URDHËR
Nr. 2981, datë 30.12.2025

PËR MIRATIMIN E STANDARDEVE MINIMALE TË SIGURISË, TË DETYRUESHME PËR SUBJEKTET E LICENCUARA

Në mbështetje të pikës 4, të nenit 102, të Kushtetutës së Republikës së Shqipërisë; të pikës 5, të nenit 18, të ligjit nr. 87/2024, "Për rregullimin e prodhimit, tregtimit, kërkimit dhe zhvillimit të armëve, municioneve, pajisjeve dhe teknologjive ushtarake",

URDHËROJ:

1. Miratimin e standardeve minimale të sigurisë, të detyrueshme për subjektet e licencuara", sipas tekstit që i bashkëlidhet këtij urdhri dhe pjesë e pandarë e tij.
2. Ngarkohet Agjencia e Industrisë së Mbrojtjes për zbatimin e këtij urdhri.
3. Ndjek zbatimin e këtij urdhri sekretari i përgjithshëm i Ministrisë së Mbrojtjes dhe drejtori i Përgjithshëm i Agjencisë së Industrisë së Mbrojtjes.

Ky urdhër hyn në fuqi menjëherë dhe botohet në Fletoren Zyrtare.

MINISTËR I MBROJTJES
Pirro Vengu

STANDARDEVE MINIMALE TË SIGURISË, TË DETYRUESHME PËR SUBJEKTET E LICENCUARA

(Miratuar me urdhër të ministrit të Mbrojtjes nr. 2981, datë 30.12.2025)
Tiranë më ___. ___.2025

TABELA E PËRMBAJTJES

DISPOZITA TË PËRGJITHSHME
1.1. Qëllimi
1.2. Fusha e zbatimit
1.3. Detyrimet e subjekteve
1.4. Përkufizime
KREU II
STANDARDET MINIMALE TË SIGURISË
2.1. Klasifikimi i standardeve
2.2. Standardet minimale të organizimit të zonave të punës dhe kushtet teknike
2.2.1. Ndarja funksionale e zonave
2.2.2. Distancat e sigurisë
2.2.3. Kushtet teknike të ambienteve të punës
2.2.4. Sinjalistika dhe organizimi vizual
2.3. Standardet minimale të kushteve teknike të ambientit
2.3.1. Ventilimi dhe qarkullimi i ajrit
2.3.2. Kontrolli i temperaturës dhe i lagështisë
2.3.3. Parandalimi i shkarkimeve elektrike

2.3.4. Ndriçimi dhe siguria kundër zjarrit
2.3.5. Organizimi i zonave të punës përfshirë ndarjen funksionale të zonave
2.4. Standardet minimale të pajisjeve mbrojtëse individuale (PMI)
2.4.1. Kategoritë e detyrueshme të PMI-së
2.4.2. Standardet teknike
2.4.3. Detyrimi i përdorimit
2.5. Standardet minimale të sistemeve elektronike të mbikëqyrjes dhe të aksesit
KREU III
MARRËVESHJET NDËRKOMBËTARE REFERUESE
3.1. Marrëveshje dhe Konventa të Zbatueshme
ANEKS A
ANEKS B
ANEKSI C
ANEKS Ç
ANEKS D
ANEKS DH
ANEKSI E
ANEKSI Ë

KREU I
DISPOZITA TË PËRGJITHSHME

1.1. Qëllimi

1.1.1. Standardet minimale kanë për qëllim:

- mbrojtjen e jetës dhe shëndetit të personave, përmes masave teknike dhe organizative që parandalojnë aksidentet, incidentet dhe ekspozimin ndaj rreziqeve fizike, kimike ose digjitale;
- mbrojtjen e pronës dhe mjedisit, duke siguruar zhvillimin e qëndrueshëm të veprimtarive të licencuara;
- reduktimin dhe menaxhimin e rreziqeve operacionale, teknologjike, mjedisore dhe atyre që lidhen me sigurinë kombëtare.

1.2. Fusha e zbatimit

1.2.1. Standardet minimale zbatohen nga çdo subjekt i licencuar, për:

- prodhimin, tregtimin, transportin dhe magazinimin e armatimit ushtarak;
- zhvillimin dhe kërkimin shkencor e teknologjik mbi armatimin ushtarak.

1.2.2. Bazuar në këto standarde dhe pa u kufizuar në to, subjektet që ushtrojnë veprimtarinë sipas pikës 1, hartojnë një rregullore të brendshme, ku parashikohen masat dhe procedurat e sigurisë.

1.3. Detyrimet e subjekteve

1.3.1. Subjektet e licencuara zbatojnë në mënyrë të plotë, të vazhdueshme dhe të dokumentuar, të gjitha standardet minimale të sigurisë, por pa u kufizuar në to.

1.3.2. Në përmbushje të këtij detyrimi, subjektet:

- hartojnë dhe zbatojnë një rregullore të brendshme, ku parashikohen qartësisht masat dhe procedurat për garantimin e sigurisë së jetës së njerëzve, shëndetit të personelit, produkteve, pajisjeve, të dhënave dhe infrastrukturës, si dhe planin e emergjencës;
- integrojnë standardet minimale të sigurisë në të gjitha proceset operacionale dhe menaxheriale të veprimtarisë së tyre;

- mbajnë dokumentacion të plotë dhe të përditësuar mbi masat e zbatuara, përfshirë planet e emergjencës, raportet e trajnimeve dhe inspektimeve të brendshme;

- zbatojnë pa vonesë rekomandimet që lidhen me masat korrigjuese të dhëna nga autoritetet inspektuese dhe raportojnë pranë Agjencisë së Industrisë së Mbrojtjes mbi përmbushjen e tyre;

- caktojnë oficerin e sigurisë për menaxhimin dhe mbikëqyrjen e çështjeve të sigurisë, i cili siguron zbatimin e standardeve;

- të gjitha aktivitetet e punës të ndërmarra duhet të mbulohen nga analiza të rreziqeve dhe ndikimeve mjedisore, të përgatitura nga persona kompetentë.

- Në rastet kur subjektet e licencuara, perimetrin e jashtëm do ta sigurojnë nëpërmjet FARSH-it. sipas legjislacionit në fuqi, janë të detyruara të zbatojnë procedurat e hyrje-daljeve dhe t'i nënshtrohen "kontrollit" nga struktura e FARSH-it.

1.4. Përkufizime

Termat e mëposhtëm kanë këtë kuptim:

- **"Incident"** është çdo ngjarje ose situatë, e cila shkakton ose ka gjasë të shkaktojë pasoja të rënda për jetën, shëndetin, sigurinë publike, funksionimin e sistemeve të sigurisë, integritetin e infrastrukturës kritike ose cenimin e të dhënave të ndjeshme ose të klasifikuara.

