



REPUBLIKA E SHQIPËRISË

STRUKTURA E POSAÇME KUNDËR KORRUPSIONIT DHE KRIMIT TË ORGANIZUAR

Nr. 960 Prot.

Tiranë më, 22.12. 2023

URDHËR

Nr. 960, datë 22.12. 2023

“PËR MIRATIMIN E RREGULLORES SË PËRDORIMIT TË POSTËS DHE KOMUNIKIMIT ELEKTRONIK”

Në mbështetje të nenit 148 pika 4 e Kushtetutës së Republikës së Shqipërisë dhe neneve 15, 48 dhe 52 të ligjit nr.95/2016 “Për Organizimin dhe Funksionimin e Institucioneve për të Luftuar Korrupsionin dhe Krimin e Organizuar” dhe nenit 62 të Ligjit nr.97/216 “Për Organizimin dhe Funksionimin e Prokurorisë në Republikën e Shqipërisë”.

URDHËROJ:

1. Miratimin e “Rregullores për Përdorimin e Postës dhe Komunikimit Elektronik” bashkëlidhur.
2. Ngarkohen me zbatimin e këtij urdhri punonjësit e Strukturës së Posaçme kundër Korrupsionit dhe Krimit të Organizuar.

Ky urdhër hyn në fuqi menjëherë.

DREJTUESI I PROKURORISË

ALTIN DUMANI



RREGULLORE
“PËR PËRDORIMIN E POSTËS DHE KOMUNIKIMIT ELEKTRONIK”

KREU I

DISPOZITA TË PËRGJITHSHME

Neni 1

Qëllimi

1. Kjo rregullore ka si qëllim rregullimin e postës dhe komunikimit elektronik të punonjësve të Strukturës së Posaçme kundër Korrupsionit dhe Krimit të Organizuar (këtu e më poshtë referuar si “SPAK”) dhe sigurinë e tyre nga rreziqet e mundshme nga moskujdesi i treguar në përdorimin e postës elektronike, internetit dhe mediave sociale.

Neni 2

Objekti i Rregullores

1. Objektivat e kësaj rregulloreje janë:
 - a. Administrimi dhe përdorimi i rregullt i postës elektronike nga punonjësit e SPAK;
 - b. Vendosja e parimeve të përgjithshme mbi etiken e komunikimit elektronik në institucion dhe me të tretët;
 - c. Siguria e komunikimit elektronik gjatë përdorimit të tij nga punonjësit e SPAK, pavarësisht nëse ky komunikim kryhet brenda ose jashtë orarit zyrtar të punës, dhe nëse gjatë këtij komunikimi do të përdoren pajisje të institucionit ose personale, siç janë telefonat, kompjuterat, PC, laptop, tabletët etj.

Neni 3

Përkufizime

Në këtë rregullore, termat/emërtimet kanë kuptimet e mëposhtme:

1. “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;¹
2. “Domain Name” është pjesa e tekstit që vjen pas shenjës “@” në një adresë email. Meqenëse interneti funksionon në bazë të adresave IP (katër numra) çdo domain name ka korresponduesin numerik unik;
3. “Mail Client” është program në kompjuterat e përdoruesve që bën të mundur dërgimin, marrjen dhe organizimin e email-ve;
4. “Reply to all” është mundësi ofruar nga mail client, për të kthyer email jo vetëm dërguesit por të gjithë adresave email të vendosura në “To” apo “CC”;
5. “Recall” është mundësi e ofruar nga mail client për të tërhequr mbrapsht një email të dërguar;

¹ Shih nenin 3 paragrafi 34 të ligjit nr. 9918, datë 19.5.2008 “Për Komunikimet Elektronike në Republikën e Shqipërisë”.

6. "Antivirus / Antispyware" janë programe të cilat bëjnë të mundur kontrollimin, identifikimin, eliminimin e programeve kompjuterike të dëmshme të instaluar në kompjutera (virus, trojan etj.);
7. "Spam" janë mesazhe elektronike, email, me përmbajtje komerciale apo informuese jozyrtare;
8. "Attachment" është dosje/file në kompjuter i cili dërgohet me ane të një email;
9. "Chat" është program i cili lejon komunikimin në kohë reale midis 2 apo më shumë përdoruesve në internet;²
10. "Të dhëna personale" është çdo informacion në lidhje me punonjësën 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 4

