RREGULLORE
"PËR PËRDORIMIN E TEKNOLOGJISË SË INFORMACIONIT NË KOLEGJIN E POSAÇËM TË APELIMIT"

Miratuar nga Mbledhja e Gjyqtarëve me vendimin nr. 110, datë 21.12.2022

Neni 1
Qëllimi dhe fusha e zbatimit

1. Kjo rregullore ka për qëllim përcaktimin e rregullave për organizimin dhe funksionimin e sistemeve të teknologjisë së informacionit në Kolegjin e Posaçëm të Apelimit, në përputhje me ligjin nr. 84/2016 "Për rivlerësimin kalimtar të gjyqtarëve dhe prokurorëve në Republikën e Shqipërisë", me rregulloren "Për veprimtarinë e Kolegjit të Posaçëm të Apelimit të Gjykatës Kushtetuese", të ndryshuar, si dhe me rregulloret e tjera në fuqi.
2. Përcaktimi i rregullave, si dhe zbatimi i tyre, synon uljen e rrezikut operacional që mund të shkaktohet nga keqpërdorimi i sistemeve të TIK-ut, si edhe të ruajë integritetin e këtyre sistemeve në mbështetjen e veprimtarisë së përdoruesve.
3. Kjo rregullore zbatohet për të gjithë përdoruesit e teknologjisë së informacionit dhe për të gjitha pajisjet kompjuterike e elektronike pronë e Kolegjit të Posaçëm të Apelimit.

Neni 2
Baza ligjore

Këto rregulla nxirren në zbatim:
- të ligjit nr. 84 /2016 "Për rivlerësimin kalimtar të gjyqtarëve dhe prokurorëve në Republikën e Shqipërisë";
- të ligjit nr. 9887, datë 10.3.2008, "Për mbrojtjen e të dhënave personale", të ndryshuar;
- të ligjit nr. 10273, datë 29.4.2010, "Për dokumentin elektronik";
- të ligjit nr. 9918, datë 19.5.2008, "Për komunikimet elektronike në Republikën e Shqipërisë", të ndryshuar;
- të rregullores "Për veprimtarinë e Kolegjit të Posaçëm të Apelimit të Gjykatës Kushtetuese";
- të rregullores "Për organizimin e funksionimin e personelit dhe administrimin e dokumentacionit të Kolegjit të Posaçëm të Apelimit";
- të rregullores "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale";
- të rregullores "Për përdorimin e postës elektronike në Administratën Publike".

Neni 3
Përdoruesit

Përdoruesit e teknologjisë së informacionit në Kolegjin e Posaçëm të Apelimit janë:
1. Përdorues të brendshëm:
a) gjyqtarët e Kolegjit të Posaçëm të Apelimit;
b) këshilltarët e Njësisë së Shërbimit Ligjor;

c) punonjësit administrativë të Kolegjit të Posaçëm të Apelimit;

ç) përfaqësuesit e ONM-së.