- **"Incident i sigurisë kibernetike"** është çdo ngjarje që komprometon disponueshmërinë, vërtetësinë, integritetin, konfidencialitetin e të dhënave të ruajtura, të transmetuara apo të përpunuara, ose të shërbimeve të ofruara, apo të aksesueshme, përmes rrjeteve dhe sistemeve të informimit.

- **"Personel i autorizuar"** është individi i punësuar ose i angazhuar nga subjekti i licencuar, i cili, në bazë të funksioneve të tij dhe autorizimit zyrtar të dhënë nga drejtuesit kompetentë të subjektit, ka të drejtë të aksesojë, trajtojë ose të përdorë pajisje, sisteme, informacione dhe ambiente që lidhen me prodhimin, tregtimin, magazinimin, transportimin, apo shpërndarjen e armatimit ushtarak.

- **"Plan evakuimi"** është dokumenti i detajuar, i hartuar nga subjekti i licencuar, që përcakton masat, rrugët e lëvizjes, mënyrën e informimit dhe detyrat në rast evakuimi emergjent të personelit dhe materialeve nga ambientet ku zhvillohet veprimtaria.

- **"Plan i menaxhimit të incidenteve"** është dokumenti i miratuar nga personi kompetent i subjektit të licencuar, që përmban masat, procedurat dhe përgjegjësitë për menaxhimin dhe trajtimin e incidenteve të sigurisë, duke synuar minimizimin e pasojave të tyre dhe rikthimin e funksionimit normal.

- **"Sektorë të ndjeshëm"** janë zona, ambiente, instalime, apo procese të veçanta të veprimtarisë së subjektit të licencuar, të cilat, për shkak të natyrës së tyre, nivelit të informacionit që përmbajnë ose pajisjeve që përdorin, paraqesin rëndësi të veçantë për sigurinë dhe kërkojnë mbrojtje të shtuar.

- **"Siguri kibernetike"** është tërësia e veprimeve të nevojshme për të mbrojtur rrjetet dhe sistemet e informacionit, përdoruesit e këtyre rrjeteve dhe sistemeve, si dhe personat e tjerë të prekur nga kërcënimet kibernetike.

- **"Siguria e perimetrit të jashtëm"** është zona, ambienti, instalimi apo procedura e kontrollit të personelit, pajisjeve dhe mjeteve për të lejuar aksesin vetëm për personelin e autorizuar, subjektet apo operatorët ekonomikë në këto ambiente, me qëllim sigurimin dhe shmangien e rrezikut që mund të vijë nga jashtë.

- **"Sistemi i reagimit emergjent"** janë strukturat, procedurat, teknologjitë dhe burimet njerëzore të ngritura për të siguruar menaxhimin, koordinimin dhe zbatimin e masave të menjëhershme, në rast incidentesh, fatkeqësish ose situatash që paraqesin rrezik për jetën, shëndetin, sigurinë publike ose infrastrukturën kritike.

- **“Standard sigurie”** është përmbushja e kërkesave teknike, organizative dhe procedurale, që synojnë të garantojnë një nivel të përcaktuar mbrojtjeje ndaj rreziqeve të veprimtarisë industriale që mund të cenojnë jetën, shëndetin, pronën, informacionin dhe mjedisin. Standardet e sigurisë përfshijnë masa parandaluese, mbrojtëse dhe reaguese, të cilat zbatohen në mënyrë të integruar në të gjitha fazat e veprimtarisë.

- **“Standarde minimale të sigurisë”** janë kriteret dhe masat e domosdoshme, të cilat përfaqësojnë nivelin bazë të sigurisë që përmbushin subjektet e licencuara.

- **“Vlerësimi dhe analiza e riskut”** është procesi i identifikimit, vlerësimit dhe matjes së rreziqeve të mundshme që lidhen me prodhimin, magazinimin, transportimin, tregtimin ose shpërndarjen e armatimit ushtarak dhe pajisjeve teknologjike, me qëllim përcaktimin e masave parandaluese dhe korrigjuese për të eliminuar ose reduktuar nivelin e këtyre rreziqeve.

- **“Zonë e rrezikshme”** është çdo hapësirë, territor, objekt, instalim, ambient pune brenda subjektit të licencuar, ku ekspozimi ndaj faktorëve fizikë, kimikë, mekanikë ose teknologjikë shkakton dëmtim të shëndetit të personelit, dëmtim të pajisjeve dhe infrastrukturës ose niveli i rrezikut për aksidente, shpërthime, zjarre apo incidente të tjera të rënda është i lartë për shkak të natyrës së veprimtarisë ose materialeve të depozituara.

KREU II
STANDARDET MINIMALE TË SIGURISË

2.1. Klasifikimi i standardeve

Standardet minimale të sigurisë klasifikohen sipas natyrës së tyre në:

- Standardet teknike, që lidhen me pajisjet, sistemet dhe infrastrukturën fizike dhe të sigurisë;
- Standardet organizative, që lidhen me strukturën, rolet dhe përgjegjësitë e personelit;
- Standardet procedurale, që lidhen me mënyrën e zbatimit, dokumentimit dhe reagimit ndaj situatave të rrezikut.

2.2. Standardet minimale të organizimit të zonave të punës dhe kushtet teknike

2.2.1. Ndarja funksionale e zonave

- Zonat e prodhimit, magazinimit, testimit dhe demilitarizimit ndahen qartë, duke garantuar izolim operacional dhe sigurie nga njëra-tjetra;
- Çdo zonë ka hyrje-dalje të kontrolluar dhe të pajiset me sinjalistikë të dukshme për rrezikun specifik;
- Ndarja bëhet në përputhje me standardet vendëse ose të NATO-s dhe manualet e tyre, duke respektuar kërkesat për sasi-distancë (SD), sipas sasisë së eksplozivëve ose materialeve të rrezikshme;
- Zonat e ndaluara për personat e paautorizuar shënohen me tabela paralajmëruese dhe të kufizohen fizikisht me barriera.
- Në zonat e sigurisë së perimetrit të jashtëm kryhet kontroll dhe lejimi i aksesit vetëm për personelin, materialet dhe mjetet e autorizuara.

2.2.2. Distancat e sigurisë

- Distancat minimale ndërmjet zonave përcaktohen sipas kategorisë së materialit dhe nivelit të rrezikut, duke u bazuar në standardet AASTP-1 dhe AASTP-5;
- Çdo subjekt kryen vlerësim teknik për përcaktimin e distancave dhe mban dokumentacionin përkatës në dosjen e sigurisë;
- Për çdo ndryshim në volum, sasi ose natyrë të materialeve të rrezikshme nga ajo për të cilën është licencuar subjekti, njoftohet AIM-ja, e cila, rivlerëson dhe miraton distancat e sigurisë.

