REPUBLIKA E SHIPËRISË
SHOQËRIA "ALBPETROL" SH.A.
KËSHILLI MBIKËQYRËS

VENDIM

Nr. 02, datë 21.02.2025

PËR
MIRATIMIN E RREGULLORES "MBI MËNYRËN E DOKUMENTIMIT DHE IMPLEMENTIMIT TË MASAVE TË SIGURISË NË INFRASTRUKTURAT E RËNDËSISHME TË INFORMACIONIT NË SHOQËRINË "ALBPETROL" SH.A"

Bazuar në ligjin nr. 9901, datë 14.04.2008, "Për tregëtarët dhe shoqëritë tregtare", të ndryshuar, Vendimin nr. 570, datë 3.10.2018, të Këshillit të Ministrave, "Për Këshillat Mbikëqyrës të Shoqërive Anonime Shtetërore", dhe Statutin e shoqërisë "Albpetrol" Sh.A, Këshilli Mbikëqyrës i Shoqërisë "Albpetrol" Sh.A., në mbledhjen e datës 21.02.2025

V E N D O S I:

1. Miratimin e rregullores "Mbi mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat e rëndësishme të informacionit në shoqërinë "Albpetrol" Sh.A", sipas tekstit bashkëlidhur dhe pjesë përbërëse e këtij vendimi.
2. Ngarkohet Administratori i Shoqërisë "Albpetrol" Sh.A., për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi menjëherë.

KËSHILLI MBIKQYRËS

Ilia GJERMANI	**KRYETAR**	_____
Ami KOZELI	**ANËTAR**	_____
Ermal NUFI	**ANËTAR**	_____
Evis MAMAJ	**ANËTAR**	_____
Florenca KORBI	**ANËTAR**	_____
Edmond AHMETI	**ANËTAR**	_____

RREGULLORE

MBI MËNYRËN E DOKUMENTIMIT DHE IMPLEMENTIMIT TË MASAVE TË SIGURISË NË INFRASTRUKTURAT E RËNDËSISHME TË INFORMACIONIT NË SHOQËRINË "ALBPETROL" SH.A

2025

www.albpetrol.al

PËRMBAJTJA

Nr.		Emërtimi	Faqe
Kreu	**I**	**MASAT ORGANIZATIVE**	
Neni	1	Qëllimi	
Neni	2	Baza Ligjore	
Neni	3	Fusha e Zbatimit	
Neni	4	Parimet e Sigurisë	
Neni	5	Mbrojtja Fizike	
Neni	6	Politika e kompanisë për sigurinë e informacionit	
Neni	7	Njësia/Struktura "Computer Security Incident Response Team" CSIRT - (Ekipi i Reagimit ndaj Incidenteve të Sigurisë Kompjuterike)	
Neni	8	Rishikimi i Politikës së Sigurisë së Informacionit	
Neni	9	Menaxhimi i rrezikut kibernetik	
Neni	10	Kërkesat e sigurisë për kontratat me palët e treta	
Neni	11	Siguria e burimeve njerëzore dhe aksesit të personave	
Neni	12	Menaxhimi i Aseteve	
Neni	13	Cikli i menaxhimit te incidentit kibernetik	
Neni	14	Menaxhimi i vazhdimësisë së punës	
Neni	15	Menaxhimi i sigurisë së informacionit	
Neni	16	Kontrolli dhe Auditi	
Kreu	**II**	**MASAT TEKNIKE**	
Neni	17	Siguria Fizike	
Neni	18	Mjetet për analizë dhe mjetet shtesë	
Kreu	**III**	**Zbatimi dhe hyrja në fuqi**	
Neni	19	Zbatimi	
Neni	20	Hyrja në fuqi	
		Klasifikimi i incidenteve – Legjenda e ngjyrave	
		Tabela 1	
		Bllokskema 1	
		Bllokskema 2	

RREGULLORE

MBI MËNYRËN E DOKUMENTIMIT DHE IMPLEMENTIMIT TË MASAVE TË SIGURISË NË INFRASTRUKTURAT E RËNDËSISHME TË INFORMACIONIT NË SHOQËRINË "ALBPETROL" SH.A

KREU I
MASAT ORGANIZATIVE

Neni 1
Qëllimi

Qëllimi i rregullores "Mbi mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit në shoqërinë "Albpetrol" Sh.A", është përcaktimi i parimeve dhe rregullave të Sigurisë së Informacionit në "Albpetrol" Sh.A, dhe përcaktimi i përgjegjësive për veprimet që lidhen me sigurinë me qëllim ruajtjen e integritetit, disponueshmërisë dhe konfidencialitetit të aseteve të informacionit, si dhe garantimin e përputhshmërisë me aktet ligjore që rregullojnë çështjet e sigurisë së informacionit në shoqëri.

Neni 2
Baza Ligjore

Rregullorja është hartuar në bazë të rregullores "Mbi mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit v3.0", të Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, si dhe Vendimit Nr. 553, të Këshillit të Ministrave, datë 15.07.2020 "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit", të ndryshuar.

Neni 3
Fusha e Zbatimit

Kjo rregullore është e detyrueshme për zbatim nga të gjithë përdoruesit/aksesuesit e sistemeve të "Albpetrol" Sh.A dhe informacionit që përdorin, të cilët janë përgjegjës për garantimin e mbrojtjes dhe sigurisë së tyre. Përdoruesit e sistemeve në nivel *user* apo *administrator* kanë një kontribut për të dhënë në lidhje me përdorimin e sigurt të teknologjisë dhe informacionit.