2. Përdorues të jashtëm, të cilët i referohen çdo personi të autorizuar si përdorues për qëllime pune.

Neni 4
Përkufizime

1. **Teknologjitë e Informacionit dhe Komunikimit** janë *hardware* dhe *software* (kompjuterë, telefona celularë, internet, sistem operativ, programe kompjuterike, aplikacione celular etj.) që mundësojnë mbledhjen, ruajtjen, përdorimin dhe transmetimin e të dhënave.
2. **Aftësitë TIK** janë aftësi që mundësojnë përdorimin efektiv të mjeteve të zakonshme ose të përparuara të programeve kompjuterike (kompjuterë, programe kompjuterike, internet).
3. **Specialistët e TIK-ut (ose IT)** janë punonjës për të cilët puna kryesore është zhvillimi i TIK-ut, operimi ose mirëmbajtja e sistemeve apo aplikacioneve të TIK-ut.
4. **Kompjuteri** përfshin kompjuterët personalë, tabletat apo pajisje të tjera portative, si: *Smartphone* apo *Personal Digital Assistants* (PDAs).
5. **Aksesi në internet** i referohet një lidhjeje të jashtme në internet përmes një kompanie që operon si Ofrues i Shërbimit në Internet (Internet Service Provider – ISP).
6. ***Broadband*** janë teknologjitë apo lidhjet të cilat mundësojnë transmetimin e shpejtë të të dhënave, si p.sh.: dokumente, regjistrime audio/video, filma, lojëra, video-konferenca nëpërmjet një rrjeti interneti (për shembull: ADSL, lidhje kabllor, UMTS, lidhje optike, VDSL, fibër optike etj.).
7. ***Website*** është faqja e internetit, një dokument me *HyperText*, e cila mund të përmbajë tekst, lidhje link, video, foto, materiale të tjera të dokumenteve elektronike.
8. **Server** është kompjuteri me parametra fizikë specifikë, i cili shërben për ruajtjen e të dhënave, instalimin e aplikacioneve të ndryshme, si dhe për të vendosur, nëpërmjet tij, ndarjet e privilegjeve për përdoruesit.
9. ***Firewall*** është pajisje apo program kompjuterik që është i konfiguruar për të kontrolluar trafikun që kalon nëpër rrjet, duke e lejuar apo bllokuar atë, në bazë të një grupi rregullash.
10. **IM** (*Instant Messaging*) janë teknologji që japin mundësinë e komunikimit me tekst në kohë reale midis dy apo më shumë bashkëbiseduesve në rrjet të mbyllur apo internet.
11. **UserID/Username** është varg karakteresh që identifikon në mënyrë unike një përdorues në një sistem apo rrjet kompjuterik.
12. **Password** është fjalëkalim, kod sekret i një përdoruesi, që nuk duhet të njihet nga përdoruesit e tjerë, dhe që i përdorur bashkë me *UserID*, lejon aksesimin e një sistemi kompjuterik.
13. **Logim** është procesi nëpërmjet të cilit një përdorues fiton akses në një sistem apo rrjet kompjuterik, i cili zakonisht nënkupton futjen e një *UserID*-je (*username*) dhe një fjalëkalimi (*password*-i).
14. **Postë elektronike** konsiderohet çdo mesazh në formën e tekstit, tingullit apo imazhit të dërguar nëpërmjet rrjetit publik të komunikimeve, i cili mund të ruhet në rrjet ose në pajisjen fundore të marrësit derisa marrësi ta marrë atë.
15. ***Domain Name*** është pjesa e tekstit që vjen pas shenjës "**@**" në një adresë *e-mail*. Meqenëse interneti funksionon në bazë të adresave IP (katër numra), çdo *domain name* ka korrespondentin numerik unik.
16. **Mail Client** është program në kompjuterët e përdoruesve që bën të mundur dërgimin, marrjen dhe organizimin e *e-mail*-it.

17. ***Reply to all*** është mundësi e ofruar nga *mail client*, për të kthyer përgjigje me *e-mail* jo vetëm dërguesit, por të gjithë përdoruesve të adresave të *e-mail*-ve të përfshira në *e-mail*-in fillestar të dërguesit, në "To" apo "CC".
18. ***Recall*** është mundësi e ofruar nga *mail client* për të tërhequr mbrapsht një *e-mail* të dërguar.
19. **Antivirus*/Antispyware*** janë programe të cilat bëjnë të mundur kontrollimin, identifikimin, eliminimin e programeve kompjuterike të dëmshme, të instaluara në kompjuterë (virus, trojan etj.).
20. ***Spam*** janë mesazhe elektronike, *e-mail*, me përmbajtje komerciale apo informuese jozyrtare, zakonisht të nisura nga *software* në mënyrë automatike.
21. ***Attachment*** është një *file* në kompjuter i cili dërgohet me anë të një *e-mail*-i, mund të jetë dokument (*PDF, Word, Excel, Access* etj.), audio (format *FTR, MP3* etj.), foto (*jpeg, img* etj.), një sërë *e-mail*-esh të tjera, video apo çdo lloj elementi elektronik.
22. ***Chat*** është program i cili lejon komunikimin në kohë reale midis dy apo më shumë përdoruesve në internet.
23. **Të dhëna personale** janë çdo informacion në lidhje me punonjësin e administratës publike, i identifikuar ose i identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social.