2.2.3. Kushtet teknike të ambienteve të punës

- Të gjitha zonat e punës janë të pajisura me sisteme ventilimi të përshtatshme, për të shmangur grumbullimin e gazrave ose të substancave të rrezikshme;
- Duhet të ketë kontroll të vazhdueshëm të temperaturës dhe të lagështisë, sidomos në ambientet e ruajtjes së eksplozivëve ose kimikateve;
- Duhet të kenë masa për parandalimin e shkarkimeve elektrike, duke përdorur pajisje antistatike dhe tokëzime;
- Zonat e magazinimit të kenë ndriçim të përshtatshëm, të vazhdueshëm dhe të sigurt kundër zjarrit.

2.2.4. Sinjalistika dhe organizimi vizual

- Zonat të pajisen me tabela paralajmëruese sipas standardeve ndërkombëtare;
- Shënohen qartë rrugët e evakuimit, daljet emergjente dhe pikat e grumbullimit;
- Përdorimi i ngjyrave standarde për sinjalistikën (p.sh.: e kuqe për ndalim; e verdhë për rrezik; jeshile për dalje emergjente etj.).

2.3. Standardet minimale të kushteve teknike të ambientit

2.3.1. Ventilimi dhe qarkullimi i ajrit

- Ambientet ku trajtohen substanca kimike, eksplozive ose materiale të rrezikshme pajisen me sisteme ventilimi;
- Ventilimi duhet të sigurojë shkëmbim të vazhdueshëm ajri dhe shmangie të grumbullimit të gazrave ose tymrave të dëmshëm;
- Në zonat e magazinimit, ventilimi duhet të jetë i mjaftueshëm për të parandaluar grumbullimin e avujve të ndezshëm.

2.3.2. Kontrolli i temperaturës dhe i lagështisë

- Të sigurohet mbajtja e një temperature konstante, të përshtatshme për natyrën e materialeve të depozituara ose të përpunuara;
- Lagështia relative të monitorohet në mënyrë të vazhdueshme për të shmangur degradimin e materialeve dhe krijimin e kushteve për reaksione kimike të rrezikshme;
- Pajisjet matëse të jenë të kalibruara dhe të kontrollohen periodikisht.

2.3.3. Parandalimi i shkarkimeve elektrike

- Në ambientet ku përdoren eksplozivë ose substanca të ndezshme vendosen tokëzime, dysheme antistatike dhe rrufepritëse;
- Punonjësit të përdorin veshje dhe këpucë antistatike;
- Pajisjet elektrike të jenë për përdorim në zona me rrezik shpërthimi dhe në përputhje me standardet për zonat me atmosferë eksplozive (ATEX).

2.3.4. Ndriçimi dhe siguria kundër zjarrit

- Ndriçimi të jetë i mjaftueshëm për të siguruar normalitet në mjediset e punës, pa shkaktuar verbim apo reflektime të rrezikshme;
- Pajisjet e ndriçimit në zona me risk duhet të jenë të mbrojtura kundër shpërthimit;
- Ambientet pajisen me detektorë tymi, sisteme sprinkler dhe pajisje portative për fikjen e zjarrit.

2.3.5. Organizimi i zonave të punës përfshirë ndarjen funksionale të zonave

Si zonat e prodhimit, demontimit, magazinimit dhe testimit për të minimizuar efektin domino, me:

- respektimin e distancave të sigurisë në varësi të sasisë së eksplozivëve, duke zbatuar kriteret e Sasi-Distancë (SD).
- sinjalistikë të dukshme dhe akses të kontrolluar.

2.4. Standardet minimale të pajisjeve mbrojtëse individuale (PMI)

2.4.1. Kategoritë e detyrueshme të PMI-së

- Veshje mbrojtëse antistatike – të përdoren në të gjitha aktivitetet ku trajtohen eksplozivë ose substanca të rrezikshme, për të parandaluar shkarkimet elektrike;
- Pajisje për mbrojtjen e dëgjimit – të përdoren kufje ose tapa izoluese, sipas standardit EN 352, në zonat ku niveli i zhurmës tejkalon 85 dB;
- Mbrojtëse për fytyrën dhe sytë – të përdoren syze mbrojtëse, maska ose mburoja transparente sipas EN166, kundër grimcave, pluhurave dhe kimikateve;
- Maska respiratore – sipas standardeve EN 149 dhe EN 140, për zonat ku ka rrezik nga gazra, tym ose avuj toksikë;
- Doreza mbrojtëse – doreza të certifikuara (EN 388 për prerje, EN 374 për kimikate), të përzgjedhura sipas natyrës së aktivitetit;
- Mburoja trupore dhe veshje rezistente ndaj zjarrit – për aktivitetet me rrezik të lartë shpërthimi ose zjarri, sipas EN 469;
- Këpucë sigurie – të përdoren këpucë antistatike dhe rezistente ndaj goditjeve sipas EN ISO 20345.

2.4.2. Standardet teknike

- Të gjitha PMI-të të jenë të certifikuara sipas standardeve evropiane (EN) dhe/ose ndërkombëtare (ISO);
- Pajisjet kontrollohen rregullisht për funksionalitet dhe të zëvendësohen menjëherë në rast dëmtimi ose skadimi.

2.4.3. Detyrimi i përdorimit

- Çdo punonjës është i detyruar të përdorë PMI-në përpara hyrjes në zonat e rrezikut;
- Mospërdorimi i PMI-së përbën shkelje disiplinore dhe pasqyrohet në regjistrin e sigurisë së subjektit;
- Përgjegjësi i sigurisë ka detyrimin të verifikojë zbatimin e këtij rregulli në çdo kohë.

2.5. Standardet minimale të sistemeve elektronike të mbikëqyrjes dhe aksesit

2.5.1. Sisteme elektronike sigurie, përfshirë pajisje për mbikëqyrje dhe alarmim sipas standardeve ndërkombëtare për sigurinë digjitale, si:

2.5.1.1. Sistemi i monitorimit vizual (ÇTV)

- Kamerat të jenë me rezolucion të lartë (HD ose më sipër), të pajisura me funksion nate (IR) dhe të vendosura në pika kritike;
- Kamerat PTZ (pan-tilt-zoom) rekomandohen për zona të hapura ose pika hyrjeje;
- Regjistruesit (DVR/NVR) sigurojnë ruajtjen e materialeve audio-vizuale për një periudhë minimale 30-ditore.

2.5.1.2. Sistemi i alarmit

- Detektorë lëvizjeje, sensorë për dyer e dritare dhe sisteme akustike/vizuale paralajmëruese;
- Integrim i sistemit të alarmit me qendrën e monitorimit 24/7;
- Aktivizim automatik në rast hyrjesh të paautorizuara ose prishjes së pajisjeve.