Neni 4
Parimet e Sigurisë

Në përputhje me Politikën e Sigurisë së Infromacionit, objektivi kryesor për sigurinë e informacionit është ruajtja e integritetit, disponueshmërisë dhe konfidencialitetie të aseteve të informacionit në Albpetrol sh.a., të cilat përcaktohen si më poshtë:

- Integriteti

Informacioni duhet të jetë i plotë, i saktë dhe i qëndrueshëm ndaj modifikimeve të paautorizuara ose ndaj dëmtimev, gjatë gjithë kohës

- Disponueshmëria

Informacioni bëhet i aksesueshëm sa herë që është e nevojshme. Kjo do të thotë që të gjitha informacionet dhe të gjitha sistemet e infromacionit janë të disponueshme dhe operacionale sa herë që nevojitet një gjë e tille.

- Konfidencialiteti

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

Neni 5
Mbrojtja Fizike

Të gjitha asetet e informacionit në "Albpetrol" Sh.A mbrohen në shkallën më të lartë nga dëmtimet fizike.

Neni 6
Politika e kompanisë për sigurinë e informacionit

1. Politika e Sigurisë së Informacionit synon::
   - të mbrojë sistemet desktop, serverat, pajisjet e ruajtjes së të dhënave, sistemet e komunikimit, firewall, router, switchet dhe pajijset e lëvizshme në pronësi të "Albpetrol" Sh.A.
   - të mbrojë platformat informatike, software, sistemet e operimit dhe aplikacionet që përdor "Albpetrol" Sh.A.
   - të mbrojë të dhënat, informacionet, dokumentet, prezantimet, bazat e të dhënave ose burime të tjera informacioni të "Albpetrol" Sh.A.
2. Politikat e Sigurisë së Informacionit përcakton elementët e nevojshëm për të siguruar që kontrollet e sigurisë së informacionit të mbeten të vlefshme me gjithë ndryshimet në teknologji.
3. Dokumenti "Politikat e Sigurisë së Informacionit" publikohet dhe i komunikohet të gjithë punonjësve si dhe palëve të tretat të përfshira në kontrata shërbimi.

Neni 7
Njësia/Struktura "Computer Security Incident Response Team" CSIRT (Ekipi i Reagimit ndaj Incidenteve të Sigurisë Kompjuterike)

1. Njësia/Struktura CSIRT është përgjegjëse për monitorimin e politikave të sigurisë së informacionit dhe ka për detyrë
   a. Monitorimin e sistemeve për kërcënime të sigurisë për të siguruar konfidencialitetin, integritetin dhe disponueshmërinë e të gjitha të dhënave kritike të informacionit dhe objekteve të përpunimit të informacionit;
   b. Zbulimin e incidenteve të sigurisë;
   c. Analizimin e incidenteve;

d. Koordinimin e reagimit ndaj incidenteve;
e. Përmirësimin e sigurisë pas incidenteve, për të siguruar vazhdimësinë e aktivitetit të "Albpetrol" Sh.A, duke parandaluar dhe minimizuar ndikimin e tyre në mënyrë që të ruhet përputhshmëria ligjore, rregullatore dhe kontraktuale;
f. Edukimin dhe ndërgjegjësimin e përdoruesve për çështjet e sigurisë përmes trajnimeve

Neni 8
Rishikimi i Politikës së Sigurisë së Informacionit

Shoqëria "Albpetrol" Sh.A bën rishikimin e politikës së sigurisë së informacionit në bazë vjetore. Rishikimet e politikës janë të nevojshme kur:

- Ka ndryshime në politikat legjislative, të cilat sjellin implikime të sigurisë së informacionit;
- Planifikohet dhe implementohet një teknologji e re;
- Raportet e auditimit ose kontrollet e sigurisë, identifikojnë rrezik të lartë për rrjedhje informacioni,
- Prezantohen standarde të reja kombëtare për sigurinë e informacionit, ose standardet ekzistuese rishikohen në mënyrë të konsiderueshme, për t'ju përgjigjur nevojave tekonologjike dhe të institucioneve;

Neni 9
Menaxhimi i rrezikut kibernetik

1. Menaxhimi i rrezikut kibernetik përcakton kërkesat për raportimin e një shkelje të mundshme në sigurinë e informacionit sa më shpejt të jetë e mundur. Kjo përfshin krijimin e procedurave dhe proceseve, në mënyrë që punonjësit të kuptojnë rolin e tyre në raportimin e ngjarjeve të sigurisë.
2. Një incident i sigurisë së informacionit është një ngjarje e vetme ose një seri ngjarjesh të padëshiruara apo të papritura që kërcënojnë sigurinë e informacionit në "Albpetrol" Sh.A. Incidentet e sigurisë së informacionit përfshijnë grumbullimin, përdorimin, aksesimin, asgjësimin apo transferimin e informacionit, qoftë aksidental ose të qëllimshëm, nga persona të paautorizuar për të marrë këtë informacionin.
3. Për të siguruar një përgjigje të shpejtë, efektive dhe të rregullt ndaj incidenteve të sigurisë së informacionit është e nevojshme kategorizimi i incidenteve në:
   a. Mohimi i shërbimit;
   b. Defekte të sistemeve;
   c. Fshirja e të dhënave (wiper);
   d. Ransomware, Spyware, Worm, Trojan, etj;
4. Nëse punonjësi dyshon se pajisja që po përdorë është e kompromentuar nga sulmet e kategorizuara më sipër duhet menjëherë të kontaktojë sektorin CSIRT.
5. Specialisti i njësisë/strukturës CSIRT verifikon pajisjen e kompromentuar dhe merr masat si më poshtë:
   a. Shkëput kabllon e rrjetit nga pajisja/ shkëput lidhjen Wifi;

b. Sigurohet që asnjë nuk po e përdor pajisjen dhe software;
c. Mban shënim çdo veprim që dyshon se mund të ketë lidhje me incidentin;
d. Raporton me shkrim incidentin tek Përgjegjësi i sektorit CSIRT;
e. Në asnjë moment nuk duhet ta fikë apo t'i bëjë restart pajisjes.