Neni 5
Administrimi i pajisjeve elektronike dhe i programeve kompjuterike

1. Administrimi i pajisjeve elektronike dhe i programeve kompjuterike, të cilat janë pronë e Kolegjit kryhet në të njëjtën mënyrë si ai i aktiveve të tjera, në përputhje me legjislacionin në fuqi për menaxhimin e aktiveve dhe me rregulloret e miratuara në Kolegjin e Posaçëm të Apelimit.
2. Përdorimi i rrjetit dhe i pajisjeve kompjuterike menaxhohet nga specialistët e Teknologjisë së Informacionit dhe Komunikimit (në vijim "specialisti IT"), në varësi të Drejtorisë Ekonomike dhe Shërbimeve Mbështetëse.
3. Drejtoria Ekonomike dhe e Shërbimeve Mbështetëse është përgjegjëse për kujdesin, sigurinë dhe mirëmbajtjen e pajisjeve të teknologjisë së informacionit, *hardware*, *software* dhe *platformave TIK*, me përjashtim të rasteve kur kryhen dëmtime nga punonjësi që i ka në përdorim apo individi i paautorizuar për të përdorur këtë pajisje.

Neni 6
Pajisja me mjete IT

1. Përdoruesi i brendshëm ka të drejtën të pajisjet me mjete të teknologjisë së informacionit për të ushtruar detyrën e tij.
2. Përdoruesi i brendshëm shfrytëzon të gjitha burimet e informacionit nëpërmjet teknikave dhe metodave të IT-së, sipas detyrës që ushtron.
3. Për shpërndarjen e pajisjeve elektronike dhe programeve kompjuterike, si dhe për grumbullimin e tyre, në rast të largimit të personit nga detyra, specialistëve IT u paraqitet një kërkesë nga specialisti i burimeve njerëzore ku specifikohen:
   a) të dhënat individuale,;

b) zyra e caktuar për ushtrimin e detyrës;
c) nevojat specifike.

4. Në rast largimi nga puna të punonjësit përkatës, për dorëzimin e pajisjeve kompjuterike, zbatohen rregullat e përcaktuara në rregulloret në fuqi për dorëzimin e detyrës.

