REPUBLIKA E SHQIPËRISË
AGJENCIA PËR ZHVILLIM BUJQËSOR DHE RURAL
DREJTORIA JURIDIKE DHE SHËRBIMEVE MBËSHTETËSE

Nr. 746 prot. Tiranë, më 6 . 2 .2025

URDHËR

Nr. 19, datë 6 . 2 . 2025

PËR

MIRATIMIN E RREGULLORES PËR PËRDORIMIN E RRJETIT DHE PAJISJEVE ELEKTRONIKE NË AGJENCINË PËR ZHVILLIM BUJQËSOR DHE RURAL

Bazuar në ligjin nr. 9887, datë 10.03.2008, "Për mbrojtjen e të dhënave personale", i ndryshuar, në ligjin nr. 9918, datë 19.5.2008 "Për komunikimet elektronike në Republikën e Shqipërisë", i ndryshuar, në VKM nr. 719, datë 31.10.2014, "Për organizimin dhe funksionimin e Agjencisë për Zhvillim Bujqësor dhe Rural", i ndryshuar, në Udhëzimin nr. 1, datë 10.1.2025, të Ministrit të Bujqësisë dhe Zhvillimit Rural, "Për përcaktimin e rregullave dhe procedurave për funksionimin e brendshëm të Agjencisë për Zhvillim Bujqësor dhe Rural", në Urdhrin e Kryeministrit me nr. 93, datë 12.6.2024, "Për miratimin e strukturës dhe organikës së Agjencisë për Zhvillim Bujqësor dhe Rural",

U R DH Ë R O J:

1. Miratimin e rregullores për përdorimin e rrjetit dhe pajisjeve elektronike në Agjencinë për Zhvillim Bujqësor dhe Rural, sipas shtojcës nr. 5 bashkëlidhur këtij urdhri.
2. Për zbatimin e këtij urdhri ngarkohen strukturat e Agjencisë për Zhvillim Bujqësor dhe Rural, si dhe për kontrollin e zbatimit ngarkohet Drejtoria e Teknologjisë së Informacionit.

Ky urdhër hyn në fuqi menjëherë.

DREJTOR I PËRGJITHSHËM
Ardita Kuçi

SHTOJCA NR. 5

PËR PËRDORIMIN E TEKNOLOGJISË SË INFORMACIONIT TË INSTITUCIONIT

Përmbajtja

KREU I

DISPOZITA TË PËRGJITHSHME

1. Baza ligjore

Këto rregulla nxirren në zbatim të:

1. ISO 27001 Sistemet e menaxhimit të sigurisë së informcionit;
2. ISO 27002 Kodi i praktikës për menaxhimin e sigurisë së informacionit;
3. VKM nr. 719, datë 31.10.2014 "Për organizimin de funksionimin e Agjencisë për Zhvillim Bujqësor dhe Rural si Agjencia e Pagesave;
4. Ligji nr. 9817, datë 22.10.2007 "Për Zhvillimin Bujqësor dhe Rura";
5. Ligji nr. 107/2021 "Për bashkëqeverisjen";
6. Ligji nr. 9880, datë 25.2.2008, "Për Nënshkrimin Elektronik", i ndryshuar;
7. Ligji nr. 9887, datë 10.03.2008, "Për Mbrojtjen e të Dhënave Personale", i ndryhsuar;
8. Ligji nr. 9918, datë 19.5.2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar;
9. Ligji nr.10273, datë 29.4.2010 "Për Dokumentin Elektronik", i ndryshuar;
10. Ligji nr. 10325, datë 23.9.2010 "Për Bazat e të Dhënave Shtetërore";
11. Ligji nr. 46, datë 7.05.2015 "Për Shërbimet Postare në Republikën E Shqipërisë"
12. Legjislacioni për Krimin Kibernetik Nr. 2/2017;
13. Ligji nr. 119/2014 "Për të drejtën e informimimit";
14. Ligji nr. 9367, date 07.04.2005 "Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike", i ndryshuar;
15. Ligji nr. 90/2012 "Për organizimin dhe funksionimin e Administratës Shtetërore";
16. Ligji nr. 44/2015, "Kodi i Procedurave Administrative i Republikës së Shqipërisë";
17. Ligji nr. 153/2013 "Pë nëpunësin civil", i ndryshuar
18. Ligji nr. 10296, datë 8.07.2014 "Për menaxhimin financiar dhe kontrollin";
19. VKM Nr. 673, datë 22.11.2017 "Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit", i ndryshuar;
20. VKM nr. 542, datë 25.7.2019, "Për miratimin e rregullores "Për sigurimin e informacionit të klasifikuar që trajtohet në Sistemet e Komunikimit dhe të Informacionit (SKI)";