2.5.1.3. Kontrolli i aksesit

- Përdorimi i kartave magnetike, kodeve PIN ose pajisjeve biometrike për hyrje në zonat e ndaluara;
- Regjistrim automatik i hyrje-daljeve dhe ruajtje e të dhënave për auditim.

2.5.1.4. Sistemet e sinjalizimit emergjent

- Butona emergjent të vendosur në pika të dukshme dhe të aksesueshme;
- Sinjalistikë zanore dhe vizuale për rastet e zjarrit, shpërthimeve ose evakuimit;
- Lidhje e detyrueshme me shërbimet e zjarrfikëses dhe emergjencave civile.

2.5.2. Kërkesat teknike minimale

- Sistemet të jenë të certifikuara sipas standardeve ndërkombëtare (p.sh.: EN 50132 për CCTV, ISO/IEC 27001 për sigurinë digjitale);
- Pajisjet të kenë burim të rezervuar energjie (UPS) për funksionim të paktën 2 orë pas ndërprerjes së energjisë elektrike;
- Sistemet të testohen dhe të mirëmbahen periodikisht, me evidencë të plotë të regjistruar nga subjekti.

2.6. Standardet minimale të mbrojtjes së të dhënave personale dhe sigurisë kibernetike

2.6.1. Mbrojtja e të dhënave personale dhe informacionit sensitive.

2.6.1.1. Të dhënat personale dhe sensitive ruhen dhe përpunohen vetëm në sisteme të certifikuara, në përputhje me legjislacionin për mbrojtjen e të dhënave;

2.6.1.2. Duhet të përdoren metoda adekuate enkriptimi të standardit të industrisë (AES-256 për ruajtje, TLS 1.3/ IPsec për transmetim);

- Enkriptimin e të dhënave në transit (p.sh. SSL/TLS, VPN) dhe në pushim (p.sh. AES-256), në përputhje me nivelin e klasifikimit të informacionit;
- Menaxhimin e sigurt të çelësave të enkriptimit dhe mekanizmave të autorizimit.

2.6.1.3. Aksesi në të dhëna lejohet vetëm për personat e autorizuar dhe sipas parimit "minimumi i nevojshëm" *(least privilege),* duke vendosur RBAC për përdoruesit, ACL për filtrimin e trafikut, si dhe mbylljen e shërbimeve të panevojshme;

- kontrollin e aksesit të bazuar në role (RBAC, DAC ose MAC), sipas parimit të privilegjit minimal dhe përdorimin e autentifikimit shumëfaktorësh (2FA/MFA) për përdorues dhe administrator, duke përshtatur kërkesat sipas nivelit të klasifikimit;
- monitorimin e hyrjeve dhe aktiviteteve në sistem, me theks të shtuar për informacionin "Sekret" dhe "Tepër sekret".

2.6.2. Siguria kibernetike

Çdo subjekt zbaton masat e sigurisë të bazuar në standardet ISO/IEC 27001 dhe NIST.

2.6.2.1. Siguria kibernetike, e cila përfshin:

- Enkriptimin e të dhënave në transit dhe në ruajtje, duke përdorur standarde të njohura ndërkombëtarisht AES, RSA, ECC, TLS 1.3, IPSec, SSH;
- Autentifikimin shumëfaktorësh (2FA/MFA) dhe politikat e aksesit të bazuara në role (RBAC) për qasje në sistemet kritike dhe të dhënat sensitive;
- Monitorimin e vazhdueshëm të rrjeteve dhe sistemeve për identifikimin dhe parandalimin e ndërhyrjeve të paautorizuara;
- Përdorimin e sistemeve IDS/IPS për zbulim dhe parandalim të ndërhyrjeve të integruara me *Next-Gen Firewall,* segmentimin VLAN dhe mbrojtjen kundër sulmeve DNSSEC dhe Dos/DdoS;
- Përdorimin e platformave për *"Data Loss Prevention"* për parandalimin e rrjedhjes së informacionit;
- Auditimin periodik të sistemeve;
- Zbatimin e procedurës *hardening* të pajisjeve (serverë, *router, switch, firewall, endpoint)* dhe segmentimin e shërbimeve kritike *(databaza, web services);*
- Sistemet mbrohen me pajisje të perimetrit 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 *(Next Generation Firewall) firewall,* IDS/IPS, si dhe monitorim të vazhdueshëm;
- Të pajisen me sistem të automatizuar për menaxhimin dhe filtrimin e logimeve, me qëllim identifikimin e alerteve në kohë reale;
- Kontrolle periodike e sistemeve të informacionit mbi plotësimin e masave të sigurisë kibernetike dhe penetrim-test i detyrueshëm një herë në vit nga subjekte të akredituara;

- Përdorimin e sistemeve për zbulim dhe përgjigje ndaj ndërhyrjeve (IDS/IPS) dhe *firewall*-eve të gjeneratës së re *(Next-Gen Firewall),* të integruara me analiza të trafikut dhe mekanizma të zbulimit të sjelljes *(behavioural analysis);*

- Përcaktimin dhe zbatimin e politikave për ruajtjen, arkivimin dhe fshirjen e të dhënave, sipas nivelit të klasifikimit përfshirë zëvendësimin/izolimin e sistemeve *"End of Life";*

- Subjektet janë të detyruara të mbajnë kopje rezervë *(backup)* të rregullta dhe të testojnë planet e rikuperimit pas incidenteve (*Disaster Recovery Plans),* si dhe të implementojnë *Disaster Recovery Site* për shërbimet kritike, në mënyrë që të garantohet vazhdimësia e funksionimit edhe në rast të ndërprerjes së infrastrukturës kryesore;

- Kryet ndarja e rrjetit në nënrrjete, duke vendosur kompjuterët e përdoruesve dhe serverët në zonat/subnet/VLAN të ndryshme dhe duke i kontrolluar ato përmes listave të aksesit (ACL);

- Siguria e aplikacioneve me *WAF, Reverse Proxy,* DMARC/SPF/DKIM për *email* dhe testime të zhvillimeve në mjedis të izoluar;

- Auditimi periodik i masave të sigurisë, për verifikimin e përputhshmërisë me standardet kombëtare dhe ndërkombëtare dhe për identifikimin e mangësive, duke lëshuar rekomandime detyruese për përmirësim përfshirë testime të detajuara të penetrimit *(penetration test – Black, Gray, White box)* dhe vlerësime të vulnerabiliteteve (VA), të detyrueshme një herë në vit.

2.7. Standardet minimale për menaxhimin e mbetjeve dhe substancave të rrezikshme

2.7.1. Klasifikimi dhe etiketimi

- Substancat dhe mbetjet e rrezikshme klasifikohen sipas standardeve ndërkombëtare *(ADR, Basel Convention, ISO 11014);*

- Çdo enë ose paketim përmban etiketa paralajmëruese dhe piktograma, sipas rregullave të GHS *(Globally Harmonized System);*

- Dokumentacioni i transportit dhe magazinimit përfshin të dhëna të plota mbi llojin, sasinë dhe nivelin e rrezikut;

- Çdo substancë apo mbetje e rrezikshme do të shoqërohet me skedën e të dhënave të sigurisë (MSDS).

