kontrollit te kamerave:
   - Username:
   - Password:
   - Usera të tjerë nëse ka:
   - Username:
   - Password:

   - **Përcakto sa kamera janë të lidhura aktualisht.** Sa janë në gjendje pune? Sa janë të defektuara nëse ka të tilla, dhe deri në sa kamera mund të lidhen në pajisjen ekzistuese.

- **Në çfarë diapazoni kohor mund të mbajë regjistrime serveri i kamerave** duke u nisur nga dita aktuale? Përcakto procedurën e ruajtjes së një kopjeje në DVD.
- **A janë të regjistruara edhe me zë të gjitha filmimet e bëra nëpërmjet kamerave?**
- A është mundësia e ruajtjes në një vendndodhje tjetër në HDD apo server apo diku në rrjet?
- Kontaktet e subjektit që referohen për ndonjë problematikë.

A ka sistem tjetër kamerash përveç atij të sipërcituar?

5. **Pc e kartave të Aksesit apo i sistemit të sigurisë**
   - IP:
   - Computer name:
   - Username i pc:
   - Passwordi:

   Programi i Kartave të aksesit
   - Username:
   - Passwordi:
   - Usera të tjerë nëse ka të krijuar me kredencialet e veta:
   - Username:
   - Password:

   Kontakt të subjektit për probleme në software apo për pajisje me kartë aksesi në raste se defektohen ose shtohet personel.

6. **Lidhja e Internetit; pajisja që përdoret; si mundësohet lidhja (lidhje ADSL; fibër optike etj); subjekti që ofron shërbimin; të përcaktohet nëse përdoret IP statike dhe cila është; të përcaktohet gateaway dhe DNS-ja.**
   - **Equipment type MODEL:**
   - Username i pajisjes:
   - Passwordi i pajisjes:
   - Passwordi i Wireless:
   - IP:
   - Kontak të subjektit që ofron shërbimin në raste problemesh me lidhjen e internetit.

   Të dhëna për pajisje audio (nëse ka):

   Equipment type MODEL:

   - IP:
   - Username i pajisjes:
   - Passwordi i pajisjes:
   - Passwordi i Wireless:
   - Ku është i pozicionuar si vendndodhje.

7. **E-mail Zyrtar (GOV):**

- Kontakti me KLGJ në lidhje me hapjen dhe mbylljen e adresave zyrtare nën domain gjykata.gov.al.
- Grupet e krijuara cilat janë dhe të përcaktohen administratorët.
- Mënyrat e konfigurimit të e-mailit në Outlook, smart phone Android dhe Iphone, manualet përkatëse.

8. **Portali i gjykatës:**
   Web: www.gjykata.gov.al

   - User name i administratorit të faqes për sa i përket rifreskimit të të dhënave në portal:
   - Passwordi:
   - Cilat janë rubrikat që rifreskon informacionet administratori i faqes (Specialisti i IT).
   - Në cilën rubrikë bëhen shpalljet për njoftimet e seancave për palët në gjykim? Përcakto rubrikën.
   - Po shpalljet e ardhura nga subjekte të ndryshme p.sh. ato përmbarimore etj. në cilën rubrike afishohen?
   - Si funksionon formulari i aplikimit për marrjen e dokumenteve nga Arkiva e Gjykatës së Shkallës së Parë të Juridiksionit të Përgjithshëm në portal?
   - Ku shkarkohen këto kërkesa që bëhen nëpërmjet portalit?
   - A ka ndonjë adresë të hapur lidhur me këtë? Nëse po, të përcaktohen kredencialet.
   - Kush i akseson dhe i proceson këto kërkesa dhe nëpërmjet çfarë aplikacioni?
   - Çfarë llogarie përdoret nëse përdoret një e tillë?

9. **Centrali telefonik (nëse ka).**
   - Kompjuter name:
   - IP:
   - Username:
   - Password:
   - Konfigurimet e tjera
   - Përcakto mënyrat e konfigurimit të një numri të ri.
   - Sa është kapaciteti për këtë central?
   - Kush është subjekti që e ka instaluar në raste nëse do të nevojitet kontakti me to të probleme madhore?