21. VKM Nr. 957, date 19.12.2012 "Për mbetjet për pajisjet elektrike dhe elektronike";
22. Udhëzimit të Ministrit të Financave nr. 30, datë 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik";
23. VKM nr. 495 datë 13.9.2017 "Për miratimin e rregullave të përfitimit të shërbimeve publike elektronike"
24. VKM nr.252, datë 29.4.2022 "Për procedurat e ofrimit të shërbimeve on-line nga institucionet shërbimofruese dhe për metodologjinë e monitorimit e të kontrollit të veprimtarisë administrative të ofrimit të tyre";
25. VKM nr. 945, datë 2.11.2012 "Për miratimin e rregullores "Administrimi i sistemit të bazave të të dhënave shtetërore";
26. VKM nr. 710 datë 21.08.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmerisë së punës dhe marrëveshjeve të nivelit të shërbimit", i ndryshuar;
27. Urdhër i Kryeministrit nr.202, datë 16.12.2005 "Për forcimin e transparencës, nëpërmjet rritjes së përdorimit të internetit dhe përmirësimit të faqeve ekzistuese të internetit";
28. Ligji nr. 37, datë 9.4.2015, "Për ratifikimin e Marrëveshjes Kuadër ndërmjet Këshilli të Ministrave të Republikës së Shqipërisë dhe Komisionit të Komuniteteve Europiane për rregullat e bashkëpunimit për asistencën për Shqipërinë, në kuadër të zbatimit të Instrurnentit të Parazgjerimit (IPA II)";
29. Rregullorja (BE) nr. 231/2014, e Parlamentit Evropian dhe Këshillit, e datës 11 mars 2014, mbi krijimin e Instrumentit për Asistencën e Paraanëtarësimit (IPA II);
30. Rregullorja (BE) nr. 236/2014 e Parlamentit Evropian dhe Këshillit, e datës 11 mars 2014, që përcakton proçedura dhe rregulla të përbashkëta për zbatimin e instrumenteve të BE, për financimin e masave të jashtme;
31. Rregullorja Zbatuese e Komisionit (BE) nr. 447/2014, mbi rregullat specifike për zbatimin e Rregullores 17 (BE) 231/2014, e Parlamentit Evropian dhe Këshillit, për krijimin e Instrumentit për Asistencën e Paraanëtarësimit (IPA II);
32. Rregullorja nr. 2, datë 6.11.2023 "Për Sigurinë e Informacionit", e AKSHI
33. Manuali i Procedurave të Drejtorisë së Teknologjisë së Informacionit të AZHBR

2. Objekti

Objekt i kësaj rregulloreje është përcaktimi i Parimeve dhe Rregullave të Përgjithshme të Sigurisë së Informacionit në AZHBR dhe përcaktimi i përgjegjësive për veprimet që lidhen me sigurinë me qëllim ruajtjen e integritetin, disponueshmërisë dhe konfidencialitetit të aseteve të informacionit të Agjencisë.

3. Qëllimi

1. Qëllimi i kësaj rregullore është garantimi i përputhshmërisë me aktet ligjore që rregullojnë çështjet e sigurisë së informacionit si dhe praktikave më të mira siç përcaktohet në standardin e sigurisë ISO 27001 (ISO/IEe 27001:2013).
2. Këto rregulla: "Për përdorimin e teknologjisë së informacionit të AZHBR-së", kanë për qëllim përcaktimin e kritereve dhe të kushteve që duhet të plotësojnë subjektet e kësaj rregulloreje për organizimin dhe për funksionimin e sistemeve të tyre të Teknologjisë së Informacionit dhe Komunikimit (më poshtë, TIK).
3. Përcaktimi i këtyre kritereve dhe kushteve për organizimin dhe funksionimin e sistemeve të TIK-ut, si edhe zbatimi i tyre, synon uljen e rrezikut operacional që mund të shkaktohet nga keqpërdorimi i sistemeve të TIK-ut, si edhe të ruajë besueshmërinë e këtyre sistemeve në mbështetjen e veprimtarisë së subjekteve.

4. Përkufizime

1. Teknologjitë e Informacionit dhe të Komunikimit janë hardware dhe software (kompjuter, telefona celularë, internet, sistemi operacional, softëare kompjuterikë, aplikacione celulari 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 (kompjutera, programe kompjuterike, internet).
3. Specialistët e TIK-ut ose IT-të janë punonjës, puna kryesore e të cilëve është zhvillimi i TIK-ut, operimi ose mirëmbajtja e sistemeve apo aplikacioneve të TIK-ut.
4. Kompjuter – kompjuterat përfshijnë kompjuterat personalë, tabletat apo pajisje të tjera portabël si:
5. Akses në internet – termi "Akses 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.: filma, lojëra, video-konferenca nëpërmjet një rrjeti interneti (për shembull: ADSL, lidhje kabllor, UMTS, lidhje optike, VDSL, Fibër etj.).
7. Website – faqja e internetit është një "dokument" me HyperText. Faqet e internetit mund të kenë tekst, lidhje link, video, fotografi, materiale të tjera të dokumenteve elektronike.
8. Firewall – pajisje apo një 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.
9. Username/UserID – varg karakteresh, që identifikojnë në mënyrë unike një përdorues në një sistem apo rrjet kompjuterik.
10. Password – fjalëkalim, kod sekret i një përdoruesi, që nuk duhet të njihet nga përdoruesit e tjerë dhe që i përdorur bashkë me Username/UserID lejon aksesimin e një sistemi kompjuterik.

11. Logim – 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 (passëord-i).
12. 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.
13. Domain Name – pjesa e tekstit që vjen pas shenjës: @, në një adresë email-i. Meqenëse interneti funksionon në bazë të adresave IP (katër sekuenca numerike) çdo domain name ka korresponduesin numerik unik.
14. Mail Client – program në kompjuterat e përdoruesve, që bën të mundur dërgimin, marrjen dhe organizimin e email-eve;
15. Reply to all – mundësi e ofruar nga mail client, për t'i kthyer email jo vetëm dërguesit, por të gjithë adresave të email-it të vendosura në "To" apo "CC".
16. Recall – mundësi e ofruar nga mail client për të tërhequr mbrapsht një email të dërguar.
17. Antivirus/Antispyware/Antimalware – programe të cilat bëjnë të mundur kontrollimin, identifikimin, eliminimin e programeve kompjuterike të dëmshme të instaluara në kompjutera (virus, trojan etj.)
18. Spam – mesazhe elektronike, email, me përmbajtje komerciale apo informuese jozyrtare.
19. Attachment – file në kompjuter, i cili dërgohet me anë të një email-i.
20. Chat – program, i cili lejon komunikimin në kohë reale midis 2 apo më shumë përdoruesve në internet.
21. Të dhëna personale – çdo informacion në lidhje me punonjësin, 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.
22. VPN – rrjete private virtuale, të cilat ofrojnë siguri të lartë.
23. Storage – memorie kompjuterike, të cilat përdoren për ruajtjen masive të të dhënave.
24. Server – sistemi kompjuterik (Hardware dhe Software), i cili ofron shërbime të ndryshme në rrjet.
25. Log – konsiderohet çdo shënim digjital mbi një ngjarje ose aktivitet të caktuar.