Neni 7
Rregullat e përdorimit të pajisjeve elektronike për përdoruesit

1. Përdoruesi përdor pajisjet elektronike dhe programet kompjuterike pronë e Kolegjit, vetëm për kryerjen e detyrave të përcaktuara në rregulloret në fuqi, të miratuara në Kolegjin e Posaçëm të Apelimit.
2. Përdoruesi i sistemit elektronik duhet të zotërojë njohuritë e nevojshme dhe të ketë aftësitë e mjaftueshme teknike për përdorimin e pajisjeve të IT-së deri në masën që i shërben ushtrimit të detyrës.
3. Në asnjë rast, përdoruesi nuk duhet të ndërhyjë fizikisht, me/pa nismën e tij, në mjetet e IT-së. Nëse gjatë shfrytëzimit të tyre, përdoruesi ka hasur në probleme të natyrës teknike, ai duhet të njoftojë menjëherë specialistët e IT-së për asistencë teknike.
4. Në asnjë rast, përdoruesi nuk duhet të mbajë në monitor të dhëna të detyrës funksionale në prani të një personi të paautorizuar, si brenda institucionit, edhe jashtë tij.
5. Nuk lejohet për asnjë përdorues hapja ose shkarkimi nga USB-ja, disketa, CD-ja ose DVD-ja i materialeve të ndryshme pa u kontrolluar më parë këto pajisje për *virus*.
6. Përdoruesi është përgjegjës për ruajtjen e informacionit që disponon nga keqpërdorimi, aksesi i paautorizuar ose dëmtimi i qëllimshëm gjatë procesit të punës.
7. Përdoruesi nuk duhet të shkarkojë në asnjë rast të mundshëm në kompjuterin/at që ka në përdorim, programe kompjuterike nga interneti apo ndonjë burim tjetër, pa miratimin paraprak të specialistëve të IT-së.
8. Në rast se përdoruesi konstaton se ka pasur shkelje të sigurisë së sistemit informatik, kompjuterit ose kompjuteri është infektuar me virus apo programe të tjera, që cenojnë integritetin e sistemit, ai duhet të lajmërojë menjëherë specialistët e IT-së.
9. Përdoruesi nuk duhet të krijojë, ruajë, transmetojë në mjetet e IT-së, apo nëpërmjet tyre, materiale që kanë karakter fyes, shpifës, racist, diskriminues, denigrues, seksual, pornografik apo që përbëjnë vepër penale. Përdoruesi i cili bie në kontakt apo merr materiale të tilla, duhet të njoftojë menjëherë specialistët e IT-së.
10. Nuk lejohet përdorimi i mjeteve të IT-së pronë e Kolegjit, për arsye personale dhe përfitimi.
11. Përdoruesit e jashtëm mbikëqyren nga specialisti IT për të garantuar zbatimin e kësaj rregulloreje.
12. Në përfundim të punës, të gjithë përdoruesit duhet të fikin pajisjet elektronike që kanë në përdorim.
13. Përdoruesi duhet të kryejë procedurën e hyrjes duke përdorur fjalëkalimin personal në fillim të aksesit të tij. Fjalëkalimet ndryshohen në mënyrë periodike *(çdo tre muaj).*
14. Fjalëkalimet nuk duhet të ndahen me persona të tjerë brenda apo jashtë Kolegjit.
15. Fjalëkalimet duhet të respektojnë kriteret e sigurisë sipas rastit *(numër karakteresh, lloj karakteresh apo fjala e vendosur).*

16. Në një sistem kompjuterik pronë e Kolegjit, do të instalohen vetëm ato programe që i nevojiten përdoruesit për kryerjen e detyrës funksionale. Në çdo kompjuter instalohet sistemi operativ dhe paketa *Office*. Për çdo *software* shtesë duhet të merret miratimi nga Kryetari i Kolegjit / Sekretari i Përgjithshëm dhe të mirëmbahet nga specialistët e IT-së.
17. Programet kompjuterike të përdorura në Kolegj, duhet të jenë të pajisura me licencë që lejon instalimin dhe përdorimin e tij.