6. Njësia/Struktura CSIRT kryen monitorimit të rrjetit, sistemeve dhe pajisjeve fundore dhe, në rast të incidenteve, mban raporte me shkrim. Evidenca dhe raporti i paraqiten Drejtorit të Drejtorisë së Teknologjisë së Informacionit.
7. Struktura CSIRT për Albpetrol – Rregullat e Sigurisë Kibernetike

Caktimi i roleve dhe përgjegjësive të strukturës CSIRT (Computer Security Incident Response Team) brenda Drejtorisë së IT-së në shoqërinë "Albpetrol" Sh.A, në përputhje me rregullat e sigurisë kibernetike, përshkruhen në manualin e detyrave të pozicioneve të punës së shoqërisë.

8. Procedurat për Raportimin dhe Përgjigjen ndaj Incidenteve
   a. Kategoritë e Incidenteve
      Kritike: Sulme kibernetike të shkallës së lartë, ndërhyrje në sistemet kryesore.
      Serioze: Malware, ransomware, shkelje e të dhënave.
      Të Mesme: Përdorim i paautorizuar i sistemit, anomali në rrjet.
      Minore: Mesazhe phishing, tentativa të dështuara të qasjes.
   b. Procedura e Raportimit
      i. Raportimi i Incidentit:
         - Përdoruesit duhet të raportojnë incidentet përmes emailit ose telefonit në Helpdesk.
         - Helpdesk regjistron incidentin dhe e përcjell tek specialisti i sigurisë.
      ii. Vlerësimi dhe Eskalimi:
         - Specialisti i sigurisë analizon incidentin dhe vendos nëse duhet eskaluar. Nëse incidenti është serioz ose kritik, informohet eprori dhe Drejtori i IT-së.
      iii. Reagimi dhe Zgjidhja:
         - CSIRT merr masa për izolimin dhe zgjidhjen e problemit.
         - Për incidente të mëdha, kërkohet ndihmë nga CSIRT kombëtar ose institucione të tjera.
      iv. Dokumentimi dhe mësime të nxjerra:
         - Regjistrohet raporti për incidentin.
         - Përcaktohen masa për të parandaluar përsëritjen e incidentit.
   c. Rekomandime për Përmirësim
         - Trajnime të rregullta për stafin mbi sigurinë kibernetike.
         - Simulime periodike për reagimin ndaj incidenteve.
         - Përditësime të vazhdueshme të politikave të sigurisë.

Neni 10
Kërkesat e sigurisë për kontratat me palët e treta

1. Operatori ekonomik, ofruesit i shërbimeve të mirëmbajtjes së sistemeve hardware dhe software, përveç termave të kontratës, ka detyrim që:
   a. të njoftojë 24 orë përpara për emrat e stafit të cilët do të paraqiten onsite;
   b. të kërkojë me shkrim aksesin për VPN, Firewall, Router, Switchet;

c. të kërkojë me shkrim aksesin në makina virtuale, sisteme software;
d. në përfundim të kontratës së mirëmbajtjes, të njoftojë për revokim të aksesit.

2. Operatori ekonomik që ofron shërbime të mbulimit me kamera, përveç termave të kontratës, ka detyrim që:
   a. të njoftojë me shkrim 24 orë përpara pikën e lidhjes me kamera që do të verifikojë, riparojë;
   b. të njoftojë për emrat e stafit që do të menaxhojë kredencialet e pajisjeve NVR, sistemeve të survejimit;
   c. Në përfundim të punës, të njoftojë për revokim të aksesit.
3. Njësia/Struktura CSIRT është përgjegjëse për dhënien e aksesit të sigurt operatorit ekonomik, bazuar në njoftimet që do të bëjë operatori.

Neni 11
Siguria e burimeve njerëzore dhe aksesit të personave

1. Punonjësit e shoqërisë "Albpetrol" Sh.A, përdorues të sistemeve të saj të informacionit, duhet të njohin, kuptojnë dhe veprojnë në përputhje me politikat dhe standardet e sigurisë së informacionit. Ata duhet t'i drejtohen Drejtorisë së Teknologjisë së Informacionit në lidhje me çështje/problematika mbi politikën e sigurisë së informacionit ose çdo shqetësimi tjetër në lidhje me të.
2. Punonjësi duhet të njohë asetet informatike për të cilat ai është përgjegjës dhe mënyrën se si duhen mbrojtur ato. Punonjësi duhet të respektojë të drejtat specifike që i jepen për aksesimin e sistemeve të informacionit në përputhje me detyrën dhe funksionin e tij.
3. Punonjësit e shoqërisë "Albpetrol" Sh.A organizohen në përputhje me strukturën organizative të saj dhe hierarkinë në të cilën ndodhet punonjësi. Atyre u vihet në dispozicion llogaria përkatëse personale, e cila hapet vetëm pas përdorimit të fjalëkalimit. Me fjalëkalimin, që i jepet nga Drejtoria e Teknologjisë së Informacionit, punonjësi logohet herën e parë, për të vijuar me ndryshimin e menjëhershëm të tij.
4. Përdoruesve të rrjetit informatik të shoqërisë "Albpetrol" Sh.A u ndalohet:
   - Futja në rrjet me një identitet tjetër;
   - Importimi apo eksportimi i aplikacioneve, lojërave etj.;
   - Instalimi ose ndryshimi, në çfarëdolloj mënyre, të pajisjeve kompjuterike apo programeve;
   - Regjistrimi ose përdorimi i adresën zyrtare të punës në rrjetet sociale, për argëtim etj.
5. Politikat dhe procedurat e marra për kontrollet e background si dhe udhëzimet përkatëse të personelit janë të raportuara dhe dokumentuara në politikat e brendshme të kompanisë.
   - Politikat dhe procedurat e marra për kontrollet e background përfshijnë:
     - Verifikimin e identitetit të punonjësve para pranimit në punë.
     - Kontrollin e përvojës dhe kredencialeve profesionale për pozitat që kanë akses në të dhënat sensitive.
     - Auditimin e historikut të punës për të identifikuar ndonjë problem të mundshëm në lidhje me sigurinë.