5. Parimet e Sigurisë

Në përputhje me Politikën e Sigurisë së Informacionit, objektivi kryesor për sigurinë e informacionit është të ruajë *integritetin*, *disponueshmërinë* dhe *konfidencialitetin* e aseteve të informacionit të Agjencisë. Termat e mësipërme përcaktohen si më poshtë:

i. Integriteti

Gjatë gjithë kohës informacioni duhet të jetë i plotë, i saktë dhe i qëndrueshëm ndaj modifikimeve të paautorizuara ose ndaj dëmtimeve.

ii. Disponueshmëria

Informacioni bëhet i aksesueshëm sa herë që është e nevojshme. Kjo do të thotë që të gjitha informacionet dhe të gjitha sistemet e informacionit janë të disponueshme dhe operacionale (të gatshme për punë) sa herë që nevojitet një gjë e tillë.

iii. Konfidencialiteti

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

iv. Përgjegjësia

Të gjithë personat, qofshin këta nëpunës, kontraktues, konsulentë ose përdorues të jashtëm, mbajnë përgjegjësi për pasojat që rrjedhin direkt nga veprimet e tyre dhe që kanë të bëjnë me asetet e informacionit të AZHBR. Çdo nëpunësi i bëhen të qarta përgjegjësitë e tij në lidhje me detyrën që kryen.

v. Mbrojtja fizike

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

6. Objektivat e Sigurisë

1. Aksesimi i të gjitha sistemeve të informacionit të Agjencisë kontrollohet rreptësisht për të garantuar integritetin dhe mbrojtjen e tyre.
2. Të gjitha sistemet (përfshirë këtu mjediset e zhvillimit, të testimit dhe produktet) mbrohen nga kërcënimet dhe nga dëmtimet fizike.
3. Të gjithë individët mbajnë përgjegjësi direkte për veprimet që kryejnë mbi asetet e informacionit të Agjencise.
4. Çdo person që autorizohet të aksesojë sistemet e AZHBR, për identifikimin e tij, ka një llogari përdoruesi unike me kredenciale personale të përbërë nga një username dhe një fjalëkalim (password). Llogaria e përdoruesit do të çaktivizohet automatikisht pas tre muajsh mospërdorimi. Përdoruesi detyrohet të mbajë të fshehtë fjalëkalimin e tij dhe ta ndyshojë atë në mënyrë periodike sa më shpesh të jetë e mundur. Fjalëkalimi duhet të jetë konform politikave të njohura të sigurisë të shpjeguara më poshtë. Aksesimi i pajisjeve dhe i sistemeve të AZHBR bëhet në përputhje me detyrat funksionale të përdoruesit. Asnjë përdoruesi nuk i lejohet të aksesojë lirisht funksionet e ndryshme të sistemeve.
5. Çdo punonjës duhet të njohë dhe të zbatojë procedurën e Clear Desk dhe Clear Screen.
6. Ndalohet rreptësisht përdorimi i të njëjtës llogari, prej dy ose më shumë përdoruesve. Çdo rast i tillë trajtohet si një shkelje serioze e rregullave të sigurisë.
7. Çdo sistem i Agjencisë në përdorim është i aksesueshëm nga një sistem menush dhe mbi bazën e aksesimit unik. Asnjë nga sistemet e Agjencisë, në asnjë rrethanë, nuk do të lejojë

hyrjen e njëkohshme të më shumë se një përdoruesi me të njëjtin fjalëkalim.

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

9. Përpara se të bëhen zhvillime/ndryshime aplikimesh, hartohen masa/procedura sigurie, të propozura nga Drejtoria TIK dhe miratuara nga Drejtori i Përgjithshëm i AZHBR-së.

10. Mjediset e zhvillimit, të testimit dhe produktet janë maksimalisht të ndara. Asnjë zhvillim/ndryshim aplikimi nuk duhet të kryhet në mjedise testimi ose produkti. Për këtë do të jetë e detyrueshme kryerja me rigorozitet e kontrolleve të zëvendësimit dhe të kalimit të aplikimeve nga ambienti i tyre i zhvillimit në atë të testimit dhe nga ai i testimit, në atë të produktit.

11. Për çdo mjedis të teknologjisë së informacionit (këtu përfshihen pajisjet në dhomën e serverave, bazat e të dhënave dhe të gjitha pajisjet e rrjetit të brendshëm të Agjencisë) hartohen masa/procedura sigurie. Ato klasifikohen si konfidenciale dhe kopja origjinale e tyre do të ruhet në mënyrë të sigurtë nga administratori përgjegjës i sigurisë i teknologjisë së informacionit.

12. Masat e sigurisë zbatohen në përputhje me funksionimin e sistemeve të Agjencisë, prej një regjimi pune 24 orë në ditë, për 7 ditë në javë.

KREU II

MIRËMBAJTJA, ADMINISTRIMI DHE PËRDORIMI I PAJISJEVE ELEKTRONIKE DHE I RRJETIT

7. Miradministrimi i pajisjeve elektronike dhe i programeve kompjuterike Rregullat e përdorimit të rrjetit dhe të pajisjeve kompjuterike

1. Administrimi i pajisjeve kompjuterike dhe elektronike kryhet në të njëjtën mënyrë si ai i aktiveve të tjera të AZHBR-së, në përputhje me Rregulloren e brendshme.
2. Përdorimi i rrjetit dhe i pajisjeve kompjuterike në institucion menaxhohen ngaDrejtoria e Teknologjisë së Tnformacionit.
3. Të gjitha pajisjet/sistemet kompjuterike, që janë pronë e AZHBR-së, duhet të përdoren vetëm për qëllime pune.
4. Ndalohet përdorimi për nevoja personale i postës elektronike.
5. Përdorimi i faqes së web-it duhet të jetë i kufizuar vetëm për qëllime pune.
6. Cilido përdoruesi, kur konstatohet se përdor për një kohë të gjatë këto burime për qëllime personale, mund t'i ndërpritet mundësia e përdorimit të këtyre burimeve.
7. Komunikimet që dërgohen me postën elektronike, duhet të konsiderohen si çdo lloj tjetër komunikimi për qëllime pune. Këto mjete komunikimi në tërësinë e tyre përfaqësojnë AZHBR-në, ndaj duhet të përdoren në mënyrën e duhur dhe profesionale.