10. **Pajisja Kioska (nëse ka)**
    - IP:
    - Username:
    - Password:
    - Çfarë fushash paraqiten në filtrimin a mund të paraqitet edhe fusha të tjera kërkimi? Nëse po përcakto mënyrën si bëhet ky ndryshim.

11. **Pajisja e video konferencave (nëse ka),** listimi i pajisjeve që mundësojnë lidhjen me gjykata të tjera ndërkombëtare.
    - IP statike që përdoren, parametrat që konfigurohen në secilën prej pajisjeve (kamera, boxi audio, etj.) dhe kredencialet që përdoren.

12. **Useri i Microsoft teams (nëse ka) për planifikimin dhe organizimin e sesioneve online që aplikohet për seancat gjyqësore apo edhe me pjesëmarrje të treta**
    - Username:
      Password:
    - (Platforma elektronike e krijuar për lidhje audiovizive për zhvillimin e seancave në distancë me pajisje elektronike, manualet përkatëse).
    - Përcakto nëse ka pajisje shtesë për të realizuar këto lidhje përveç kompjuterave të sallave të gjykimit.
    - A ka manuale përdorimi për administratorin që krijon takimin online dhe për palët pjesëmarrëse në gjykim?

13. **Faqja e Gjykatës në Facebook dhe në Instagram, kredencialet përkatëse (nëse ka).**

14. Shërbimi i fotokopjeve:
    - Sa fotokopje janë sjellë nga subjekti?
    - Sa janë në gjendje punë dhe ku përdoren?
    - Kontaktet përkatëse me firmën. Sa është numri i printimeve deri më tani? Me çfarë komande gjenerohet ky raport?
    - Çfarë praktike ndiqet nëse i kalohet ndonjë dokument financës apo jo lidhur me shërbimet e kryera në periudha kohore të ndryshme?

15. Përcakto sistemet e alarmit në gjykatë të tillë si:
    - Sensorët për zjarrin, metal detektori, sensorët e lëvizjes etj.

16. A janë gjyqtarët pjesë e ndonjë platforme tjetër që nuk është e listuar më lart?
    Nëse po kredencialet e tyre i zotërojnë vetë ata apo janë të ruajtuara diku?
    - Nëse ka gjëra të tjera, platforma të tjera që nuk janë listuar më sipër, të shënohen.

Për çdo detyrë e cila vijon të jetë në proces realizimi në momentin e largimit nga puna, të detajohet statusi mbi të cilin ndodhet dhe të shoqërohet me dokumentacionin përkatës.

Plotësuar nga	**Dorëzuar**
Specialisti IT në proces shkëputje nga ky pozicion	Specialisti IT në Detyrë

ANEKSI III

FORMULARI PËR PËRCAKTIMIN E AKSESIT NË SISTEMIN KOMPJUTERIK

SEKSIONI A (Plotësohet nga Drejtoria e Burimeve Njerëzore)

HAPJE LLOGARIE ☐ MBYLLJE LLOGARIE ☐

A1. TË DHËNA IDENTIFIKUESE TË PUNONJËSIT

EMRI														
MBIEMRI														
NUMRI TELEFONIT														

A2. POZICIONI I PUNËS

DEPARTAMENTI														
DREJTORIA														
SEKTORI														
NUMRI I VENDIMIT TË PUNËSIMIT														

PLOTËSOI: _____

MIRATOI:_____

SEKSIONI B (Plotësohet nga eprori i drejtpërdrejtë)

_____

Llogaria e e_mail-it													
Llogaria e e_mail-it të përbashkët të Drejtorisë/Sektor													
Llogaria të sistemeve të tjera													

PLOTËSOI: _____ **MIRATOI:**

SEKSIONI C (Plotësohet nga Drejtoria IT)

Llogaria	e krijuar	e mbyllur
në e_mail		
në e_mail-it të përbashkët të Drejtorisë/Sektor		
në Active Directory		
në Microsoft Teams		
në M-files		
në Kartës së Aksesit		

PLOTËSOI: _____

MIRATOI:_____