- Verifikimin e precedentëve penalë për punonjësit që do të punojnë në pozita kritike për sigurinë kibernetike.
- Nënshkrimin e marrëveshjeve për konfidencialitetin dhe sigurinë e informacionit para fillimit të punës.
- Udhëzimet përkatëse për Personelin

- Për të garantuar sigurinë kibernetike, punonjësit duhet të ndjekin udhëzime të qarta dhe të dokumentuara, të cilat përfshijnë:
  - Detyrimin për të njohur dhe zbatuar politikat dhe standardet e sigurisë së informacionit.
  - Kontaktimin e Drejtorisë së Teknologjisë së Informacionit për çështje të sigurisë.
  - Respektimin e nivelit të aksesit në sistemet e informacionit sipas detyrës dhe funksionit.
  - Përdorimin e llogarisë personale dhe ndërrimin e detyrueshëm të fjalëkalimit pas regjistrimit të parë.
  - Ndalimin e përdorimit të një identiteti të rremë për të hyrë në sistemin e kompanisë.
  - Ndalimin e importimit/eksportimit të aplikacioneve dhe instalimit të softuerëve të paautorizuar.
  - Ndalimin e përdorimit të adresave zyrtare të punës në rrjetet sociale.

6. Njësia/Struktura CSIRT është përgjegjëse për informimin dhe dokumentimin e fushatave të ndërgjegjësimit të punonjësve mbi sigurinë kibernetike, kërcënimet kibernetike, modelet e phishing etj.

Neni 12
Menaxhimi i Aseteve

1. Shoqëria "Albpetrol" Sh.A krijon inventarin e aseteve IT/OT (Software dhe Hardware) ku identifikohet vjetërsia, afektimi CIA (Konfidencialiteti, Integriteti, Disponueshmëria), vunerabilitetet. Inventari rishikohet çdo 6 muaj ose sa herë ka furnizime hardware dhe software.
2. Punonjësi i shoqërisë "Albpetrol" Sh.A ka përgjegjësi personale për sigurinë e informacionit që administron në të gjitha format e tij. Kjo përgjegjësi përfshin ndër të tjera të paturit e njohurive mbi rregullat që zbatohen në lidhje me sigurinë e informacionit.
3. Politika/procedura e menaxhimit të aseteve.
   Punonjësi duhet të kthejë asetet që ka pasur në përdorim në përfundim të marrëdhënies së punës ose ndryshimit të pozicionit të punës.
   - Kthimin:
     - E pajisjeve kompjuterike, software dhe pajisjeve të lëvizshme si laptop, tablet, PDA etj.
     - E aksesit virtual në sistemet që ka përdorur gjatë marrëdhënieve të punës.
   - Verifikimin e aseteve të kthyera me inventarët e aseteve;

- Kompesimin për asetet që nuk janë kthyer, në bazë të kritereve të përcaktuara në lidhje me amortizimin dhe vlerën e zëvendësimit për llojin e asetit që nuk është kthyer;
- Identifikimin e pajisjeve të aksesit, kartave dhe çelësave të pakthyer që mund të çojnë në akes të paautorizuar në sisteme, në mënyrë që të dhënat dhe sistemet e sigurisë të mund të jenë të mbrojtura;

4. Politika Clean Desk dhe kyçja e ekranit:
   - Të gjitha informacionet e ndjeshme, konfidenciale ose personale në formë të printuar (hard copy) ose elektronike duhet të sigurohen në fund të ditës së punës, ose në çdo kohë, kur nuk janë në përdorim aktiv;
   - Pajisjet informatike duhet të kyçen në çdo kohë, kur nuk janë në përdorim aktiv;
   - Kompjuterët duhet të fiken në fund të ditës së punës;
   - Laptopët duhet të mbyllen në sirtarë të sigurt;
   - Kur nuk nevojiten më, dokumente që përmbajnë informacione konfidenciale, të ndjeshme ose informacioni personal duhet të copëtohet ose të futet në asgjësim;
   - Fjalëkalimet nuk duhet të jenë të shkruar në copa letre apo në blloqe shënimesh;
   - Ekrani duhet të kyçet automatikisht pas 5 minutash, nëse nuk po përdoret.
5. Tipologji e detajuar e rrjetit dhe sistemeve të informacionit paraqitet sipas bllokskemës 2, bashkëlidhur dhe pjesë e kësaj rregulloreje.
6. Gjatë procesit të verifikimit të sistemeve mbahen evidenca dhe procesverbal ku përcaktohet lloji i sistemit, sistemi operativ, viti i blerjes, versionet e instaluara, vitet e mirëmbajtjes, nëse është "end of life".
7. Gjatë procesit të verifikimit të sistemeve të patch-imeve për pajisjet fundore dhe antivirusin mbahen evidenca dhe procesverbale për çdo pajisje informatike fundore pc, laptop, tablet, ku të përcaktohet lloji i sistemit, marka dhe numri serial i pajisjes, patch-imet që janë instaluar si dhe modeli dhe versioni i antivirusit të instaluar.

Neni 13
Cikli i menaxhimit te incidentit kibernetik

Menaxhimi i incidentit kibernetik përfshin disa faza, të cilat detajohen në formë skematike në bllokskemën 1.

1. Faza e parë është identifikimi i incidentit, i cili mund të realizohet nga vetë infrastruktura, nga palë të treta, nga sektorë të tjerë në Drejtorinë e Teknologjisë së Informacionit, ose nga sisteme të automatizuara që menaxhohen nga njësia/struktura CSIRT.
2. Faza e dytë është regjistrimi i incidentit, i cili kryhet në minutën e 30 pas identifikimit të incidentit. Në rastin e identifikimit të incidentit nga njësia/struktura CSIRT, regjistrimi i incidentit kryhet nga njësia/struktura CSIRT.
3. Faza e tretë është procesi i *triage*, i cili përfshin kategorizimin, prioritizimin, korrelimin e incidentit. Kategorizimi i incidentit realizohet sipas Tabelës 1, e cila është bazuar në modelin e AKSK për klasifikimin e incidenteve. Klasifikimi i incidenteve, në zbatim të akteve nënligjore në fuqi, parashikon 4 lloje dhe 13 kategori incidentesh. Bazuar në impaktin e incidentit, realizohet prioritizimi i tij. (Klasifikimi i incidenteve dhe tabela 1, bashkëlidhur kësaj rregulloreje dhe pjesë përbërëse e saj).