Pajisja me adresë postare elektronike

1. SPAK siguron burimet materiale për përdorimin e postës elektronike me qëllim që të ndihmojë punonjësën për përmbushjen e detyrave institucionale.
2. Të gjithë mesazhet e hartuara dhe/ose dërguara nëpërmjet rrjetit të brendshëm të SPAK dhe/ose rrjeteve qeveritare duhet të jenë në pajtim me ligjin Nr. 9131, datë 8.9.2003 "Për rregullat e etikës në administratën publike" dhe aktet nënligjore të SPAK.³
3. Rrjeti elektronik i brendshëm është pronë e SPAK. Gjithashtu edhe i gjithë informacioni i postuar, hartuar, dërguar dhe/ose marrë në sistemin elektronik të SPAK nga punonjësën ose jo, është pronë e SPAK, duke respektuar parashikimet në Ligjin Nr. 9380, datë 28.04.2005 "Mbi të Drejtën e Autorit".
4. Adresa zyrtare e postës elektronike dhe mesazhet elektronike nuk janë pronë individuale e punonjësve të SPAK por mjet pune për përmbushjen e detyrave funksionale.
5. Për krijimin e adresës zyrtare të postës elektronike, Drejtoria e Burimeve Njerëzore, Dokumentacionit dhe Shërbimeve pranë Prokurorisë së Posaçme dhe/ose Drejtoria e Burimeve Njerëzore pranë Byrosë Kombëtare të Hetimit (këtu e më poshtë referuar si "BKH") për rastet e emërimit të punonjësve pranë saj, njofton Drejtorinë e Teknologjisë së Informacionit (këtu e më poshtë referuar si "DTI") elektronikisht (e-mail) ose me shkresë zyrtare duke bashkëlidhur urdhërin e emërimit, për të kryer procedurat e krijimit të adresës postare elektronike.
6. Çdo punonjësi i caktohet një adresë zyrtare poste elektronike me qëllim që të përdoret ekskluzivisht për nevoja të punës së institucionit. Adresa është individuale dhe përdorimi i saj është i mbrojtur me fjalëkalim që zotërohet vetëm nga punonjësi.
7. Me ndërprerjen e marrëdhënies së punës për çdo shkak apo përfundimin e kontratës së punonjësës, Drejtoria e Burimeve Njerëzore, Dokumentacionit dhe Shërbimeve pranë

² Shih nenin 5 pika 9 i Rregullores nr. 1 datë 16.06.2023 "Për Përdorimin e Postes Elektronike në Administratën Publike".

³ Shih "Rregullat dhe Standartet e Etikës në Prokurorinë e Posaçme kundër Korrupsionit dhe Krimit të Organizuar", miratuar me Urdhërin nr. 640, dt.25.09.2023 dhe "Rregulloren e Disiplinës dhe Kodin e Etikës" të BKH, miratuar me Urdhërin nr. 116, date 28.04.2021 të Drejtuesit të Prokurorisë së Posaçme kundër Korrupsionit dhe Krimit të Organizuar.

Prokurorisë së Posaçme dhe/ose Drejtoria e Burimeve Njerëzore pranë BKH në rastet e punonjësve të saj njofton DTI përpara përfundimit të marrëdhënieve të punës për të kryer procedurat e pezullimit dhe ndalimit të përdorimit të adresës postare elektronike.

Neni 5

Pezullimi dhe ndalimi i përdorimit

1. Punonjësi i DTI-së nis procedurat e nevojshme në lidhje me adresën postare elektronike të përcaktuara si më poshtë:
 - a. Drejtoria e Burimeve Njerëzore, Dokumentacionit dhe Shërbimeve pranë Prokurorisë së Posaçme dhe/ose Drejtoria e Burimeve Njerëzore pranë BKH për rastet e punonjësve të saj, njofton punonjësën që para largimit të tij nga puna të aktivizojë një mesazh automatik (*Out of Office*) për të njoftuar të gjithë dërguesit për pamundësinë e komunikimit të mëtejshëm si pasojë e largimit nga puna. Në rast të pamundësisë për kryerjen e aktivizimit të mesazhit automatik nga vetë punonjësi mund të kërkohej suporti i punonjësit të DTI.
 - b. Aksesit i punonjësit në postën e tij elektronike ndalohet menjëherë pas shkëputjes së marrëdhënieve të punës me institucionin, duke përfshirë këtu të drejtën për të shkarkuar, dërguar, printuar apo rimarrë ndonjë mesazh të vendosur në sistem, pavarësisht nga dërguesi apo marrësi ose rëndësia e mesazhit përveç rasteve të parashikuara ndryshe nga Drejtuesi i Prokurorisë së Posaçme ose Drejtori i BKH për rastet e punonjësve respektiv.
 - c. Pas përfundimit të një afati 3 mujor nga dita e largimit nga puna të punonjësit, Drejtori i DTI-së pas miratimit të Drejtuesit të Prokurorisë së Posaçme ose të Drejtorit të BKH për rastet e punonjësve të saj rishikon arkivën dhe vendos fshirjen përfundimtare të adresës së postës elektronike zyrtare.

KREU II

DETYRAT DHE PËRGJEGJËSITË

Neni 6

Trajtimi i informacionit

1. SPAK trajton dhe vlerëson të gjithë informacionin elektronik si çështje të brendshme. Për këto arsye, SPAK ndjekë të gjitha praktikën dhe procedurat përkatëse për sigurimin, ruajtjen si dhe shkatërrimin e informacionit në rrjet në zbatim të dispozitave të parashikuara në ligjin “Për Arkivat” nr. 9154 datë 06.11.2003, kreu V “Për arkivat e numerizuara”.

Neni 7

Detyrat e Drejtorisë së Teknologjisë së Informacionit (DTI)