Neni 8
Përdorimi i postës elektronike

1. Adresa zyrtare e postës elektronike dhe mesazhet elektronike nuk janë pronë individuale e përdoruesve të brendshëm. Është i ndaluar përdorimi i adresës së postës elektronike zyrtare për qëllime private.
2. Administrimi i postës elektronike zyrtare kryhet në përputhje me standardet e vendosura nga Agjencia Kombëtare për Shërbimin e Informacionit (AKSHI), në përputhje me legjislacionin në fuqi për teknologjinë e informacionit dhe organizimin dhe funksionimin e kësaj agjencie.
3. Çdo përdoruesi të brendshëm i caktohet një adresë poste elektronike me qëllim që të përdoret ekskluzivisht për nevoja të punës. Adresa është individuale dhe përdorimi i saj është i mbrojtur me fjalëkalimin që zotërohet vetëm nga punonjësi. Fjalëkalimi i postës elektronike skadon automatikisht pas 90 ditëve, si protokoll sigurie nga AKSHI.
4. Posta elektronike mund të përdoret edhe nëpërmjet telefonave *mobile*, pas instalimit nga specialisët e IT-së.
5. Punonjësit e kanë të ndaluar të ridrejtojnë (*forward*) në mënyrë automatike mesazhet elektronike të marra nëpërmjet rrjetit të institucionit tek adresa e postës elektronike private.
6. Institucioni rezervon të drejtën për të monitoruar, rishikuar, ndërprerë apo publikuar çdo mesazh të hartuar, dërguar apo marrë nëpërmjet rrjetit. Monitorimi, rishikimi dhe ndërprerja e mesazheve mund të kryhet nga specialisti IT me ndihmën e *software*-ëve për filtrimin e përmbajtjes.
7. Institucioni rezervon të drejtën që të ndryshojë rrugën, destinacionin apo të pezullojë dërgimin e mesazheve në varësi të rrethanave, duke njoftuar menjëherë dërguesin. Kjo përfshin, por nuk është e kufizuar me:
   a) pengimin e dërgimit, alternimin, arkivimin apo fshirjen e dokumenteve të bashkëngjitura (*attachment*) ose kodin e mesazhit atëherë kur dyshohet se përbën rrezik për funksionimin e sistemit kompjuterik;
   b) eliminimin e përmbajtjeve shtesë në mesazhe (p.sh., muzikë), që konsiderohen pa vlerë për institucionin dhe zënë vend në memorie;
   c) pengimin e dërgimit apo arkivimin e mesazheve me përmbajtje të dyshimtë, mesazheve që përmbajnë dokumente të bashkëlidhura (*attachment*) me emra dhe prapashtesa të dyshimta;
   ç) pengimin e dërgimit apo arkivimin e mesazheve të formuluara në gjuhë fyese;
   d) pengimin e dërgimit apo arkivimin e mesazheve që konsiderohen si jozyrtarë apo/ose reklama komerciale (*spam*).

8. Në rast largimi nga puna të punonjësit:
   a) specialisti i burimeve njerëzore informon specialistin IT, kur një punonjës e lë punën ose afati i tij i punësimit mbaron për çdo lloj arsyeje. Specialisti IT bën arkivimin e korrespondencës elektronike të llogarisë dhe heqjen e të drejtave të aksesimit në infrastrukturën TIK, përpara se punonjësi të largohet fizikisht nga ambienti i punës;
   b) nëse kërkohet nga eprori direkt i punonjësit, aktivizohet një mesazh automatik (*Out of Office*) për të njoftuar të gjithë dërguesit për pamundësinë e komunikimit të mëtejshëm si pasojë e largimit nga puna;
   c) pas përfundimit të një afati 3-mujor nga dita e largimit, bëhet fshirja përfundimtare e adresës së postës elektronike zyrtare.

Neni 9
Rregulla mbi përdorimin e shërbimit të internetit

1. Specialisti IT, në ushtrimin e detyrës:
   a) siguron që për çdo kompjuter të lidhur në internet, të aplikohet *firewall* dhe kontrollet e sigurisë së aksesit të konfigurohen në mënyrë të tillë që asnjë aplikacion i brendshëm të mos hapë porta alternative komunikimi me internetin;
   b) siguron aksesin në internet dhe pajisjen me fjalëkalime individuale të punonjësve;
   c) vendos opsionet e sistemit dhe kompjuterëve lokalë në mënyrë që përdoruesit mos të kenë të drejta të plota mbi *software*-ët e sigurisë dhe antiviruset.
2. Përdoruesit e brendshëm duhet të tregohen të kujdesshëm gjatë aksesimit të shërbimeve *online*, me qëllim:
   a) mirëpërdorimin e burimeve të internetit;
   b) minimizimin e kërkimit të paautorizuar nga eprori i drejtpërdrejtë, në internet;
   c) ruajtjen e tërësisë se informacionit në internet;
   ç) të mos çaktivizojnë opsionet e *antivirusit* për materialet që shkarkohen nga interneti.
3. Kryetari i Kolegjit mund të autorizojë:
   a) bllokimin e faqeve të caktuara të internetit që gjykohen si të pavlefshme për punën (p.sh., me përmbajtje të paligjshme, diskriminuese apo pornografike);
   b) monitorimin e faqeve të internetit dhe listës se tyre, të hapura në mënyrë kronologjike nga punonjësi;
   c) shkarkimin e *software*-ëve nga interneti;
   ç) përdorimin e faqeve me pagesë për informacion të vlefshëm për qëllime pune.