2.7.2. Ruajtja dhe depozitimi

- Mbetjet dhe substancat e rrezikshme ruhen në ambiente të veçanta, të ventiluara dhe të pajisura me masa kundër zjarrit;

- Ambientet e depozitimit të kenë tokëzim dhe dysheme të papërshkueshme nga lëngjet;

- Duhet të respektohen distancat e sigurisë sipas standardeve AASTP-1 dhe AASTP-5.

2.7.3. Transporti

- Transporti i mbetjeve dhe substancave të rrezikshme kryhet vetëm me mjete të certifikuara sipas ADR;

- Çdo ngarkesë shoqërohet me dokumentacion përkatës (manifest, certifikata të sigurisë, leje transporti);

- Personeli i transportit të jetë i trajnuar sipas kërkesave të ADR dhe të pajiset me mjetet e PMI-së;

- Subjekti duhet të jetë i pajisur me leje mjedisore përkatëse për çdo mbetje.

2.8. Standardet minimale për reagimin ndaj emergjencave dhe menaxhimin e incidenteve

2.8.1. Reagimit ndaj emergjencave

2.8.1.1. Çdo subjekt i licencuar është i detyruar të hartojë, miratojë dhe të zbatojë një plan emergjence të integruar, i cili përfshin si minimum këto elemente:

- evakuimin e menjëhershëm të personelit;

- mbrojtjen e pasurisë dhe materialeve të rrezikshme;

- komunikimin me koordinatorin e sigurisë në AIM dhe autoritetet publike;

- rikuperimin e funksioneve pas emergjencës.

2.8.1.2. Plani rishikohet të paktën një herë në vit dhe menjëherë pas çdo incidenti sigurie.

2.8.2. Plani i menaxhimit të incidenteve

2.8.2.1. Klasifikimi i incidenteve.

Incidentet ndahen në tri kategori:

- me impakt të ulët – situata që nuk cenojnë drejtpërdrejt sigurinë e personelit apo funksionimin e sistemit;
- me impakt të mesëm – situata që paraqesin rrezik të kufizuar, por që mund të eskalojnë, nëse nuk menaxhohen;
- me impakt të lartë – situata që rrezikojnë jetën, shëndetin, pronën, mjedisin apo sigurinë kombëtare.

2.8.3. Evakuimi i personelit:

- Rrugët e evakuimit të jenë të qarta, të sinjalizuara dhe të ndriçuara;
- Daljet emergjente të jenë gjithmonë të lira nga pengesat dhe të kontrollohen periodikisht nga personeli i sigurisë;
- Pikat e grumbullimit të përcaktohen qartë në plan dhe të jenë të vendosura në distancë të sigurt nga objekti kryesor;
- Ushtrimet e evakuimit të kryhen të paktën dy herë në vit, të dokumentohen dhe të analizohen për qëllime evakuimi.

2.9. Standardet minimale për trajnimin e personelit

2.9.1. Kriteret e trajnimit:

- Detyrim periodik – trajnimet zhvillohen të paktën një herë në vit për çdo punonjës;
- Përshtatja sipas funksioneve – programi i trajnimit përcaktohet në varësi të rolit, nivelit të riskut dhe detyrave specifike të punonjësit;
- Dokumentimi – çdo trajnim regjistrohet në një regjistër të posaçëm, ku shënohet emri i pjesëmarrësit, data, tema e trajnimit dhe nënshkrimi i punonjësit;
- Certifikimi – trajnimi kryhet nga vetë subjekti ose nga institucione të akredituara.

2.9.2. Fushat e detyrueshme të trajnimit

- Sistemeve elektronike të mbikëqyrjes dhe akses përdorimi i pajisjeve të sigurisë (CCTV, alarme, kontrolle hyrjeje, sisteme emergjente);
- Mbrojtjes së të dhënave personale dhe sigurisë kibernetike njohuri mbi mbrojtjen e të dhënave, parandalimin e sulmeve kibernetike *(phishing, malware)* dhe raportimin e incidenteve të dyshimta;
- Organizimit të zonave të punës dhe kushtet teknike;
- Pajisjeve të mbrojtëse personale (PPE);
- Menaxhimin e mbetjeve dhe substancave të rrezikshme reagimit ndaj emergjencave dhe menaxhimit të incidenteve – procedurat e evakuimit, përdorimi i pajisjeve të fikjes së zjarrit, komunikimi emergjent dhe koordinimi me shërbimet publike;
- Ndihma e parë – trajtimi fillestar i lëndimeve, përdorimi i pajisjeve të ndihmës së parë njoftimi i shërbimeve mjekësore;
- Raportimi i incidenteve – mënyra e identifikimit dhe njoftimit të menjëhershëm të ngjarjeve të pazakonta.

2.9.3. Ushtrimet praktike

- Subjektet janë të detyruara të zhvillojnë ushtrime periodike simulimi *(drills)* për situata të tilla, si: zjarr, shpërthim, rrjedhje kimike, sulm kibernetik;
- Rezultatet e ushtrimeve dokumentohen dhe analizohen për përmirësimin e planeve të reagimit.

2.10. Standardet minimale për komunikimi dhe koordinimi

2.10.1. Komunikimi emergjent

- Çdo subjekt duhet të ketë kanale komunikimi të posaçme për situata emergjente (linjë telefonike, radio, aplikacione të dedikuara);
- Përgjegjësi i sigurisë njofton menjëherë koordinatorin për sigurinë në AIM për çdo ngjarje emergjente.

2.10.2. Koordinimi me autoritetet publike

Subjektet janë të detyruara të bashkëpunojë me strukturën e FARSH-it, e cila bën ruajtjen e perimetrit të jashtëm, Policinë e Shtetit, Shërbimin e Zjarrfikëses, Emergjencat Civile dhe Shërbimet Shëndetësore.

2.10.3. Skema e komunikimit emergjent

Protokolli i komunikimit gjatë një incidenti është i ndërtuar sipas hierarkisë së mëposhtme:

Personi që konstaton incidentin → Përgjegjësi i sigurisë së subjektit → Drejtuesi teknik/operacional → Sipas rastit komunikim me Agjencinë e Industrisë së Mbrojtjes, Policia e Shtetit, Shërbimi Zjarrfikëses dhe Emergjencat Civile

2.10.4. Testimi dhe auditimi

- Planet e emergjencës testohen periodikisht përmes ushtrimeve praktike *(drills);*
- Rezultatet e ushtrimeve dokumentohen dhe përdoren për përmirësimin e planeve;
- Auditimi i pasincidentit dhe përditësimi i planit të reagimit bazuar në mësimet e nxjerra.