1. Detyrat e DTI janë si më poshtë:

- a. Është përgjegjës për zbatimin e masave të sigurisë për mbrojtjen nga kërcënimet digjitale, përfshirë antivirus, firewall dhe masat e sigurisë për të parandaluar aksesin e paautorizuar dhe sulmeve kibernetike të ndryshme.
- b. Sipas nevojës, DTI është e detyruar të identifikojë dhe klasifikojë të dhënat sipas nivelit të tyre të rrezikut dhe ndjeshmërisë. Klasifikimi do të përdoret për të vendosur nivelet e aksesit dhe masat e sigurisë për secilën kategori të të dhënave.
- c. Zgjidhjen e problemeve teknike në raste anomalish apo defektesh.
- d. Monitorimin e trafikut në përputhje me legjislacionin në fuqi.
- e. Sigurimin e madhësisë së skedarëve që mund ti bashkëngjiten mesazheve të postës, të cilët së bashku me përmbajtjen e e-mailit nuk duhet të jenë më të mëdhenj se 25 MB e cila mund të ndryshohet sipas kërkesave të veçanta nga Drejtuesi i Prokurorisë së Posaçme, Prokurorët, Drejtori dhe zëvendësdrejtori i BKH, hetuesit e BKH, oficerët nga shërbimet e Policisë Gjyqësore, punonjësit e administratës së Prokurorisë së Posaçme me miratimin e Kancelarit dhe punonjësit e BKH me miratimin e Drejtorit të kësaj të fundit⁴.
- f. Sigurimin e standardit të konfigurimit të adresës elektronike sipas referimeve të Shtojcës III.
- g. “Domain Names” të SPAK duhet të përmbajë akronimin SPAK.
- h. Nuk duhet të përmbajnë numra ose karaktere simbolik përveç vizës.
- i. Punonjësi i DTI është përgjegjës për instalimin dhe përditësimin e programeve “antivirus” dhe “antispymware” si në servera ashtu edhe në kompjuterët lokal të punonjësve. Punonjësve ju ndalohet e drejta për ndryshimin e opsioneve të këtyre programeve.
- j. Punonjësi i DTI është përgjegjës për krijimin, modifikimin dhe shkatërrimin e list adresave sipas nevojave që dikton SPAK në përputhje me legjislacionin në fuqi.
- k. Në rastet kur vërehen punonjës që nuk zbatojnë rregulloret përkatëse që lidhen mbi përdorimin e shërbimeve atëherë duhen marrë masa për ndërprerjen e përkohshme dhe/ose të përhershme të shërbimit.
- l. DTI kujdeset për zbatimin dhe monitorimin e politikave të mbrojtjes së të dhënave për sa i përket postës dhe komunikimit elektronik të punonjësve të SPAK.

Neni 8

Përgjegjësitë e Punonjësve

1. Përdoruesit e sistemit kompjuterik në SPAK kanë këto detyra dhe përgjegjësi:
 - a. Të respektojnë procedurat për përdorimin e mirë të postës elektronike duke e përdorur atë vetëm dhe ekskluzivisht për qëllime të punës. Ato duhet të aksesojnë rregullisht postën elektronike dhe t’i përgjigjen mesazheve sa më shpejt. Në raste të veçanta kur nevojitet akses në shërbime të tjera shtesë duhet kërkuar asistencë e stafit të DTI.
 - b. Nuk lejohet instalimi apo përdorimi i paautorizuar i softëve të komunikimit (direkt apo me Email) të paautorizuar.

⁴ Është ndjekur e njëjta praktikë me AKSHI sipas Rregullores nr. 1 datë 16.06.2023 “Për Përdorimin e Postës Elektronike në Administratën Publike”, neni 8, paragrafi 1, germa 2 pika iii).

- c. Nuk lejohet përdorimi i programeve të komunikimit (direkt ose me e-mail) për arsye personale, përfitimi dhe diskriminimi.
- d. Punonjësit e paautorizuar nuk lejohen të çaktivizojnë apo alternojnë sistemet antivirus të instaluar në kompjuterët e institucionit.
- e. Punonjësit nuk kanë të drejtë të instalojnë programe aplikative në kompjuterin e tyre përveç programeve të instaluar nga DTI. Nëse për arsye pune nevojitet instalimi i programeve të tjerë duhet paraprakisht të autorizohet instalimi nga Drejtori i DTI. Në çdo rast instalimi kryhet nga punonjësi i DTI i cili ka të drejta administratori.
- f. Nuk lejohet shpërndarja me e-mail i dokumenteve ose të dhënave të klasifikuara
- g. Punonjësit e SPAK duhet të zbatojnë rregullat e sigurisë kibernetike në përputhje me legjislacionin në fuqi dhe politikës së brendshme të institucionit e parashikuar në Shtojcën IV “Për Sigurinë e Informacionit dhe Mbrojtjes Kibernetike të SPAK”, e cila përditësohet nga DTI.
- h. DTI njofton punonjësit e SPAK me email në mënyrë të vazhdueshme dhe kur është e nevojshme organizon dhe trajnime në lidhje me përditësimet e politikës së brendshme të sigurisë së informacionit dhe mbrojtjes kibernetike.
- i. Punonjësit gjithashtu duhet të mos hapin mesazhe elektronike që u duken të dyshimtë dhe/ose që vijnë nga adresa të jashtme të panjohura.
- j. Punonjësit nuk duhet që të hapin materialet e bashkëngjitur me mesazhin që nuk presin ti marrin ose që vijnë nga adresa të panjohura, jo zyrtare, të internetit dhe/ose të dyshimta;
- k. Punonjësit nuk duhet të aktivizojnë optionet që mundësojnë përhapjen e emailit në mënyrë automatike në rastet kur përdoren programe për menaxhimin e postës elektronike (MAIL CLIENT).
- l. Punonjësit duhet të mos dërgojnë mesazhe zinxhir por ti fshijnë ato në rastet kur vijnë nga adresa të jashtme apo nga adresa zyrtare por nuk kanë përmbajtje që lidhet me punën.
- m. Punonjësit të mos përpiqen të eliminojnë mesazhe “spam” ose “malware” nëpërmjet shërbimeve që ofrohen në internet. Në këto raste duhet kërkuar ndihma e stafit të DTI.
- n. Punonjësit të mos ridërgojnë mesazhe që përmbajnë spam, malware, në adresa të tjera zyrtare.
- o. Punonjësit të dërgojnë ose ridërgojnë mesazhe (qofshin këto zyrtare ose private) që i kanë marrë gabimisht tek personat e adresuar ose tek dërguesi dhe ta fshijnë kopjen që ndodhet në mailboxin e tyre.