Neni 10
Garantimi i kushteve të sigurisë për teknologjinë e informacionit

1. Specialisti IT duhet të njoftohet për të gjitha incidentet që ndikojnë në besueshmërinë, integritetin ose aksesin e të dhënave apo pajisjeve të teknologjisë së informacionit pronë e Kolegjit.
2. Vjedhja, hyrja e paautorizuar, infektimi nga viruset janë raste për të cilat parashikohen masa disiplinore, sipas legjislacionit në fuqi. Në rast se konstatohet që pajisjet e teknologjisë së

informacionit janë dëmtuar në çfarëdo mënyre, specialisti IT mban një procesverbal i cili përmban:

a) të dhënat e personit që e ka në ngarkim pajisjen;

b) datën, orën dhe vendin e konstatimit të dëmtimit, mosfunksionimit, defektit;

c) llojin, specifikat, shkaqet e problematikës;

ç) mendimin për procedimin e mëtejshëm;

d) emrat dhe firmat e specialistëve që ekzaminuan rastin;

dh) emrin dhe firmën e personit që ka në ngarkim pajisjen.

3. Në rastin kur konstatohet një problematikë e cila nuk mund të riparohet, pajisjet elektronike kthehen në zyrën e specialistit IT, që të asgjësohen në përputhje me legjislacion në fuqi. Nuk mund të jepet pajisje e re nëse nuk kthehen pajisjet e dëmtuara.
4. Për të krijuar kushte optimale të sigurisë, specialisti IT përpunon sistemin e fjalëkalimeve për:

a) platformën *e-albania outlook;*

b) shërbimin e *sharefolder*-it;

c) kompjuterët në përdorim;

ç) shërbimin *wireless*;

5. Për shkaqe sigurie, specialisti IT nuk mund të transmetojë dhe të marrë përmes telefonit, fjalëkalimet për të gjitha shërbimet e teknologjisë së informacionit, për të cilat është i nevojshëm përdorimi i fjalëkalimit. Specialisti IT pajis të gjithë punonjësit me një fjalëkalim fillestar, i cili është i detyruar nga përdoruesit të ndryshohet në hyrjen e parë.
6. Fjalëkalimi për logimin në serverët e institucionit administrohet vetëm nga specialistët IT të institucionit.
7. Logimi në server kryhet vetëm për qëllime pune dhe në çdo rast, në përfundim të procesit të punës, specialisti IT raporton nëpërmjet *e-mail*-it te Sekretari i Përgjithshëm dhe tek eprori direkt mbi arsyen e logimit në server. Kur logimi kryhet për nevoja të një punonjësi të caktuar, në *e-mail*-in e raportimit vendoset për dijeni edhe punonjësi përkatës.
8. Punonjësit e teknologjisë së informacionit aplikojnë politikat e sigurisë së *firewall*-it të rrjetit *network.*
9. Ambientet në të cilat do të përpunohen të dhënat elektronike personale, duhet të mbrohen nga masa organizative, fizike dhe teknike që të parandalojnë aksesin e personave të paautorizuar.
10. Në ambientet ku përpunohen të dhëna personale, zbatohen këto masa sigurie:
    a) Ndalohet hyrja e personave të paautorizuar.
    b) Personat që hyjnë në këto ambiente, duhet të jenë të pajisur me autorizimin përkatës, të shoqërohen nga punonjës i sigurisë.
    c) Ambientet e hyrje-daljes survejohen me kamera gjatë 24 orëve.
    ç) Vendosen pajisje dhe sisteme të sigurimit elektronik (sisteme alarmi, telekamera, sensorë të tymit, lagështirës dhe temperaturës në ambientet përkatëse etj.), si dhe sinjalizues në rastet kur detektohet ndryshim i parametrave referues të përcaktuar.
11. Specialisti IT, në ushtrimin e detyrës:
    a) zbaton legjislacionin në fuqi për mbrojtjen e të dhënave personale dhe çdo legjislacion tjetër të nevojshëm për realizimin e detyrave të tij;

b) siguron që konfigurimi i të gjitha pajisjeve të sigurisë është një e dhënë konfidenciale vetëm për personelin teknik. I njëjti rregull vlen edhe kur stafi teknik është i jashtëm;
c) ndërmerr kështillime, që mund të përfshijnë trajnime intensive rreth përdorimit të pajisjeve.