2.11. Standardet minimale për raportimin

2.11.1. Detyrimi për raportim të menjëhershëm

2.11.1.1. Subjektet e licencuara njoftojnë menjëherë te koordinatori i sigurisë pranë Agjencinë e Industrisë së Mbrojtjes për çdo incident me impakt të rëndë, që:

- përbën rrezik për jetën, shëndetin ose sigurinë publike;
- ka shkaktuar ndërprerje të funksionimit të sistemit të sigurisë;
- përfshin rrjedhje informacioni të ndjeshëm ose të klasifikuar.

2.11.1.2. Njoftimi të bëhet brenda 30 minutave nga momenti i konstatimit të incidentit. Njoftimi bëhet me shkrim; në raste emergjente njoftohet koordinatori i sigurisë dhe formalizohet me shkrim brenda 1 dite pune.

2.11.1.3. Raporti i detajuar teknik të paraqitet brenda 72 orëve.

2.11.2. Raportimi pas incidentit

Çdo subjekt paraqet pranë AIM-së një raport përfundimtar brenda 72 orëve nga incidenti, i cili përmban:

- një përshkrim të detajuar të incidentit, duke përfshirë rëndësinë dhe ndikimin e tij;
- llojin e kërcënimit ose shkakun kryesor që e shkaktuar incidentin;
- masat e zbatuara dhe masat e vazhdueshme për zvogëlimin e pasojave;
- aty ku është e aplikueshme, ndikimin ndërkufitar të incidentit;
- rekomandimet për përmirësim, analiza e shkaqe dhe propozime për parandalim në të ardhmen.

2.11.3. Raportimi i incidenteve kibernetike

2.11.3.1. Çdo incident që prek sigurinë e të dhënave ose të sistemeve të informacionit raportohet menjëherë te koordinatori i sigurisë pranë Agjencisë së Industrisë së Mbrojtjes, duke përmbajtur:

- numri i përdoruesve të prekur nga ndërprerja e shërbimit;
- kohëzgjatja e incidentit;
- shtrirja gjeografike në lidhje me zonën e prekur nga incidenti;
- shkalla e ndërprerjes së funksionimit të shërbimit;
- shtrirja e ndikimit në aktivitet ekonomike dhe shoqërore;
- varësia e sektorëve nga shërbimet e ofruara të operatorit të infrastrukturës së informacionit;

- rëndësia e ruajtjes së një niveli të mjaftueshëm të shërbimit, duke marrë parasysh disponueshmërinë.

2.11.3.2. Raporti përfundimtar përmban:

- një përshkrim të detajuar të incidentit, duke përfshirë rëndësinë dhe ndikimin e tij;
- llojin e kërcënimit ose shkakun kryesor që e shkaktuar incidentin;
- masat e zbatuara dhe ato të vazhdueshme për zvogëlimin e pasojave;
- ndikimin ndërkufitar të incidentit aty ku është e aplikueshme.

2.11.4. Mbajtja e të dhënave.

2.11.4.1. Subjektet e licencuara mbajnë dokumentacion dhe raporte të cilat janë objekt inspektimi nga Agjencia e Industrisë së Mbrojtjes, mbi zbatimin e standardeve të sigurisë.

2.11.4.2. Raportet përmbajnë, të paktën:

- përshkrimin e masave të sigurisë të zbatuara gjatë periudhës raportuese;
- të dhëna mbi trajnimin e stafit dhe certifikimet e kryera;
- informacion mbi incidentet e ndodhura dhe masat e marra për menaxhimin e parandalimin e tyre;
- përditësimet në infrastrukturën teknike dhe sistemet e sigurisë;
- rezultatet e auditimeve të brendshme dhe të jashtme;
- analizë të rrezikut dhe planifikim të inspektimeve auditimeve të ardhshme.

KREU III
MARRËVESHJET NDËRKOMBËTARE REFERUESE

3.1. Marrëveshje dhe Konventa të Zbatueshme

Në rastet kur veprimtaria e subjekteve të licencuara përfshin elemente ndërkombëtare zbatohen dispozitat e marrëveshjeve dhe konventave ndërkombëtare të ratifikuara nga Republika e Shqipërisë, por pa u kufizuar:

- Konventën ADR për transportin rrugor të mallrave të rrezikshme;
- Konventën e Baselit për mbetjet e rrezikshme;
- Konventën e Roterdamit për substancat kimike të rrezikshme;
- Standardet ISO, IATG dhe praktikat e mira të ILO për sigurinë në punë;
- Standardet e NATO-s;
- Standardet EDA EDSTAR.

ANEKS A
Skema e komunikimit emergjent

Protokolli i Komunikimit gjatë Incidentit

○ Personi që konstaton incidentin	Gri e hapur
Përgjegjësi i sigurisë së objektit	Portokalli
◍ Drejtuesi teknik/operacional	Blu
◍ Agjencia e Industrisë së Mbrojtjes	E Kuqe

Në rast incidentesh kritike: aktivizohet menjëherë edhe bashkëpunimi me Policinë e Shtetit, Shërbimin e Zjarrfikëses dhe Emergjencat Civile.

ANEKS B
Sistemet elektronike të sigurisë

REGJISTËR I MIRËMBAJTJES SË SISTEMEVE ELEKTRONIKE TË SIGURISË

Nr.	Data e ndërhyrjes/testimit	Lloji i pajisjes/ sistemi	Përshkrimi i ndërhyrjes / mirëmbajtjes	Përgjegjësi teknik	Nr. licence/ certifikate	Rezultati i testimit/ vërejtje teknike	Nënshkrimi

ANEKSI C
Matrica e planit të veprimit – Trajnimi i personelit

Nr.	Elementi	Përshkrimi/Kërkesa	Frekuenca/Afati	Përgjegjësia	Dokumentimi/Evidenca
1					
1.1					
1.2					
1.3					
1.4					
2					
2.1					
2.2					
2.3					
2.4					
2.5					
3					
3.1					
3.2					

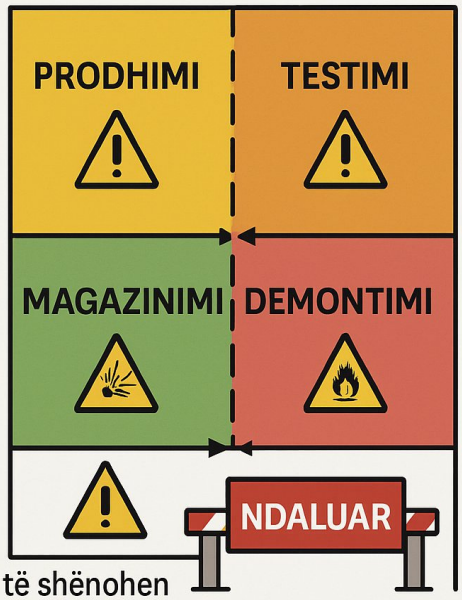
ANEKS Ç
Organizimi i zonave të punës dhe kushtet teknike
1. Ndarja funksionale e zonave

NDARJA FUNKSIONALE E ZONAVE

a. Zonat e prodhimit, magazinimit, testimit dhe demontimit duhet të ndahen qartë nga njëra-tjetra.

b) Çdo zonë duhet të ketë hyrje/dalje të kontrolluar dhe të pajiset me sinjalistikë të dukshme për rrezikun specifik.

c) Ndarja bëhet në përputhje me standardet e NATO-s dhe manualet DESR 6055.09, duke respektuar kërkesat për Quantity-Distance (QD) sipas sasisë së eksplozivëve ose materialeve të rrezikshme.