KREU III ETIKA

Neni 9

Etika dhe forma e komunikimit elektronik

1. Formatimi i postës elektronike zyrtare duhet të ketë një formë estetike dhe duhet të zbatohen një sërë rregullash për mënyrën e të shkruarit. Përdorimi i saj nuk limitohet

- vetëm në dërgimin e mesazheve të thjeshtë në formë teksti por edhe në dërgimin e skedarëve të formateve të ndryshëm me kapacitete të limituara.
2. Mesazhet elektronike mund të ruhen dhe printohen për arsye administrative. Një formë etike është edhe përgatitja e një formati bazë, të përgjithshëm të mesazheve elektronike që do ti bashkëngjitet kësaj rregulloreje në fund në formën e një shtojce.
 3. Ky format është i detyrueshëm për të gjitha adresat e SPAK dhe nuk mund të ndryshohet nga askush përveç se nga institucioni kompetent.

Neni 10

Rregullat mbi etikën e komunikimit elektronik

1. Rregullat e mëposhtme mbi etiken e të shkruarit janë të detyrueshme.
 - a. Në SPAK ndalohet çdo formë diskriminimi bazuar në moshë, racë, gjini, aftësi fizike apo mendore, burimet e të ardhurave, besimi fetar apo përkatësia politike duke përdorur burimet dhe shërbimet e TI-së;
 - b. Përdorimi i rrjetit kompjuterik dhe postës elektronike më qëllim kërcënim, poshtërimi, ofendimi apo diskriminimi është i ndaluar sipas legjislacionit në fuqi;
 - c. Mesazhet elektronike duhet të formulohen duke përdorur gjuhë zyrtare;
 - d. Duhet treguar kujdes me komente konfidenciale. Mesazhet mund të publikohen për nevoja administrative;
 - e. Duhet përdorur gramatika dhe gjuha letrare për të evituar keqkuptime.
 - f. Mesazhet duhet të rilexohen para dërgimit.
 - g. Mesazhi duhet të përmbajë formatim të pranueshëm të tekstit.
 - h. Duhet të evitohen përdorimet e fjalive shumë të gjata. Është e këshillueshme të përdoren nga 10 deri në 20 fjalë në një fjali.
 - i. Nuk duhet formuluar mesazhe krejtësisht me gërma të mëdha.
 - j. Duhet shkruar në mënyre koncize dhe të drejtpërdrejtë.
 - k. Mesazhet duhet të jenë në përputhje me “Rregullat dhe Standartet e Etikës në Prokurorinë e Posaçme kundër Korrupsionit dhe Krimit të Organizuar” të miratuara me Urdhërin nr. 640, datë 25.09.2023 dhe “Rregulloren e Disiplinës dhe Kodin e Etikës” të BKH-së, miratuar me Urdhërin nr. 116, datë 28.04.2021 të Drejtuesit të Prokurorisë së Posaçme kundër Korrupsionit dhe Krimit të Organizuar.
 - l. Nuk duhen bashkëngjitur skedarë të panevojshëm.
 - m. Duhet përdorur me kriter prioritetet.
 - Nuk janë të pakta rastet kur nëpër fushat e subjektit të postës-e shkruhet Urgjent!. Duke e përdorur pa kriter prioritetin ai do humbiste funksionin dhe do gjendeshit në vështirësi atëherë kur do nevojitej realisht.
 - I njëjti rregull vlen edhe kur fjalët **URGJENT** ose **I RËNDËSISHËM** që shkruhen në përmbajtjen e mesazhit.
 - n. Mesazhet e postës duhet të përmbajnë në fund një shënim me emrin dhe kontaktet e personit që e dërgon sipas skemës në Shtojca I.

- o. Duhet përdorur me kriter dhe vetëm atëherë kur nevojitet, dërgimi i mesazhit të gjithë adresat e institucionit. Përdorni opsionin “Reply To All” vetëm atëherë kur është realisht e nevojshme.
- p. Duhet bërë kujdes me shkurtime dhe përdorimin e ikonave emocionale. Në mesazhet zyrtare duhet përpjekur të mos përdoren sigla ose shkurtime emrash si p.sh. SPAK në vend të emrit të plotë kur nuk është sqaruar paraprakisht. I njëjti rregull vlen edhe për ikonat emocionale si p.sh. ☹, :- (, etj.).
- q. Duhet pasur kujdes me formatin e mesazhit (html, rich text apo plain text). Formatimi i komplikuar mund të sjellë mos marrjen e plotë të mesazhit ose çrregullimin e plotë të tij që në marrje mund të jetë shumë i vështirë për t’u lexuar, ose shkon në formën e një dokumenti të bashkëngjitur.
- r. Nuk duhet përpjekur të tërhiqet mbrapsht një mesazh, (opsioni RECALL). Në rast se dërgoni një mesazh jo të plotë ose një adresë të gabuar mos u përpiqni ta tërhiqni mbrapsht por dërgoni një email tjetër sqarues.
- s. Duhet pasur kujdes në përdorimin e panevojshëm në fushën “Cc:” (carbon copy) atëherë kur marrësit nuk kanë pse të marrin një kopje të mesazhit. Kur i përgjigjeni një mesazhi të marre nga “Cc:” duhet vendosur nëse do përfshihen edhe marrësit e tjerë të listuar në fushën “Cc:”.
- t. Mesazhet e postës elektronike duhet të jenë të formuluar me mirësjellje dhe të shfaqin një komunikim formal.