Neni 11
Përditësimi i faqes zyrtare në internet të Kolegjit të Posaçëm të Apelimit

1. Përditësimi i faqes zyrtare kryhet nga specialisti IT sa herë që kërkohet nga Kryetari i Kolegjit, Sekretari i Përgjithshëm, Drejtori i Drejtorisë së Menaxhimit të Çështjeve dhe Marrëdhënieve me Median dhe Publikun, Drejtori i Drejtorisë Ekonomike dhe i Shërbimeve Mbështetëse, nga Koordinatori për Mediat dhe Marrëdhëniet me Jashtë.
2. Komunikimi për përditësimin e faqes bëhet nëpërmjet postës elektronike.
3. Përditësimi në Programin e Transparencës në faqen zyrtare në internet, kërkon 2-5 ditë pune.
4. Specialisti i IT-së, për nevoja të përditësimit të faqes zyrtare në internet:
   a) mban kontakt të vazhdueshëm me kompaninë e mirëmbajtjes së faqes dhe raporton vazhdimisht, në përputhje me parashikimet e kontratës;
   b) mban komunikim të vazhdueshëm me AKSH-in me qëllim informimi dhe mbikëqyrjeje të serverit të hostit pranë datacenterit të AKSHI-t;
   c) ruan një *back-up* të plotë të faqes së internetit në një HDD të jashtëm çdo ditë të premte, për arsye sigurie.

Neni 12
Përdorimi i TIK-ut në sallën e gjyqit

1. Sistemi elektronik audio-video në Kolegjin e Posaçëm të Apelimit, përdoret vetëm për kryerjen e funksionit të përcaktuar në këtë rregullore. Ky sistem përdoret vetëm nga specialisti IT. Në rast nevoje, për qëllim mirëmbajtjeje ose riparimi, sistemi do të aksesohet edhe nga persona të tretë të specializuar, nën mbikëqyrjen e personelit të institucionit. Sistemi është në funksion vetëm të seancave gjyqësore, për regjistrimin, arkivimin, si edhe për monitorimin e seancave për efekt sigurie dhe nuk mund të përdoret për asnjë qëllim tjetër.
2. Specialisti IT regjistron dhe dokumenton, nëpërmjet mbajtjes së një procesverbali, çdo modifikim të nevojshëm në rast gabimi, defekti apo incidenti në sistemin audio-video.
3. Përdorimi i sistemit kryhet nga specialisti IT sipas detyrave të përcaktuara në përshkrimin e punës, në zbatim të rregullores "Për organizimin e funksionimin e personelit dhe administrimin e dokumentacionit të Kolegjit të Posaçëm të Apelimit".
4. Personeli i autorizuar IT mirëmban infrastrukturën e sistemit dhe kryen kontrollet e nevojshme teknike. Për çdo gabim, defekt apo incident në sistemin elektronik audio-video, njoftohet personeli i kualifikuar dhe i autorizuar, i cili kryen evidentimin dhe riparimin përkatës.
5. Kur specialisti IT i ngarkuar për përdorimin e sistemit audio-video ndryshon vendin e punës ose largohet nga puna, ai humbet të drejtën e aksesimit që lidhet me detyrën e mëparshme.