8. Drejtoria e Teknologjisë së Informacionit është përgjegjëse për kujdesin, sigurinë dhe mirëmbajtjen e pajisjeve të teknologjisë së informacionit, hardware, software dhe platformave TIK të AZHBR-së, me përjashtim të rasteve kur dëmtimet janë shkaktuar nga vetë punonjësi që i ka në ngarkim dhe përdorim.
9. Kompjuter, laptop, printera, fotokopje, programe, pajisje periferike, HDD - Hard Disk Drive, kufje apo çdo lloj tjetër pajisjeje kompjuterike, që i jepet një përdoruesi nga AZHBR-ja, trajtohet sipas rregullave të menaxhimit të aktiveve.
10. Në një sistem kompjuterik do të instalohen vetëm ato programe që i nevojiten përdoruesit për kryerjen e detyrës. Lista e programeve ose programet e lejuara për instalim përcaktohen nga Specialisti i IT-së, të Drejtorisë e Teknologjisë së Informacionit.
11. Përmirësimet në software, instalime programesh, për shkak të rrezikut të lartë të viruseve të transmetuara në mënyrë elektronike, shkarkohen apo instalohen nga Specialisti i IT-së.
12. Me marrjen e kodit të përdoruesit (user account), për rrjetin dhe sistemet kompjuterike, përdoruesi është përgjegjës direkt për të gjitha veprimet që ndërmerren gjatë përdorimit të atij kodi.
13. Të gjitha pajisjet elektronike dhe programet kompjuterike të marra në ngarkim nga punonjësit e institucionit janë dhe mbeten gjithmonë pronë e AZHBR-së.
14. Specialisti i Burimeve Njerëzore dhe Shërbimeve Mbështetëse bashkëpunon me Specialistin e IT-së në realizimin e detyrave të tij. Për shpërndarjen e pajisjeve elektronike dhe programeve kompjuterike, si dhe për grumbullimin e tyre, në rast të largimit të personit nga detyra, Sektori i Burimeve Njerëzore paraqet një kërkesë, ku specifikohen:
    - të dhënat individuale;
    - zyra e caktuar për ushtrimin e detyrës;
    - nevoja për postën elektronike, adresë email-i nën domanin e institucionit, @azhbr.al;
    - nevoja specifike etj.
15. Pajisjet elektronike nuk duhet të nxirren nga ambientet e AZHBR-së dhe as nuk duhet të zhvendosen brenda ndërtesës, pa miratimin dhe mbështetjen e Specialistit të IT-së. Bëjnë përjashtim pajisjet: laptop, HDD dhe USB, në funksion të punës jashtë orarit, pajisje të dhëna nga institucioni për qëllime pune. Në rastin kur dëshirohet përdorimi i pajisjeve të jashtme elektronike në mjediset e AZHBR-së, për lidhjen e tyre në rrjetin e institucionit duhet marrë miratimi nga Specialisti i Teknologjisë së Informacionit.
16. Nuk lejohet instalimi i programeve kompjuterike shtesë në kompjuterat e institucionit pa miratimin e punonjësit të Teknologjisë së Informacionit.
17. Të gjitha programet kompjuterike të instaluara në kompjuterat e institucionit, si dhe materialet i importuara në to, duhet të jenë të mbrojtura me programe antivirus. Specialisti i Teknologjisë së Informacionit zotëron një program antivirus me licenca nga AKSHI, i cili duhet të përdoret për të gjithë kompjuterat e institucionit.

8. Garantimi i kushteve të sigurisë për teknologjinë e informacionit

1. Specialisti i Teknologjisë së Informacionit duhet të njoftohet për të gjitha incidentet që ndikojnë në besueshmërinë, integritetin ose aksesueshmërinë e të dhënave apo të pajisjeve të teknologjisë së informacionit. Vjedhja, hyrja e paautorizuar, infektimi nga viruset janë raste për të cilat parashikohen masa sipas legjislacionit në fuqi.
2. Në rast se konstatohet që pajisjet e teknologjisë së informacionit janë dëmtuar në çfarëdo mënyre, Specialisti i Teknologjisë së Informacionit 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;
    d. mendimin për procedimin e mëtejshëm;
    e. emrat dhe firmat e specialistëve që ekzaminuan rastin;
    f. dh. emrin dhe firmën e personit që ka në ngarkim pajisjen.
3. Për të krijuar kushte optimale të sigurisë, Specialisti i Teknologjisë së Informacionit përpunon sistemin e fjalëkalimeve për:
    a. platformën OËA outlook (Microsoft Exchange Server Outlook);
    b. shërbimin e printimit të centralizuar, shareprinting;
    c. kompjuterat në përdorim;
    d. ç. shërbimin ëireless.
4. Për shkaqe sigurie, Specialisti i Teknologjisë së Informacionit nuk mund të transmetojë dhe të marrë përmes telefonit fjalëkalimet. Për të gjitha shërbimet e teknologjisë së informacionit, për të cilat është e nevojshme përdorimi i fjalëkalimit, Specialisti i pajis të gjithë punonjësit me një fjalëkalim fillestar, i cili është i detyruar nga përdoruesit të ndryshohet në hyrjen e parë.
5. Punonjësi i Teknologjisë së Informacionit aplikon politikat e sigurisë së fireëall-it të rrjetit kompjuterik. Në rastet kur ndryshojnë politikat apo urdhrat e brendshëm mbi organizimin dhe funksionimin e AZHBR-së, duhet të bëjë ndryshimet e nevojshme në konfigurimet e tij.