KREU IV KOMUNIKIMI ZYRTAR

Neni 11 Komunikimi elektronik

1. Punonjësit e SPAK, në komunikimet zyrtare të brendshme ose të jashtme, në përmbushje të detyrimeve të tyre, dhe përveç dokumenteve zyrtarë, përdorin edhe postën elektronike me anë të rrjetit elektronik të brendshëm të prokurorisë;
2. Është i ndaluar përdorimi i adresës zyrtare e postës elektronike për qëllime private;
3. Punonjësit e kanë të ndaluar të ridrejtojnë (Forward) në mënyrë automatike mesazhet elektronike e marra nëpërmjet rrjetit të SPAK tek adresa e postës elektronike private.
4. Shkrimi që duhet të përdoret nga të gjithë punonjësit për të gjithë korrespondencën dhe dokumentacionin është Times New Roman, 12;
5. Çdo punonjës i SPAK ka detyrimin për çdo ditë zyrtare të punës të kontrollojë dhe t’i përgjigjet postës zyrtare elektronike;
6. Çdo mesazh elektronik i dërguar me anë të postës zyrtare nga eprori për vartësin e tij ose për një vartës, i cili përmban një mesazh, urdhër, udhëzim ose kërkesë në lidhje me procesin e punës është i barasvlershëm me një mesazh, urdhër, udhëzim ose kërkesë të bërë me shkrim dhe të dërguar me anë të protokollit të brendshëm;
7. Për ekonomi administrative, të gjithë prokurorët, hetuesit dhe punonjësit e administratës, pasi shqyrtojnë praktikën për punën e eprorit, në momentin e përfundimit të saj, kanë

- detyrimin të dërgojnë bashkëngjitur një kopje elektronike të dokumentit në adresën zyrtare elektronike të eprorit të tyre respektiv;
8. Në rastin kur komunikimi elektronik përdoret për të ofruar dhe për të marrë informacione me institucione të brendshme ose të jashtme, në të gjitha rastet, mbikëqyrësi i drejtpërdrejtë duhet të informohet në seksionin “Cc” të mesazhit elektronik;
 9. Mesazhet zyrtare me email duhet të përmbajnë në fund të mesazhit emrin, mbiemrin, pozicionin dhe detajet e kontaktit;
 10. Një punonjës nuk mund të transmetojë, ofrojë ose marrë informacione me anë të përdorimit të adresës elektronike të një punonjësi tjetër;
 11. Mesazhet zyrtare elektronike mund të ruhen dhe printohen për arsye administrative, vetëm nga përdoruesi i adresës zyrtare elektronike. Gjithashtu në raste të veçanta ky veprim mund të kryhet nga punonjësi i DTI, por në çdo rast vetëm me miratimin e Drejtuesit të Prokurorisë së Posaçme ose Drejtorit të BKH për rastet e punonjësve të saj;
 12. Në rastin kur një masë administrative ose disiplinore dërgohet me email, një kopje e printuar e një mesazhi elektronik zyrtar ka të njëjtën vlerë si një dokument zyrtar i dërguar nga një protokoll i brendshëm;
 13. Është e ndaluar që të dërgohet një mesazh elektronik, i cili përmban një pozicion zyrtar të SPAK tek institucionet ose palët e treta, pa miratimin paraprak të Drejtuesit të Prokurorisë së Posaçme ose Drejtorit të BKH për rastet e punonjësve të saj;
 14. Rregullat për përdorimin dhe etikën e hartimit të emaileve të parashikuara në këtë rregullore, konsiderohen se janë të njohura për përdoruesit e sistemit të komunikimit elektronik dhe janë të detyrueshme për të gjithë punonjësit e institucionit.
 15. Ndalohet përdorimi i mediave sociale për çështje private.

Neni 12

Hyrja në postën zyrtare elektronike në mungesë të mbajtësit të saj

1. SPAK rezervon të drejtën për të hyrë në llogarinë e postës elektronike të një anëtarit të stafit në mungesë të papritur të tij ose të zgjatur (psh. për shkak të sëmundjes) në mënyrë që të lejojë që institucioni të sigurojë delegimin e detyrës tek një punonjës tjetër.
2. Një akses i tillë duhet të bëhet, në rrethana normale, me njohurinë dhe dakortësinë paraprake të punonjësit.
3. Sidoqoftë, kur nuk është e mundur për të kontaktuar punonjësin ose në raste urgjente, atëherë SPAK rezervon të drejtën për të hyrë në llogarinë e postës elektronike të punonjësit për të marrë informacionin që lidhet me funksionin e tij zyrtar.
4. Kërkesat për hyrje në llogarinë e një punonjësi në mungesë të këtij të fundit duhet të bëhen vetëm nga Drejtuesi i Prokurorisë së Posaçme ose nga Drejtori i BKH për rastet e punonjësve të saj pranë Drejtorit të DTI, i cili pas marrjes së kërkesës kryen procedurën e nevojshme për hyrje në llogarinë e punonjësit për të cilin është kryer kërkesa.