4. Izolimi
   Njësia/Struktura CSIRT në bashkëpunim me sektorë të tjerë të Drejtorisë së Teknologjisë së Informacionit kryhen izolimin e pajisjeve fundore ku është identifikuar incidenti.
5. Analiza e Incidentit
   Qëllimi i analizës së incidentit është të identifikojë shkakun e tij, shtrirjen e dëmit, natyrën e incidentit dhe strategjitë e mundshme të përgjigjes.
6. Forma e raportimeve te incidenteve kibernetike
   - Specialisti i njësisë/strukturës CSIRT raporton incidentin drejt nivelit epror/përgjegjësit ;
   - Përgjegjësi i njësisë/strukturës CSIRT raporton incidentin drejt Drejtorit të Drejtorisë së Teknologjisë së Informacionit;
   - Drejtori i Drejtorisë së Teknologjisë së Informacionit raporton incidentin drejt Drejtorit të Departamentit Administrativ, Administratorit dhe Autoritetit Kombëtar për Sigurinë Kibernetike;
   - Forma e raportimit:
     1. Bën thirrje telefonike (nëse nuk përgjigjet);
     2. Dërgohet mesazh (nëse nuk përgjigjet);
     3. Dërgohet email zyrtar.

Neni 14
Menaxhimi i vazhdimësisë së punës

1. Strategjia e vazhdimësisë së shërbimit: Pasi incidenti është raportuar dhe analizuar, Drejtoria e Teknologjisë së Informacionit fillon me pastrimin e komponentëve të incidentit në sistemet e prekura, sipas kategorisë së incidentit.
2. Politika Backup: Pas kryerjes së pastrimit të sistemeve / rrjeteve të prekura, mund të procedohet me rikuperimin e sistemit dhe rikthimin e tij në gjendje pune, në rastet kur është e mundur. Të dhënat e rikuperuara duhet të ruhen në një sistem të pastër , i cili duhet të jetë i izoluar nga pjesa tjetër e rrjetit. Në rastin e një procesi investigimi penal, rikthimi i sistemit në gjendje pune kryhet pas përfundimit të investigimi penal.
3. Verifikimi i konfigurimeve të RAID dhe evidencat: Verifikim i konfigurimeve RAID 1/5/6/10 për të shmangur humbjen e të dhënave sensitive dokumentohet direkt nga faqet e menaxhimit të hosteve, tape library apo storage.
4. Raporte të testimit të planeve rezervë (backup) dhe testimit të integritetit të tyre: Raportet e testimit të backup dhe integriteti i tyre testohen çdo 24 orë. Raporti i testimi i dërgohet me email personave përgjegjës.

Neni 15
Menaxhimi i sigurisë së informacionit

1. Raporti i monitorimit të pajtueshmërisë mbahet sa herë që pajtueshmëria e standardeve dhe kërkesat ligjore në fuqi ndryshojnë;
2. Raporti shoqërohet me standardet e reja, si dhe kërkesat ligjore të ndryshuara;
3. Raporti i përpiluar nga njësia/struktura CSIRT i dorëzohet Drejtorit të Drejtosisë së Teknologjisë së Informacionit;

4. Politika/procedurat për monitorimin e pajtueshmërisë dhe auditimit.
   Njësia/struktura CSIRT auditon rrjetet dhe sistemet në mënyrë periodike në mënyrë që të sigurojë përputhshmëri të plotë me politikat dhe udhëzimet e Autoritetit Kombëtar për Sigurinë Kibernetike (AKSK).

Neni 16
Kontrolli dhe Auditi

1. Politika/Procedura e auditit të brendshëm.
   Të gjitha strukturat (sektorët/drejtoritë) janë subjekt i një kontrolli zyrtar vjetor për të siguruar zbatimin e rregullave dhe standardeve të sigurisë. Përgjegjësit e aseteve të informacionit mbështesin rregullisht auditime për përputhjen e sistemeve të tyre me këtë rregullore. Të gjitha pajisjet kompjuterike kontrollohen nga Drejtoria e Teknologjisë së Informacionit, për përputhshmërinë me standardet e implementuara të sigurisë. Këto kontrolle përfshijnë ekzaminimin e sistemeve operacionale për t'u siguruar që kontrollet e sigurisë të pajisjeve dhe të programeve janë implementuar me korrektësi.
2. Raporti i auditit dhe plani i trajtimit.
   Raportet e auditimit nga palë të treta për sigurinë e informacionit do të trajtohen sipas afateve të vendosura në rekomandime. Drejtori i Drejtorisë së Teknologjisë së Infromacionit sëbashku me sektorin CSIRT përpilon planin e trajtimit për zbatimin e standardeve të sigurisë të gjetura nga auditimi i palëve të treta.

KREU II
MASAT TEKNIKE

Neni 17
Siguria Fizike

1. Aksesimi i të gjitha ambienteve të sistemeve të informacionit në Albpetrol Sh.A do të kontrollohet në çdo kohë, në mënyrë që të parandalohen humbjet ose kompromentimet e aseteve të informacionit dhe të aseteve të tjera.
2. Siguria fizike duhet të fillojë me vetë ndërtimin dhe duhet të kryhet një vlerësim i cënueshmërisë së sistemit. Ndërtimi duhet të ketë mekanizma të duhur kontrolli si:
   - Alarme të vendosura dhe aktivizuara jashtë orarit të punës;
   - Mekanizma të kontrollit të aksesit;
   - Kamera CCTV;
   - Mbrojtje ndaj dëmtimit (zjarr, përmbytje, vandalizëm);
3. Mjetet/fjalëkalimet e identifikimit dhe aksesit (kartat, çelësat, kodet e hyrjes etj.) duhet të ruhen nga punonjës të autorizuar për të aksesuar ato ambiente dhe nuk duhet t'i jepen askujt tjetër.
   Të gjitha ambientet kritike sigurohen me sisteme aksesimi dhe karta elektronike. Çdo punonjës i autorizuar për një ambient specifik pajiset me një kartë individuale aksesi. Është e detyrueshme mbajtja e logeve për të gjitha aktivitetet e aksesimit, kur sistemet e aksesimit të ambienteve e lejojnë një gjë të tillë.