6. Specialisti IT aktivizon sistemin FTR sipas kalendarit të seancave gjyqësore, që të funksionojë paralelisht me sistemin "audio-video". Vënia në punë e sistemit elektronik "audio-video", bëhet sipas kalendarit të zhvillimit të seancave gjyqësore.
7. Personat përgjegjës (specialisti IT dhe sekretarja gjyqësore) që kryejnë regjistrimin e seancave gjyqësore, ndërpresin regjistrimin kur seanca mbaron, ndërpritet, ose trupi gjykues e kërkon një gjë të tillë.
8. Kopje nga arkivi i seancave gjyqësore në formatin "audio", nxirren nga specialisti IT me kërkesë të sekretarisë gjyqësore, në dijeni të eprorit të drejtpërdrejtë dhe Sekretarit të Përgjithshëm
9. Kopje nga arkivi i seancave gjyqësore në formatin "video", nxirren nga specialisti IT vetëm me urdhër të Kryetarit të Kolegjit.

Neni 13
Dhoma e serverëve

1. Në ambientet e vendndodhjes së serverëve, lejohet vetëm aksesi i specialistit IT.
2. Në rast nevoje të një personeli të jashtëm, i mirëmbajtjes së sistemit elektronik, ai lejohet të hyjë në këto ambiente i shoqëruar nga specialisti IT dhe plotëson formularin përkatës në përfundim të procesit, formulari përfundimtar është pjesë e aneksit A.
   Ky formular përmban:
   - të dhënat për personin;
   - kohën: datën, orën e hyrjes, orën e daljes;
   - të dhënat për arsyen dhe veprimet që janë kryer;
   - nënshkrimin nga palët.
3. Ndalohet duhani.
4. Ndalohet përdorimi i mjeteve ngrohëse.
5. Mjetet për mbrojtën nga zjarri duhet të jenë gjithmonë në gjendje pune dhe në vende të dukshme.

Neni 14
***Backup*-i të dhënave**

1. Specialisti IT realizon procedurën e *backup*-it në serverët e institucionit. Të dhënave dhe programeve në serverë duhet t'u bëhet *backup* (kopje) në mënyrë periodike, në përputhje me praktikat e zakonshme.
2. Specialisti i Teknologjisë së Informacionit dhe Komunikimit duhet të ketë një kopje dhe një dublikatë të të gjitha të dhënave dhe *software*-ëve që mbahen ose ruhen në kompjuterin qendror (Server 1). Kopja dublikatë ruhet në kompjuterin sekondar (Server 2), në dhomën e serverit
3. Kopjet (*backup*-et) e të dhënave duhet të ruhen në vende të mbrojtura nga zjarri dhe jashtë ambienteve ku mbahen serverët.
4. Kopjet e të dhënave duhet të testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme. Procedurat e rikrijimit (*restore*) të të dhënave duhet të testohen

rregullisht, për t'u siguruar që janë të efektshme dhe që mund të ekzekutohen brenda kohës së lejuar.

5. Çdo punonjës, i asistuar nga specialisti IT, i cili krijon/prodhon dokumente në mënyrë elektronike në pajisjet që disponon, në përmbushje të detyrave të tij, ose kur i merr ato nga çdo burim tjetër (*e-mail*, USB, HDD, CD/DVD etj.) për çështje pune, duhet t'u bëjë dublikim (kopje) atyre, të paktën një herë në tre muaj.
6. Përgjegjësia për realizimin e këtyre dublikimeve, është e secilit punonjës, me qëllim për të mbrojtur të dhënat nga humbjet.

Neni 15
Ruajtja e privatësisë

Për ruajtjen e privatësisë së të dhënave të përdoruesve të brendshëm të Kolegjit të Posaçëm të Apelimit, zbatohen dispozitat e legjislacionit në fuqi për mbrojtjen e të dhënave personale, për dokumentin elektronik, si dhe për komunikimet elektronike, si dhe rregulloret në fuqi të miratuara në Kolegjin e Posaçëm të Apelimit.

Neni 16
Sanksionet

Çdo veprim ose mosveprim në kundërshtim me këtë rregullore, përbën shkelje dhe ndiqet sipas rregullave të përcaktuara në legjislacionin në fuqi.

Neni 17
Hyrja në fuqi

Kjo rregullore hyn në fuqi menjëherë pas miratimit nga Mbledhja e Gjyqtarëve.