Neni 15
Ndërhyrja tek mesazhet elektronike

1. SPAK rezervon të drejtën që të ndryshojë rrugën, destinacionin apo të pezullojë dërgimin e mesazheve në vartësi të rrethanave duke njoftuar menjëherë dërguesin kur ajo mund të sjellë pasoja në lidhje me punën dhe funksionimin e SPAK. Kjo përfshin, por nuk është e kufizuar me:⁵
 - a. Pengimin e dërgimit, alternimin, arkivimin apo fshirjen e dokumenteve të bashkëngjitur (attachment) ose kodit të mesazhit atëherë kur dyshohet se përbën rrezik për funksionimin e sistemit kompjuterik.
 - b. Eliminimin e përmbajtjeve shtesë në mesazhe (p.sh muzike), që konsiderohen pa vlerë për SPAK dhe zënë vend në memorie.
 - c. Pengimin e dërgimit apo arkivimin e mesazheve me përmbajtje të dyshimtë. Mesazhe që përmbajnë dokumente të bashkëlidhura (attachment) me emra dhe prapashtesa të dyshimta.
 - d. Pengimin e dërgimit apo arkivimin e mesazheve të formuluar në gjuhë fyese.
 - e. Pengimin e dërgimit apo arkivimin e mesazheve që konsiderohen si jozyrtar apo/ose reklama komerciale (spam).

KREU IV
PËRGJEGJËSIA DISIPLINORE, ZBATIMI, HYRJA NË FUQI DHE PUBLIKIMI

Neni 16
Strukturat për Zbatimin e Rregullores

1. Ngarkohen për zbatimin dhe monitorimin e kësaj rregulloreje, Drejtuesi i Prokurorisë së Posaçme, Drejtori i BKH, Kancelari i Prokurorisë së Posaçme, Drejtorja e Burimeve Njerezore ne BKH dhe DTI.
2. Çdo veprim ose mosveprim në kundërshtim me këtë rregullore përbën shkak për nisjen e procedimit disiplinor.

Neni 17
Hyrja në fuqi

Kjo rregullore hyn në fuqi menjëherë.

⁵ Shih nenet 20 dhe 27 paragrafi 3 i ligjit nr.9887, datë 10.3.2008 “Për Mbrojtjen e të Dhënave Personale”.

SHTOJCA I

SHEMBULL I ETIKETËS SË PËRDORUESIT

Emër Mbiemër

Funksioni

Departamenti

Sektori

Institucioni

Logo ne formatin .GIF

Adresa postare

Rr

Nr.

Qyteti

Tel:

Fax:

Mobile:

E-mail: emri.mbiemri@spak.gov.al

Web:

SHTOJCA II

Informacioni i transmetuar në përmbajtje të këtij mesazhi është i destinuar vetëm për individin ose për institucionin të cilit i është nisur, mund të përmbajë materiale konfidenciale dhe / ose të privileguara vetëm për marrësin. Çdo rishikim, transmetim, shpërndarje apo kryerje e ndonjë veprimi tjetër të ngjashëm me këto, nga personat apo nga subjekte të tjera të ndryshme nga marrësi i synuar, është i ndaluar. Nëse merrni gabimisht këtë mesazh, ju lutem kontaktoni urgjentisht dërguesin e tij dhe fshini çdo material të transmetuar në kompjuterin tuaj. Ne nuk pranojmë asnjë detyrim lidhur me dëmtimin apo humbjen e shkaktuar nga programe të dëmshme apo nga viruse, përveç rastit të neglizhencës së plotë, apo sjelljes së gabuar dhe të qëllimshme.

SHTOJCA III

Konfigurimi i adresës së emailit

A. Mesazhet që dërgohen jashtë infrastrukturës së shërbimit të postës elektronike të institucionit/institucioneve gjithashtu duhet të përmbajnë një “deklaratë” sipas Shtojcës II. Kjo deklaratë duhet të shtohet në mënyrë automatike nga sistemi i postës elektronike.

B. Adresa e postës duhet të jetë e formuluar në këtë mënyrë:

emer.mbiemer@spak.gov.al

- Emri i personit të jetë i plotë me të gjitha gërmat e vogla të alfabetit të gjuhës shqipe përjashtuar gërmat “ë” dhe “ç”;
- Mbiemri i personit duhet të jetë i plotë me të gjitha gërmat e vogla të alfabetit të gjuhës shqipe përjashtuar gërmat “ë” dhe “ç”;
- Pjesa pas karakterit @ përmban emrin e domain-it të institucionit;
- Punonjësit e autorizuar të përdorin softuerë komunikimit direkt do të pajisen me një adresë identifikuese individuale e mbrojtur me fjalëkalim.

C. Fjalëkalimet e adresave postare duhet të kenë jo më pak se **10 karaktere**:

- Germa të mëdha dhe të vogla të alfabetit;
- Një karakter duhet të jetë numër (0-9);
- Një karakter duhet të jetë një simbol (p.sh *,\$,”,£,%,&).

Përdoruesit duhet të ndërrojnë fjalëkalimet e tyre brenda një periudhe kohore të përcaktuar nga institucioni. Në rast të kundërt këto fjalëkalime do të skadojnë, duke humbur të drejtën e aksesimit të shërbimit të postës elektronike dhe të shërbimeve të tjera, deri në ndërhyrjen e Drejtorisë së Teknologjisë së Informacionit (DTI).