Neni 18
Mjetet për analizë dhe mjetet shtesë

Mjetet për analizë dhe mjetet shtesë përcaktohen si më poshtë:

a. **Mjete për analizë të log-eve:**
   1. SPLUNK: analizë të logeve (SIEM)
   2. ELFK (ElasticSearch+Logstash+Kibana): analizë të logeve (SIEM)
   3. Security Onion: analizë të logeve (SIEM)
   4. WireShark: analizë të logeve network
   5. NetworkMiner: analizë të logeve network
   6. Apackets: analizë të logeve network
   7. Chainsaw: analizë të logeve Windows
   8. Sysinternals Suite: analizë të logeve Windows
   9. Event Log Explorer: analizë të logeve Windows

b. **Mjete për analizë malware:**
   1. Ghidra: reverse engineering
   2. REMnux: malware analyses dhe Reverse engineering
   3. Hybrid Analysis: malware analyses
   4. Analyze.intezer: malware analyses
   5. Cuckoo.cert: malware analyses
   6. Recorded future Sandbox: malware analyses and simulation
   7. AnyRun: Sandbox: malware analyses and simulation
   8. X64Debugger: malware analyses dhe Reverse engineering
   9. IDA: malware analyses dhe Reverse engineering
   10. CAPA: malware analyses dhe Reverse engineering
   11. DetectItEasy: malware analyses dhe Reverse engineering
   12. PE-Bear: malware analyses dhe Reverse engineering
   13. MD5SUM: malware analyses - për gjetjen e HASH të skedarëve
   14. Strings: malware analyses - për eksfiltrimin e stringjeve nga skedarët keqdashës
   15. Radare 2: malware analyses - për gjetjen e karakteristikave dhe instruksioneve të skedarëve keqdashës
   16. Binwalk: malware analyses - për gjetjen e karakteristikave të skedarëve keqdashës

c. **Mjetet shtesë**
   1. Wireshark,
   2. Nikto (Kali Linux),
   3. Httpstatus.io,
   4. Nmap (active scan),
   5. UrlScan,
   6. Virus Total,
   7. SNIPER,

8. Nessus Vulnerability Scanner

d. **Mjetet të tjera**

Në listën e mjeteve për analizë do të përfshihen dhe mjete të tjera, të paparashikuara në këtë rregullore, sipas përcaktimeve të Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.

KREU III
ZBATIMI DHE HYRJA NË FUQI

Neni 19
Zbatimi

Rregullorja "Mbi mënyrën e dokumentimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit në shoqërinë "Albpetrol" Sh.A", është e zbatueshme nga të gjithë punonjësit dhe njësitë e strukturës organizative të shoqërisë "Albpetrol" Sh.A.

Neni 20
Hyrja në fuqi

Kjo rregullore hyn në fuqi dy javë pas miratimit nga Këshilli Mbikëqyrës.

KRYETARI I KËSHILLIT MBIKËQYRËS

Ilia GJERMANI

Legjenda e Ngjyrave

Tabela 1

Nr	KLASIFIKIMI I INCIDENTIT	SHEMBUJ TË INCIDENTEVE		PËRSHKRIMI
1	**Përmbajtje abuzive**	Spam		Dërgimi në grup i postës elektronike pa aprovimin e marrësit, e cila mund të përmbajë malware, ose skema mashtruese me qëllim kompromet imin e sigurisë së informacionit të përdoruesve.
		Të folurit e dëmshëm		Diskreditimi ose diskriminimi i dikujt (p.sh. ndjekja kibernetike, racizmi dhe kërcënimet ndaj një ose më shumë individëve).
		Përmbajtje online e dhunshme/seksuale/bullizuese ndaj fëmijëve		Pornografia e fëmijëve, shpërndarja e materialeve të dhunshme etj.
		Keqinformimi me dashje		Shtrembërimi i informacionit, i cili ka për qëllim të shkaktojë panik.
2	**Kod keqdashës**	Virus drejt shërbimeve kritike	Virus drejt shërbimeve të tjera	Softuer që instalohet qëllimisht në një sistem për qëllime të dëmshme.
		Worm drejt shërbimeve kritike	*Worm* drejt shërbimeve të tjera	
		Trojan drejt shërbimeve kritike	Trojan drejt shërbimeve të tjera	
		Spyware drejt shërbimeve	*Spyware* drejt shërbimeve të	