9. Posta elektronike

Përdorimi i postës elektronike

1. Sistemi i postës elektronike duhet të përdoret vetëm për qëllime pune.
2. Specialisti i IT-së monitoron problematikat eventuale lidhur me ecurinë e postës elektronike dhe të përdorimit të internetit.
3. Punonjësit e Institucionit të AZHBR-së janë përgjegjës direkt mbi keqpërdorimin e postës elektronike në pajisjet mobile private.
4. Administrimi i postës elektronike zyrtare kryhet në përputhje me standardet e vendosura nga Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI), në rolin e administratorit. Në përdorimin e postës elektronike duhen pasur parasysh rregullat e hartuara nga AKSH-i në "Rregullore për përdorimin e postës elektronike në Administratën Publike".

Personi përfitues (useri i postës elektronike) është informuar se institucioni do t'i përdorë të dhënat e tij personale në përputhje të plotë me përcaktimet e ligjit nr. 9887, datë 10.3.2008, "Për Mbrojtjen e të Dhënave Personale", të ndryshuar, Aktet nënligjore të Komisionerit për Mbrojtjen e të Dhënave Personale, si dhe legjislacionin shqiptar në fuqi.
Ligjit nr. 10273, datë 29.4.2010, "Për Dokumentin Elektronik", ligjit nr. 9918, datë 19.5.2008, "Për komunikimet elektronike në Republikën e Shqipërisë", të ndryshuar.

5. Për pajisjen me postë elektronike zyrtare, adresë email-i nën domanin e institucionit, Specialistit të IT-së i vihet në dispozicion Urdhëri i emërimit të punonjesit, dhe më pas bëhet e-mail zyrtar drejt departamentit përkatës tek AKSHI për hapjen e postës elektronike zyrtare.
6. Në momentin që një punonjës pezullohet apo largohet nga puna, serisht Drejtorisë së Teknologjisë së Informacionit i vihet në dispozicion urdheri përkatës dhe vijohet me mbylljen e aksesit të postës elektronike (disable për një periudhe 1 mujore dhe më pas fshirje nga Active Directory nëse punonjësi largohet përfundimisht);

9.1. Fjalëkalimet

Të gjithë përdoruesit e Agjencisë instruktohen në lidhje me mënyrat e administrimit të fjalëkalimeve. Këtu futet:

- zgjedhja e fjalëkalimit fillestar;
- ndryshimi i fjalëkalimit dhe këshilla të njohura sigurie për zgjedhjen e tij;
- mbrojta e fjalëkalimit si dhe ndalimi i dhënies së fjalëkalimit midis përdoruesve;
- inicializimi ose mbivendosja e fjalëkalimit (në qoftë se një llogari përdoruesi është mbyllur ose në qoftë se përdoruesi ka harruar fjalëkalimin). Mbivendosja e fjalëkalimit duhet të bëhet vetëm nga punonjësi i autorizuar i teknologjisë së informacionit pas një kërkese me e-mail.

Përdoruesve u kërkohet të firmosin një formular ku pranojnë se ata i kanë lexuar e i kanë kuptuar rregullat, dhe se do t'i zbatojnë ato. Kjo proçedurë përfshihet në procedurat e punësimit të personelit të Agjencisë.

9.1.1 Monitorimi i profileve të përdoruesve

Është e rëndësishme të garantohet që:

- vetëm përdoruesve të duhur u është lejuar akses në sistemet e Agjencisë (janë fshirë\çaktivizuar të gjitha llogaritë që kanë skaduar);
- përdoruesit nuk kanë privilegje aksesimi të niveleve më të larta nga ato që u duhen për të kryer punën e tyre (është hequr "shtimi i privilegjeve").

9.1.2 Politikat e password-eve të aplikuara në infrastrukturën tonë:

9.1.3 Historiku i Passëord-it – 24 passëord-e të mbajtur mend;

9.1.4. Koha maksimale e vlefshmërisë së passëord-it – Passëord-i do të skadojë për 90 ditë;

9.1.4. Koha minimale e vlefshmërisë së passëord-it – Passëord-i mund të ndryshohet në logimin e parë;

9.1.5. Password-i duhet të përmbushë kërkesat e kompleksitetit.:

- nuk duhet të përmbajë emrin e përdoruesit ose pjesë të emrit të plotë, në më shumë se 3 karaktere
- duhet të jetë të paktën 14 karaktere i gjatë;
- duhet të përmbajë tri karaktere nga katër kategoritë e mëposhtme:
- shkronja të mëdha (nga A në Z);
- shkronja të vogla (nga a në z);
- numra nga 0 deri 9;
- Simbole speciale ose karaktere joalfabetike (për shembull: !, $, #, % etj.).

Shumë nga aplikacionet dhe sistemet kompjuterike janë të mbrojtura me një fjalëkalim. Për arsye sigurie, këto fjalëkalime herë pas here duhet të ndryshohen (çdo 3 muaj).

Disa rregulla mbi përdorimin dhe vendosjen e fjalëkalimeve:

a. Fjalëkalimi për aksesimin e burimeve të teknologjisë dhe informacionit (p.sh., kompjuteri) nuk duhet të ndahet me persona të tjerë brenda apo jashtë institucionit. Punonjësit janë përgjegjës për ruajtjen dhe mosshpërndarjen e këtij informacioni.
b. Gjatë vendosjes së fjalëkalimit, duhet të vendoset një fjalë apo frazë që mund të mbahet mend lehtësisht, por jo diçka që identifikohet lehtësisht, si p.sh.: emri apo adresa. Këshillohet të përdoret një fjalëkalim i fortë, që përmban shkronja të mëdha dhe të vogla, numra dhe karaktere pikësimi.