SHTOJCA IV

Për Sigurinë e Informacionit dhe Mbrojtjes Kibernetike të SPAK

Hapat që duhet të ndërmarrë DTI për Sigurinë e Informacionit dhe Mbrojtjes Kibernetike të SPAK janë:

1. Kontrolli i aksesit në pajisjet e rrjetit sipas masave të autentifikimit (p.sh. përdorues/fjalëkalim ose masa të tjera më të forta).
 - Aksesit i pajisjeve të rrjetit informatik bëhet nëpërmjet masave të autentifikimit, ku çdo punonjësi që do të aksesojë këtë rrjet i është dhënë një emër përdoruesi dhe një fjalëkalim, sipas group policies të përcaktuara në server.
 2. Kontrolli i aksesit në sistem sipas roleve dhe detyrave të përdoruesve.
 - Kontrolli i aksesit në sistem kryhet nga rregullat (domain policy) të përcaktuara në serverin domain controller. Ky akses është i strukturuar sipas roleve të cilat janë përcaktuar sipas përdoruesve që do të përdorin rrjetin e SPAK.
 3. Kompleksiteti i fjalëkalimeve dhe menaxhimi i tyre.
 - Fjalëkalimi, sipas politikave të përcaktuara, duhet të jetë jo më pak se 10 karaktere dhe duhet të përmbajë domosdoshmërisht karaktere të vogla, karaktere të mëdha (shkronja kapitale), karaktere speciale dhe numra.
 - Të gjithë përdoruesit e sistemit instruktohen në lidhje me mënyrat e administrimit të fjalëkalimeve.
- Këtu përfshihen:
- i. zgjedhja e fjalëkalimit fillestar;
 - ii. ndryshimi i fjalëkalimit dhe këshilla të njohura sigurie për zgjedhjen e tij;
 - iii. mbrojtja e fjalëkalimit si dhe ndalimi i dhënies së fjalëkalimit midis përdoruesve;
 - iv. Resetimi i fjalëkalimit (në qoftë se një llogari përdoruesi është mbyllur ose në qoftë se përdoruesi ka harruar fjalëkalimin).
4. Monitorimi i ndërhyrjeve të pa autorizuar nëpërmjet logeve të auditimit.
 - Punonjësi i DTI është gjithmonë në vëzhgim dhe monitorim të vazhdueshëm të logeve të auditit të të gjithë tentativave për ndërhyrje të paautorizuara.
 5. Specifikimi i adresave IP dhe portave të lejuara
 - Shpërndarja e adresave IP për përdoruesit e rrjetit kompjuterik është bërë me metodën automatike sipas protokollit DHCP dhe manualisht në raste të veçanta. Në rast se nga DTI shikohen problematika në lidhje me shërbimet që meren në porta të caktuara, këto porta mund të mbyllën ose rikonfigurohen.
 6. Lejimi ose jo i ndarjes (share) të dosjeve

- SPAK ka gjykuar të arsyeshme lejimin e dosjeve (direktori) share, ku informacioni që hidhet në këto dosje lejohet të ndahet ndërmjet grupeve të përcaktuara të përdoruesve.
7. Kontrolli i konfigurimit të hardware-it dhe të softwaret-it
 - Çdo pajisje apo program (software) që përdoret në SPAK kalon në fazën e kontrollit të konfigurimit. Kjo është faza që vendos mbi përdorimin dhe qëllimin e përdorimit të hardwaret-it apo software-it. Ky kontroll kryhet nga DTI dhe për testime të tilla specialisti mund të mbajë raporte
 8. Instalimi i pajisje të rrjetit që bëjnë analizë të thellë të trafikut duke u mbështetur jo vetëm në rregullat e listave të aksesit por edhe në sjelljen e tij (Firewall-et).
 - Kjo masë i referohet përmirësimit të perimetrit të sigurisë së rrjetit. Perimetri i rrjetit i mbrojtur me anë të teknikave të analizës së rregullave të aksesit të konfigurara nga administratori i rrjetit është i pamjaftueshëm dhe kollaj i anashkalueshëm.
 - Zhvillimet e fundit teknologjike kërkojnë ngritjen e teknikave të mbështetura në analizën e sjelljes së trafikut duke integruar firewall-et me shërbime IDS/IPS. Këto lloj firewall-esh janë quajtur Next Generation Firewall, duke bërë një analizë nga shtresa e 1-rë e arkitekturës OSI deri në atë të 7 të saj, duke eliminuar mundësinë e trafikut me sjellje jo të zakonshme.

Përdoruesit e rrjetit të SPAK udhëzohen si më poshtë:

1. Nuk lejohet përdorimi i wi-fi, Përdorimi i rrjeteve wi-fi mund të lejojë sulmuesit të aksesojnë rrjetin e SPAK në distanca ku rrjeti është i gjetshëm.
2. Nuk lejohet ndarja e fjalëkalimeve për llogaritë personale me kolegët, eprorët etj.
3. Nuk lejohet përdorimi i fjalëkalimeve të dobëta. Fjalëkalime të dobëta janë fjalëkalimet të cilat përfshijnë vetëm numra, fjalëkalimet që përmbajnë emrin, ose fjalëkalime të cilat janë të njëjtë për të gjithë përdoruesit Psh. 12345678, emri1234 etj..
4. Nuk lejohet përdorimi i të njëjtit fjalëkalim për shërbime të ndryshme: Nuk lejohet të përdorni të njëjtën fjalëkalim për disa llogari online. Përdorni një fjalëkalim të ndryshëm për secilën llogari.
5. Nuk lejohet hapja e email-eve dhe lidhjeve(link) të dyshimta, Nuk lejohet të hapni email-et ose lidhjet e dyshimta që vijnë nga adresa të panjohura.
6. Nuk lejohet përdorimi pajisjeve USB të përdorura jashtë rrjetit të SPAK, të cilat nuk janë skanuar dhe verifikuar paraprakisht për malëare, viruse etj.