		kritike	tjera	
		Dialler drejt shërbimeve kritike	*Dialler* drejt shërbimeve të tjera	
		Rootkit drejt shërbimeve kritike	*Rootkit* drejt shërbimeve të tjera	
		Ransomware drejt sistemet kritike	Ransomware drejt sistemet të tjera	Kod keqdashës, i cili enkripton të dhënat në sistemet kompjuterike të një përdoruesi fundor ose/edhe servera.
		Fshirja e të dhënave *(wiper)* në sistemet kritike	Fshirja e të dhënave *(wiper)* në sistemet e tjera	Kod keqdashës, i cili ka për qëllim të shkatërrojë ose të fshijë të dhënat nga sistemi i prekur, duke bërë që të dhënat të bëhen të papërdorshme ose sistemi të mos funksionojë më.
3	**Mbledhja e informacionit**	Skanimi		Kërkesa për të zbuluar pikat e dobëta të një sistemi. Gjithashtu, kjo kategori incidenti përfshin procesin e testimit, me qëllim mbledhjen e informacioneve rreth hosteve, shërbimeve dhe llogarive. Shembuj: *fingered, DNS Query, RCE, ICMP, SMTP (EXPN, RCPT, etj.),* skanim i portave.
		Sniffing drejt shërbimeve kritike	*Sniffing* drejt shërbimeve teë tjera	Vëzhgimi dhe regjistrimi i trafikut të rrjetit (përgjimi).
		Inxhinieria sociale		Mbledhja e informacionit nga përdoruesit fundorë, në mënyrë jo-teknike (p.sh. mashtrime, "shoulder surfing", "tailgating", "piggy-backing", spiunazh ose kërcënime).
4	**Përpjekjet për ndërhyrje**	Shfrytëzimi i vulnerabilitetev e të njohura për të aksesuar shërbime kritike	Shfrytëzimi i vulnerabilitetev e të njohura për të aksesuar shërbime të tjera.	Përpjekje për të kompromentuar një sistem ose për të ndërprerë shërbime duke shfrytëzuar vulnerabilitetet, p.sh, backdoor, fragmentimi, etj.

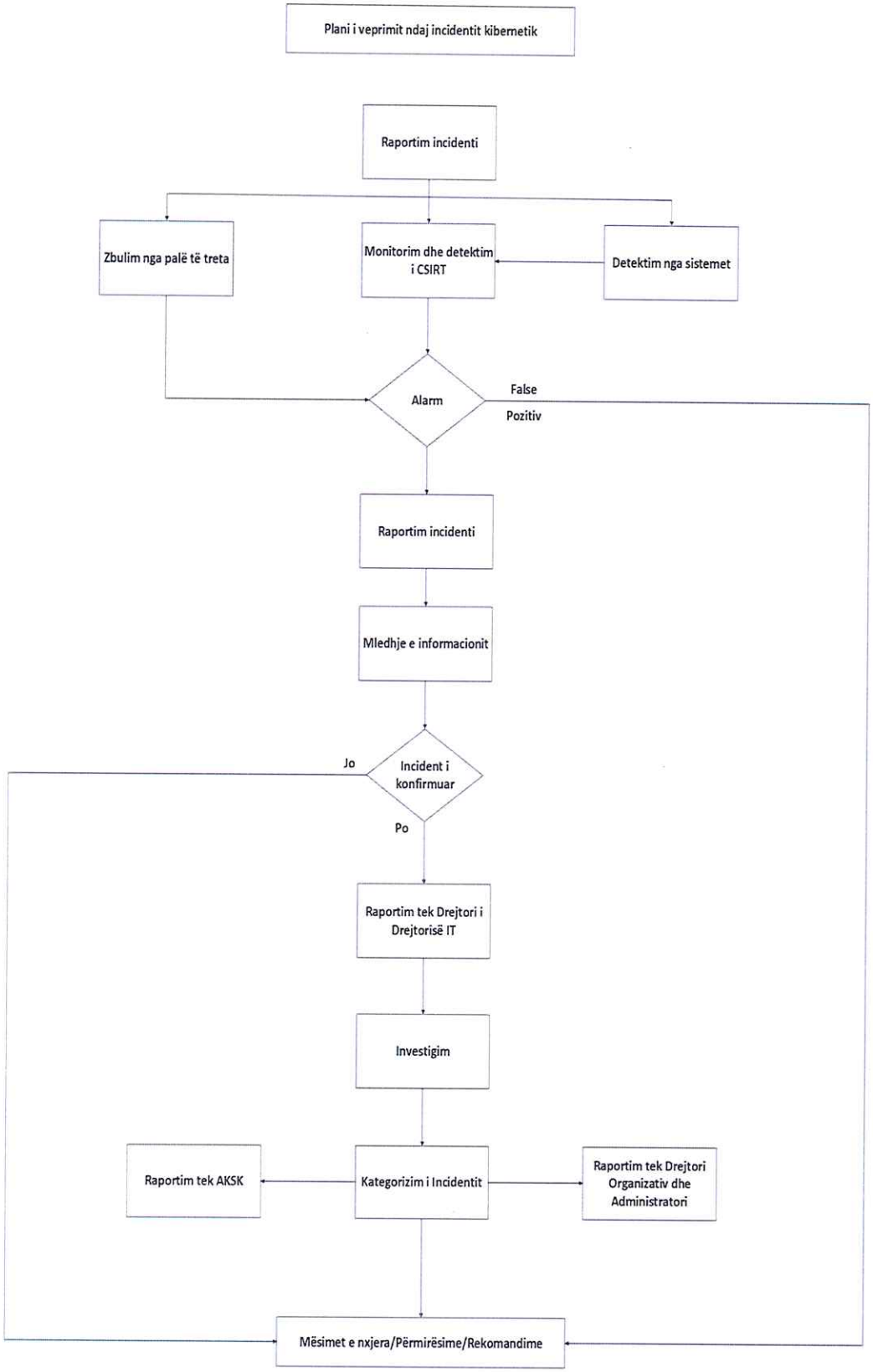
		Përpjekjet për *login*		Përpjekje të shumta për login, p.sh, *Guessing / cracking of passwords, dictionary attack, brute force, RCE.*
		0-day attack drejt shërbimeve kritike	0-day attack drejt shërbimeve të tjera	Përpjekje për ndërhyrje duke përdorur një *exploit* të panjohur.
5	**Ndërhyrjet**	Kompromentim i llogarive të privilegjuara		Kompromentim i suksesshëm i një sistemi ose aplikacioni (shërbimi). Ky incident mund të shkaktohet nga nga një vulnerabilitet i njohur ose i ri, por edhe nga aksesi lokal i paautorizuar.
		Kompromentim i llogarive të paprivilegjuara		
		Kompromentim i një aplikacioni që ofron shërbim kritik	Kompromentim i një aplikacioni që ofron shërbime të tjera	Psh ekzekutimi i teknikave *injection* si: *SQL Injection, Command Injection, File Injection, XSS, CSRF, RCE, API attack* etj.
6	**Disponueshmëria**	DoS/DDoS që ka ndërprerë sherbime kritike		DoS është një taktikë e sulmit kibernetik ku një sistem kompjuterik përdoret për të bombarduar një server, shërbim, ose rrjet me trafik të madh për të shkaktuar mbingarkesë dhe parandaluar përdorimin normal të shërbimit nga përdoruesit legjitimë. Kur në këtë sulm përfshihen më shumë se një sistem kompjuterik i infektuar, kategorizohet si DDoS. DDoS shpesh bazohet në sulmet DoS me origjinë nga botnet, por ekzistojnë edhe skenarë të tjerë si sulmet e Amplifikimit DNS. Disa shembuj, janë ICMP flood, SYN, sulmet Teardrop dhe mail-bombing.
		DoS/DDoS që ka ndikuar ndjeshëm shërbimet kritike dhe/ose ka ndërprerë shërbimet e tjera		
		DoS/DDoS që nuk ka ndikim në shërbime kritike, por ka ndikuar ndjeshëm tek shërbimet e tjera.		
		Sabotimi që ka prekur sistemin kritik.	Sabotimi që ka prekur sisteme të tjera.	
		Ndërprerje e shërbimeve si pasojë e një incidenti gjatë procesit të mirëmbajtjes ose/edhe teknike si: Energjia/Zjarri/Përmbytje që ka prekur infrastrukturën kritike	Ndërprerje e shërbimeve si pasojë e procesit të mirëmbajtjes ose/edhe teknike si: Energjia/Zjarri/ Përmbytje që ka prekur shërbime të tjera	