10. Përditësimi i faqes zyrtare të internetit

1. Agjencia për Zhvillim Bujqësor dhe Rural duhet të publikojë çdo informacion të nevojshëm për publikun, si dhe njoftime të tjera. Përditësime në kategori si Programi i Transparencës, njoftime punësimi, statistika dhe raporte të ndryshme.
   Përditësimi i faqeve zyrtare të internetit (www.azhbr.gov.al dhe www.ipard.gov.al) të Agjencisë për Zhvillim Bujqësor dhe Rural kryhet nga Specialisti i IT-së dhe Sektori i Burimeve Njerëzore dhe Shërbimeve Mbështetëse, dhe ndiqet nga:
   a. Drejtori i Drejtorisë së Teknologjisë së Informacionit;
   b. Drejtori i Drejtorisë Juridike dhe Shërbimeve Mbështetëse, që ndjek dhe mbikëqyr procesin e përditësimit të të dhënave;
2. Përditësimi i faqes zyrtare kryhet sa herë që kërkohet, duke u nisur nga kerkesat e ardhura në e-mailn nga personat përgjegjës.
3. Materialet dhe informacionet që hidhen, përditësohen në faqen zyrtare të web-it, janë të formatuara, të miratuara dhe të konfirmuara, në versionin e tyre formal dhe zyrtar, të përdorura nga çdo drejtori sipas fushës së aktivitetit të tyre.
4. Specialisti i IT-së ruan një backup të plotë të faqes së internetit në një HDD (Hard Disk Drive) të jashtëm çdo muaj.

5. Komunikimi dhe aksesimi i faqes web nga jashtë rrjetit GOVNet bëhet nëpërmjet VPN - Rrjete private virtuale, të cilat ofrojnë siguri të lartë, nëpërmjet futjes të një UserID-je (username) dhe një fjalëkalimi (passëord-i) specifik për aksesimin e saj.

11. Dhoma e serverave

Përdorimi i infrastrukturës TIK në dhomën e serverave.

□ Drejtori i DIT, specialistët e IT-së dhe OSI kanë autorizim për akses në zonën e ruajtjes dhe dhomën e serverit.

□ Të gjithë përdoruesit e tjerë duhet të marrin autorizimin, të nënshkruar nga Drejtori i Përgjithshëm i AZHBR-së ose Drejtori i DIT-it për akses në dhomat teknike dhe dhomën e serverit, sipas formularit për aksesin në dhomën e serverit.

□ Formularët bosh për autorizim mbahen nga DIT-i, i cili plotëson formularin sipas nevojës. Autorizimi plotësohet në dy kopje. Njëra i dorëzohet përdoruesit ose punonjësit nga furnizuesi i jashtëm i autorizimit, dhe tjetra mbahet nga DIT-i.Specialisti i Teknologjisë së Informacionit mban dhe plotëson një formular me të dhënat përkatëse për vizitorët (formular për hyrje-dalje në dhomën e serverit), punonjësit e mirëmbajtjes dhe persona të tjerë të huaj, që aksesojnë ambientet kritike në dhomën e serverave. 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.

1. Ndalohet duhani.
2. Ndalohet përdorimi i mjeteve ngrohëse.
3. Mjetet për mbrojtjen nga zjarri duhet të jenë gjithmonë në gjendje pune dhe në vende të dukshme.

12. Backup-i i të dhënave

Drejtoria e Teknologjisë së Informacionit është përgjegjëse për të siguruar që të gjitha të dhënat sensitive të mbajtura në serverat e Agjencise t'u bëhet *backup* (kopje) i rregullt në përputhje me procedurat e përcaktuara, për çdo sistem.

Kopjet (backup-et) e të dhënave duhet të ruhen në vende të mbrojtura nga zjarri dhe jashtë ambienteve ku mbahen serverat prej të cilëve janë marrë ato.

Kopjet (backup) e të dhënave duhet të testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme.

Procedurat e rikrijimit (restore) të të dhënave duhet të testohen rregullisht për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar.

12.1.1. Të dhënat që ndodhen në kompjuterat personalë të përdoruesve

Çdo punonjës, i cili ruan të dhëna në një kompjuter personal, është *përgjegjës personalisht* për të siguruar kopjet e duhura të *backup*-it për të mbrojtur të dhënat nga humbjet duhet të firmosë një dokument të pranimit të kësaj përgjegjësie.

12.1.2 Mbajtja e log-eve

Është e detyrueshme të mbahen e të ruhen *log-e* (shënime të shkurtuara) për të gjitha aksesimet në sistemet e Agjencisë, për të gjithë përdoruesit e brendshëm e të jashtëm

13.Të drejtat dhe detyrimet

Institucioni e trajton dhe e vlerëson të gjithë informacionin elektronik si çështje të brendshme. Për këtë arsye, institucioni do të ndjekë të gjitha praktikat dhe procedurat përkatëse për sigurimin, ruajtjen, si dhe administrimin e informacionit në përputhje me dispozitat ligjore në fuqi.