ç) Zonat e ndaluara për publikun duhet të shënohen me tabela paralajmëruese dhe të kufizohen fizikisht me barriera.

2. Distancat e sigurisë

DISTANCAT E SIGURISË

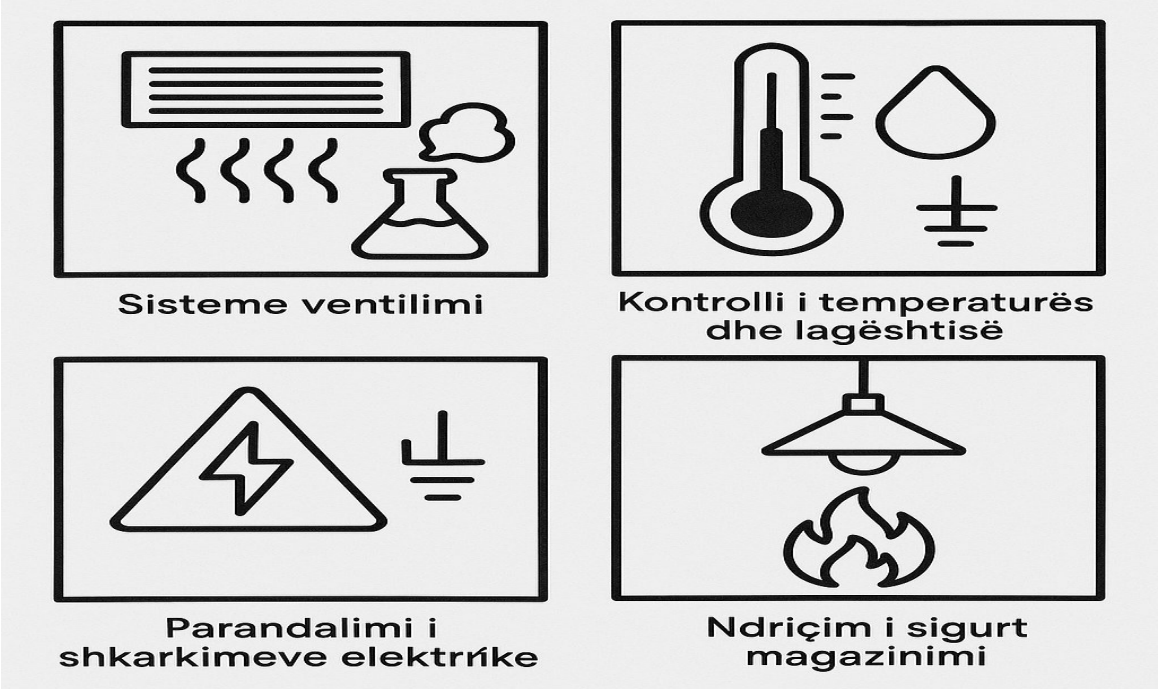
a) Distancat minimale ndërmjet zonave përcaktohen sipas kategoisë së materialit dhe nivelit të rrezikut, duke u bazuar në standardet AASTP-1 dhe AASTP-5;

b) Çdo subjekt është i detyruar të kryejë vlerësim teknik për përcaktimin e distancave dhe të mbajë dokumentacionin përkatës në dosjen e sigurisë.

c) Për çdo ndryshim në volum, sasi ose natyrë të materialeve të rrezikshme, distancat e sigurisë duhet të rivlerësohen dhe të aprovohen nga AIM.

Distanca minimale

3. Kushtet teknike të ambienteve



4. Sinjalistika dhe organizimi vizual

ANEKS D
Pajisjet mbrojtëse individuale (PMI)

1. Kategoritë e detyrueshme të PMI

Kategoritë e detyrueshme të PMI

Veshje mbrojtëse antistatike – të përdoren në të gjitha aktivitetet ku trajtohen eksplozivë ose substanca të rrezikshme, për të parandaluar shkarkimet elektrike.

Pajisje për mbrojtjen e dëgjimit – kufje ose tapa izoluese, sipas standardit EN 852, në zonat ku niveli i zhurmës tejkalon 85 dB.

Mbrojtëse për fytyrën dhe sytë – syze mbrojtëse, maska ose mburoja transparente sipas EN 166, kundër grimcave, pluhurave dhe kimikateve.