		Ndërprerje për shkak të katastrofave natyrore që ka prekur infrastrukturen kritike	Ndërprerje për shkak të katastrofave natyrore për shërbime të tjera	Disponueshmëria mund të afektohet edhe nga veprimet lokale (shkatërrim, ndërprerje e furnizimit me energji elektrike, etj.) - ose nga ngjarje katastrofike natyrore, dështime spontane ose gabime njerëzore, pa përfshirë keqdashje ose neglizhencë.
7	**Siguria e Përmbajtjes së Informacionit**	Akses i paautorizuar në shërbime kritike	Akses i paautorizuar në shërbime të tjera	Siguria e përmbajtjes së informacionit mund të cënohet nga kompromentim i suksesshëm i llogarive, aplikacioneve, të dhënave dhe sistemeve. Gjithashtu, sulmet mund të përgjojnë dhe aksesojnë informacionin gjatë transmetimit (*wiretapping*, *spoofing* or *hijacking*). Këto sulme mund të shkaktohen nga gabimet njerëzore, të konfigurimit, ose erore të softuerit.
		Modifikimi i paautorizuar në shërbime kritike	Modifikimi i paautorizuar në shërbime të tjera	
8	**Mashtrimi**	Përdorimi i paautorizuar i burimeve		Përdorimi i paautorizuar i burimeve, për qëllime përfitimesh personale të palidhura me aktivitetin e punës, si: chain-letter, përdorimi i emaileve të punës për regjistrimin në platforma që nuk lidhen me aktivititetin e punës, etj.
		E drejta e autorit		Ofrimi ose instalimi i kopjeve të softuerit komercial të paliçensuar ose materialeve të tjera të mbrojtura nga e drejta e autorit.
		Maskimi		Teknikë e sulmit ku një individ ose proces përpiqet të fitojë qasje të paautorizuar në burime ose të dhëna duke u

					përfaqësuar si një entitet legjitim. Kjo bëhet përmes falsifikimit të identitetit të tyre, si përmes përdorimit të të dhënave të vjedhura për autentifikim ose manipulimit të protokolleve të rrjetit për të mashtruar sistemet e sigurisë që të besojnë se trafiku ose kërkesat janë nga një burim i lejuar.
		Phishing/Spear Phishing/Whaling/Smishing/Vishing			Phishing është një teknikë mashtrimi që synon të marrë informacione të ndjeshme përmes email-eve, mesazheve, telefonatave, të targetuara (*spear phishing*), për nivelet e larta drejtuese (whaling), ose të pa targetuara, dërguesi i të cilave pretendon të jetë një entitet legjitim.
9	**Vulnerabiliteti**	Vulnerabilitete të dukshme për abuzim në shërbime kritike	Vulnerabilitete të dukshme për abuzim në shërbime të rëndësishme	Vulnerabilitete të dukshme për abuzim në shërbime të tjera	Vulnerabilitete të cilat bëhen publike nga palë të paautorizuara dhe i përkasin shërbimeve të një infrastrukture informacioni.
10	**Cryptomining**	Cryptomining në sistemet kritike ose në sisteme të tjera			Shfrytëzimi i burimeve për qëllime përfitimi nga gjenerimi i monedhave virtuale, si psh: Bitcoin.
11	**Eksfiltrimi**	Nxjerrja e të dhënave nga sistemet kritike të infrastrukturës drejt një serveri C2	Nxjerrja e të dhënave nga sistemet e tjera të infrastrukturës drejt një serveri C2		Procesi i paautorizuar i nxjerrjes së të dhënave nga sistemet e infrastrukturës drejt një serveri C2 për qëllime keqdashëse.
12	**Incident në ambjent testimi**	Incident i ndodhur në ambjent testimi për sistemet kritike ose sistemet e tjera			Keqpërdorimi i të dhënave sensitive në ambjent testimi si psh: Në sistemin financiar kur implementohet një sistem i ri

			dhe përdoren të dhënat reale të klientëve duhet të shfrytëzohet standarti PCI DSS → Marrjen leje të dhënave, dhe në fund shkatërrimin e tyre në mënyrë të përhershme.

Bllokskema 1



Bllokskema 2