1. Të drejtat dhe detyrimet e Specialistit të Teknologjisë së Informacionit:
   Specialisti i Teknologjisë së Informacionit në ushtrimin e detyrës së tij duhet të:
   a. Zbatojë legjislacionin në fuqi për mbrojtjen e të dhënave personale, konfidencialitetin e komunikimit, lirinë dhe të drejtat e njeriut.
   b. Sigurojë 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. Sigurojë që për çdo kompjuter të lidhur me internet të jete i futur në domain azhbr.gov.al, të ketë të instaluar të gjithe Agjentët e sigurisë, të ketë të instaluar programet e nevojshme për të realizuar punët sipas përshkrimeve të punës perkatese, të ketë të instaluar pajisjet për printim/scanim si dhe të aksesojnë postën elektronike.
   d. Sigurojë aksesin në internet dhe pajisjen me fjalëkalime individuale të punonjësve.
   e. Ndërmarrë këshillime, që mund të përfshijnë trajnime intensive rreth rregullores dhe përdorimit të pajisjeve.
   f. Bashkëpunojë me organet kompetente për sigurimin e informacionit të nevojshëm për çështje të sigurisë kombëtare dhe në rastet e tjera të parashikuara me ligj.
   g. Gjithashtu, me qëllim sigurimin e mbarëvajtjes së funksionimit të rrjetit të internetit dhe rritjen e eficiencës së tij, punonjësi i Njësisë së Teknologjisë së Informacionit mund të monitorojë në përputhje me dispozitat ligjore, nëse është e mundur, teknikisht:
      - volumin e aktivitetit në internet dhe kapacitetin e sistemit, me qëllim sigurimin e funksionimit të tij në mënyrë eficiente;
      - faqet e aksesuara dhe kohën e shpenzuar për lundrimin e tyre.
2. Të drejtat dhe detyrimet e punonjësve të institucionit:
   a. Punonjësi ka të drejtë të përdorë shërbimin e internetit për:
      - komunikim dhe informim direkt në lidhje me procesin e punës në institucion;
      - komunikim dhe bashkëpunim për zhvillimin e tij profesional;

- kërkime, studime, standarde, këshillime, analiza dhe aktivitete profesionale dhe sociale të lidhura më punën dhe në përputhje me detyrat e punonjësve në Administratën Publike;
- çdo aktivitet zyrtar që nuk kërkon një nivel sigurie të lartë të rrjetit (p.sh., aksesi në rrjetet e klasifikuara).

b. Punonjësit janë përgjegjës për ruajtjen e fshehtësisë së fjalëkalimeve personale (username/passëord) të tyre. Ata duhet të përdorin ato dhe vetëm ato fjalëkalime, dhe nuk duhet t'i shpërdorojnë.

c. Punonjësit duhet të jenë të vëmendshëm që të mbyllin llogarinë e tyre personale në përfundim të punës.

d. Punonjësit janë përgjegjës për raportimin, nëse janë në dijeni, të shkeljeve dhe rreziqeve potenciale rreth sigurisë, si dhe të aktiviteteve joetike, që shkelin udhëzimet ose kodin e praktikës së institucionit.

e. Punonjësit janë, gjithashtu, përgjegjës për sigurimin e pajisjeve që përdorin, nga keqpërdorimi, aksesi i paautorizuar ose dëmtimi i qëllimshëm gjatë punës.

3. Punonjësit i ndalohet përdorimi i shërbimit të internetit për të:
   (i) shkarkuar, përdorur dhe/ose shpërndarë:
   (ii) materiale me përmbajtje diskriminuese (raciale, kulturore, politike, gjinore apo fizike);
   (iii) literaturë rreth drogave;
   (iv) materiale pornografike;
   (v) materiale që përmbajnë shpifje.
   (vi) favorizuar biznesin privat – përfshirë këtu reklamat, lajmërimet etj., apo për qëllime politike
   (vii) dërguar jashtë institucionit, shpërndarë, kopjuar ose modifikuar skedarët dhe të dhëna të tjera që janë konfidenciale.
   (viii) shfrytëzuar identitetin e një personi tjetër, gjatë përdorimit të internetit.
   (ix) mbledhur fonde publike dhe/ose për aktivitete që kanë të bëjnë me marrëdhëniet me publikun, jo specifikisht të lidhura me aktivitetin shtetëror të institucionit;
   (x) shkëmbyer mesazhe (Instant Messaging) ose bashkëbiseduar (si CHAT) për qëllime personale apo abuzuese me dokumentet elektronike të AZHBR-së.
   (xi) transmetimi i dokumenteve ose i mesazheve të klasifikuara nëpërmjet internetit është i ndaluar, përveç rasteve kur specifikohet nga Drejtoria e Sigurimit të Informacionit të Klasifikuar (DSIK).

KREU III

PROCEDURAT E FILLIMIT DHE TË SHKËPUTJES NGA PUNA

14. Për punonjësit që fillojnë ose përfundojnë marrëdhënien e punës Përgjegjësia për të garantuar zbatimin e procedurave të sigurisë

1. Drejtorët e drejtorive janë përgjegjës për të garantuar që punonjësve të rinj të strukturave përkatëse u është dhënë niveli i duhur i aksesimit në pajisjet dhe në sistemet e AZHBR-së, përfshi këtu llogaritë e përdoruesve për kompjuterat, miratimin e lejes së aksesimit të infrastrukturës, të dhomave të serverave, të nyjave të rrjetit, kartën elektronike të hyrje-daljes për aksesimin e mjediseve etj.
2. Çdo pjesëtari të ri, që i bashkohet personelit të institucionit, duhet t'i kërkohet, aty ku është e nevojshme, të firmosë për të gjitha pajisjet e aksesimit, duke pranuar njëkohësisht kushtet e përdorimit të tyre.
3. Të gjithë pjesëtarëve të rinj u jepen instruksione të plota për procedurat e teknologjisë së informacionit dhe në veçanti për kërkesat në lidhje me çështjet e sigurisë.
   Këto instruksione duhet të përfshijnë të paktën:
   - përdorimin e përgjithshëm të mjeteve të teknologjisë së informacionit;
   - ndihmën e kualifikuar nga Drejtoria e Teknologjisë së Informacionit dhe Drejtoria Juridike dhe e Shërbimeve Mbështetëse;
   - familjarizimin me Politikën e Sigurisë së AZHBR-së dhe rregullat e tjera;
   - trajtimin e informacioneve;
   - politikën e përdorimit të internetit, të email-it etj.;
   - rregullat për fjalëkalimet.