7. Nuk lejohet hapja e dokumenteve të dyshimta në email ose skedarë të dyshimtë që janë dërguar në email pa i verifikuar më parë.
8. Nuk lejohet shpërndarja e informacionit sekret në email. Gjithastu nuk lejohet shpërndarja e informacion sensitiv ose e fjalëkalimeve në email të pa enkriptuar.
9. Nuk lejohet të futen CD ose DVD të panjohur dhe që nuk janë të besueshme në kompjuterin tuaj.
10. Nuk lejohet përdorimi i programeve të paligjshme ose kopje të pa licensuara të programeve.
11. Nuk lejohet shpërndarja e informacionin personal në rrjete sociale që mund të rrezikojnë funksionin që ushtron dhe çënojnë integritetin e SPAK.
12. Nuk lejohet ndarja e infomacioneve sensitive në telefon, Nuk lejohet ndarja e informacionit sensitiv në aplikacionet e mesazheve(Chat) apo aplikacione të tjera pa patur siguri të mjaftueshme.
13. Nuk lejohet të përdorni Bluetooth në kompjuterin tuaj pasi mund të jetë një pikë hyrëse për sulmet.
14. Nuk lejohet të hapen ridrejtimet e linq-eve. Para se të klikoni në një link, shikoni ku ju ridrejton(redirect) për të parë nëse është i dyshimtë.
15. Nuk lejohet dhënia e informacionit personal në faqe të pa certifikatë të sigurisë (Https). Kontrolloni për certifikata të sigurisë(Https) kur shpërndani informacionin personal në internet.
16. Nuk lejohet klikimi mbi pop-up të dyshimta. Nuk lejohet klikimi mbi reklama pop-up që janë të dyshimta ose ofrojnë produkte të rrezikshme.
17. Nuk lejohet kryerja e pagesave me karta në faqe të panjohura. Kujdesuni kur jepni informacionin e kartës suaj të kreditit në internet.
18. Nuk lejohet përdorimi i kompjuterit me llogari të privileguara për aktivitete të rrezikshme.
19. Nuk lejohet përdorimi i llogarisë së e-mailit apo llogarive të tjera të përfituara nga institucioni për të kryer veprime me interes personal.
20. Nuk lejohet përdorimi i pajisje personale në rrjetin e SPAK. Në çdo rast duhet të njoftohet DTI për miratimin e përdorimit.

21. Nuk lejohet përdorimi i kopjeve të vjetra të softuerit, Përdorimi i kopjeve të vjetra të softuerit mund të ketë mungesë të patcheve të sigurisë.
22. Të mos harrohet mbyllja e sesioneve. Pas përdorimit të sesioneve tuaja online kur përfundoni përdorimin, sidomos në kompjutera të përbashkët duhet të bëni log out në mënyrë që të mbyllet sesioni i hapur.
23. Nuk lejohet të bëhen shkarkime nga burime të dyshimta: Aplikacione ose skedarë mund të shkarkohen vetëm nga burime të besueshme dhe zyrtare.
24. Nuk lejohet ndarja e informacionit financiar nëpërmjet email-it.
25. Nuk lejohet përdorimi i lidhjeve publike të Wi-Fi për hapjen e llogarisë së e-mailit apo llogarive të tjera të SPAK.
26. Nuk lejohet shpërndarja e fjalëkalimeve me anë të e-mailit.
27. Nuk duhet tu besohet pyetjeve të ndjeshme online, si psh. Pyetjet për fjalëkalimet, si "Cila është emri i nënës suaj?" pasi mund të jenë të lehta për sulmuesit të zbulohen.
28. Duhet të përditësohen sistemet operative të pajisjeve që keni në përdorim.
29. Të mos bëhen regjistrime në faqe interneti pa ndonjë nevojë të veçantë, veçanërisht në faqe që kërkojnë të dhëna sensitive.
30. Të mos harrohet që të fshini informacionin tuaj të vjetër. Duhet të fshini rregullisht dokumente dhe informacion të vjetër që nuk ju duhen më.
31. Nuk lejohet hapja e aplikacione të paautorizuara. Lista e aplikacioneve të autorizuara sipas Shtojces V.
32. Nuk duhet tu besohet mesazheve të rreme të fitimit të llotarive ose ofertave të çuditshme: Nuk ka oferta që janë shumë të mira për të qenë të vërteta. Kujdesuni për titujt dezinformues.
33. Çdo ditë në mbarim të procesit të punës kompjuteri duhet të fiket.

SHTOJCA V
Lista e Apliakcioneve të autorizuar në SPAK

1. Paketa Ms Office
2. Check Point VPN
3. Forti Client VPN
4. Win Rar
5. Adobe Acrobat Reader
6. Google Chrome
7. Google Earth
8. Vlc
9. Pdf Merger & Splitter
10. Programe dhe tools për hapjen e Audio/ Video CD/DVD