Kjo bëhet para se atyre t'u hapet ndonjë llogari përdoruesi ose t'u jepen privilegje për të aksesuar infrastrukturën e AZHBR-së.

Drejtorët janë përgjegjës për të garantuar zbatimin e procedurave të sigurisë në rastet kur pjesëtarë të personelit të tyre largohen nga puna.

Është përgjegjësi e çdo Drejtori në bashkëpunim me Specialistin e Burimeve Njerëzore dhe Shërbimeve Mbështetëse të sigurojë, që kur një pjesëtar i personelit largohet nga puna, t'i hiqen të gjitha të drejtat e aksesimit dhe t'i kërkohet të dorëzojë të gjitha kartat e aksesimit, çelësat, kompjuterat etj., të cilët i ka pasur në përdorim apo në ngarkim.

Procedurat e teknologjisë së informacionit për mbylljen e llogarisë së përdoruesit dhe për heqjen e të drejtave të aksesimit në infrastrukturës së AZHBR-së, duhet të bëhen para se pjesëtari i stafit të largohet fizikisht nga ambienti i punës.

Personi përgjegjës i caktuar nga Drejtoritë (IT-ja) informohet, sa më shpejt që të jetë e mundur, kur ndonjë pjesëtar i personelit e lë punën ose afati i tij i punësimit mbaron për çdo lloj arsyeje.

Është përgjegjësi e Drejtorit të Drejtorisë përkatëse, të sigurojë që kjo gjë të kryhet sa më parë.

Specialisti i IT-së duhet të njoftohet zyrtarisht, për largimet nga puna, si dhe duhet të udhëzohet për korrektimin e të drejtave të përdoruesit që do të largohet. Zgjedhjet për korrektimin e të drejtave do të përfshijnë:

- fshirjen e menjëhershme të llogarisë së përdoruesit;
- heqjen e privilegjeve të aksesimit.

Është përgjegjësi e drejtorit të drejtorisë përkatëse të kërkojë nivelin e duhur të korrektimit.

15.Trajnime

Personat që kanë akses në asetet e informacionit të Agjencisë janë të detyruar të jenë të vetëdijshëm për rregullat dhe standardet e sigurisë në Agjencise. I gjithë personeli duhet të marrë trajnimin e nevojshëm për rregullat dhe për procedurat organizative dhe të sigurisë. Ky trajnim kryhet sa më shpejtë që të jetë e mundur pas fillimit të punës së punonjësve të rinj.

Objektivat e edukimit në lidhje me sigurinë duhet të jenë:

- krijimi i kulturës së sigurisë në të gjithë Autoritetin;
- edukimi i personelit mbi pasojat e veprimeve të tyre mbi sigurinë e informacionit;
- udhëzimi i personelit për rregullat dhe procedurat e sigurisë sipas pozicioneve përkatëse;
- përcaktimi i përgjegjësive që mban çdo person mbi sigurinë dhe detyra e secilit për të raportuar çdo shkelje të rregullave të sigurisë.

Gjithashtu, i gjithë personeli duhet të trajnohet për përdorimin korrekt të sistemeve kompjuterike dhe të aseteve të informacionit. Kjo bëhet para se t'u jepet e drejta të aksesojnë sistemet.

Të gjithë specialistët e Drejtorisë së Teknologjisë së Informacionit duhet të marrin rregullisht trajnime përmirësuese në fushat e tyre të specializimit. Kjo duhet të përfshijë veçanërisht personelin e sigurisë, administratorët e bazave të të dhënave, administratorët e sistemeve operative dhe sistemeve të sigurisë (psh Firewall, IDS, IPS, Network Management, Content Filtering, Application Security etj.)

16.Analiza e riskut

Regjistri i riskut bazohet në Ligjin nr. 10296, datë 08.07.2020 "Për menaxhimin financiar dhe kontrollin", i ndryshuar, si dhe akteve ligjore dhe nënligjore.

Drejtoria TIK e AZHBR kryen një analizë periodike (një herë në 6 muaj) zyrtare të riskut për asetet e informacionit të institucionit sipas procedurave që rekomandohen në standardet ndërkombëtare, dhe regjistri i riskut dorëzohet pranë Oficerit të menaxhimit të Riskut.

Rezultatet e analizës së riskut përdoren për të përcaktuar strategjitë për zbutjen e çdo risku që identifikohet. Në momentin kur kemi një risk të ri potencial, së pari do të trajtohet tek plani operacional i cili ka frekuencë zbatueshmërie 1 herë në 6-muaj. Nëse risku do të vijojë pa gjetur zgjidhje dhe kthehet në risk potencial atëherë identifikohet tek regjistri i riskut i vitit që vjen, duke nxjerrë në pah një risk të ri, i cili ndikon sipas peshës që ka në performancë.

Analiza e riskut të sigurisë së informacionit kryhet duke marrë parasysh kërcenimet, dobësite dhe impaktin.

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

- Identifikimi i aseteve:
  a) Dobësitë;

b) Kërcënimet;
c) Kontrollet;

- Vlerësimi sipas nivelit të riskut (Ulët, Mesëm, Lartë);
- Trajtimi:
  a) Rregullimi (Implementimi i një kontrolli që pothuajse ose plotësisht i përgjigjet riskut themelor);
  b) Zbutja e riskut (mitigation);
  c) Transferimi i riskut;
  d) Pranimi i riskut në rastet kur risku është shumë i ulët dhe mund të pranohet;
  e) Shmangia e riskut
- Komunikimi brenda Agjencisë;
- Monitorimi i vazhdueshëm.

KREU IV

DISPOZITA TË FUNDIT

17.Hyrja në fuqi

Ky akt hyn në fuqi me miratimin nga Drejtori i Përgjithshëm dhe bëhet pjesë e pandarë e Rregullores së Brendshme të AZHBR-së.