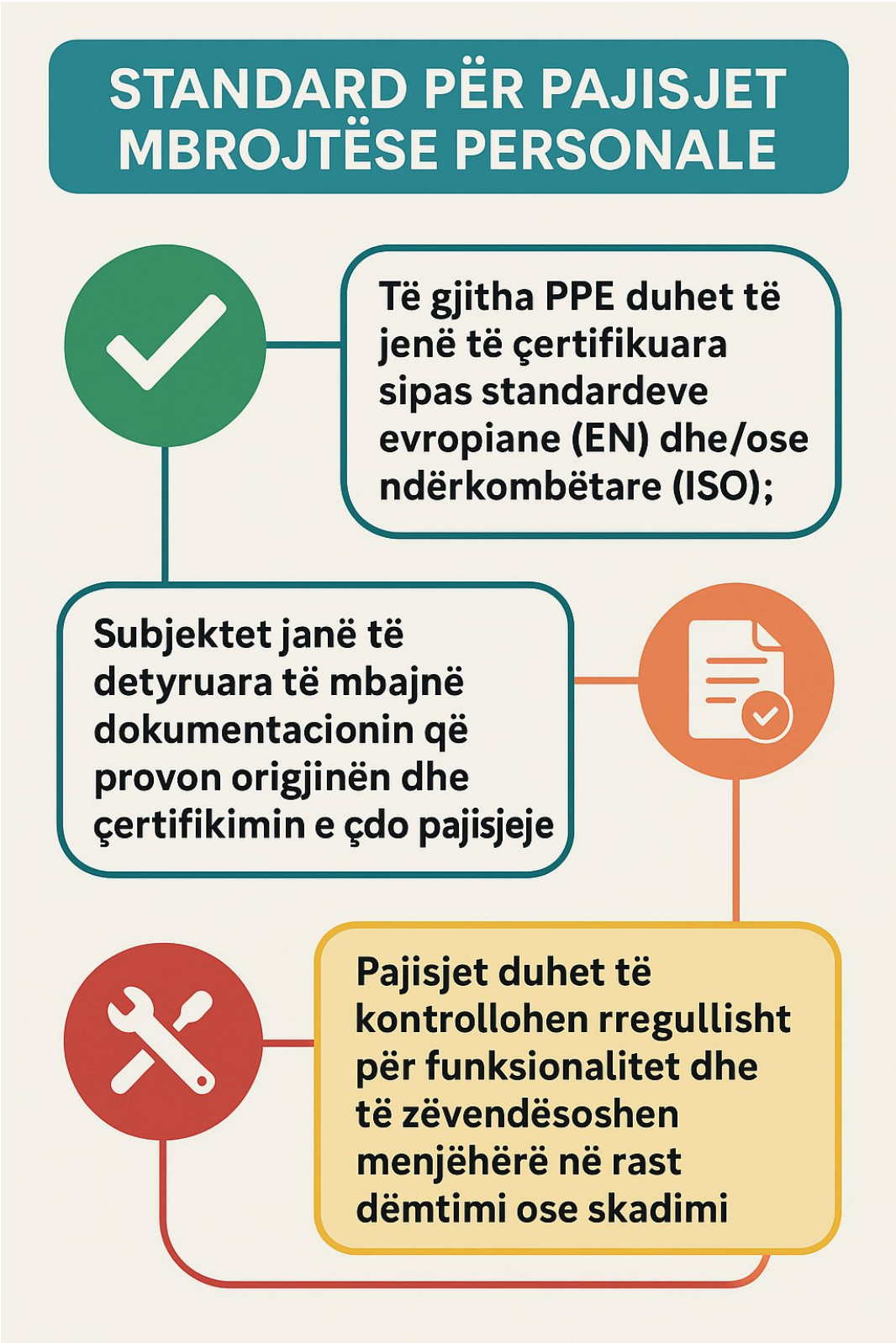
Maska respiratore – sipas standardeve EN 149 dhe EN 140, për zonat ku ka rrezik nga gazra, tym ose avuj toksikë.

Doreza mbrojtëse – doreza të certifikuara (EN 388 për prerje, EN 374 për kimikate), të përzgjedhura sipas natyrës së aktivitetit.

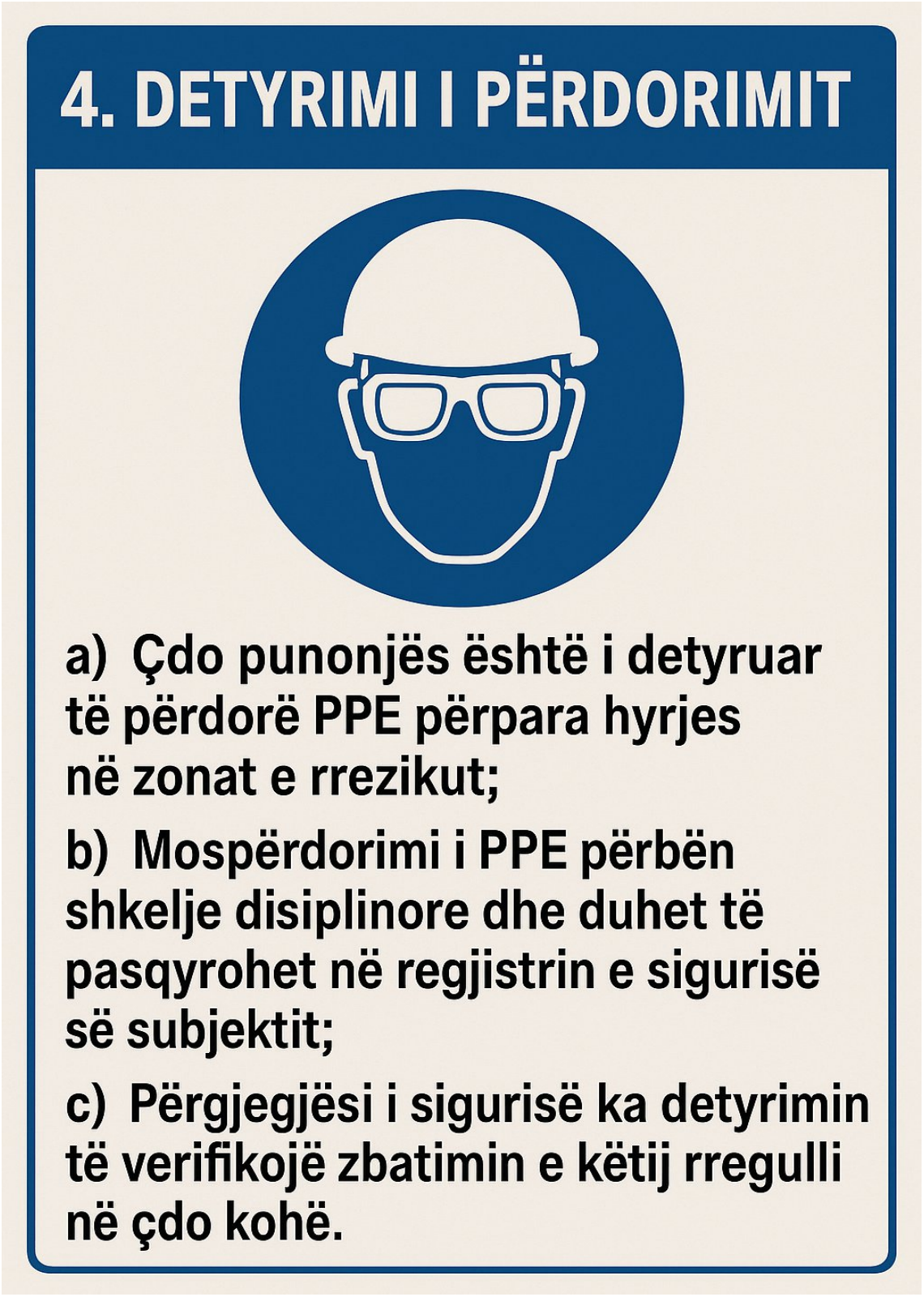
Këpucë sigurie – këpucë antistatike dhe rezistente ndaj goditjeve sipas EN ISO 20345.

Mburoja trupore dhe veshje rezistente ndaj zjarrit – për aktivitetet me rrezik të lartë shpërthimi ose zjarri, sipas EN 469.

2. Standardet teknike

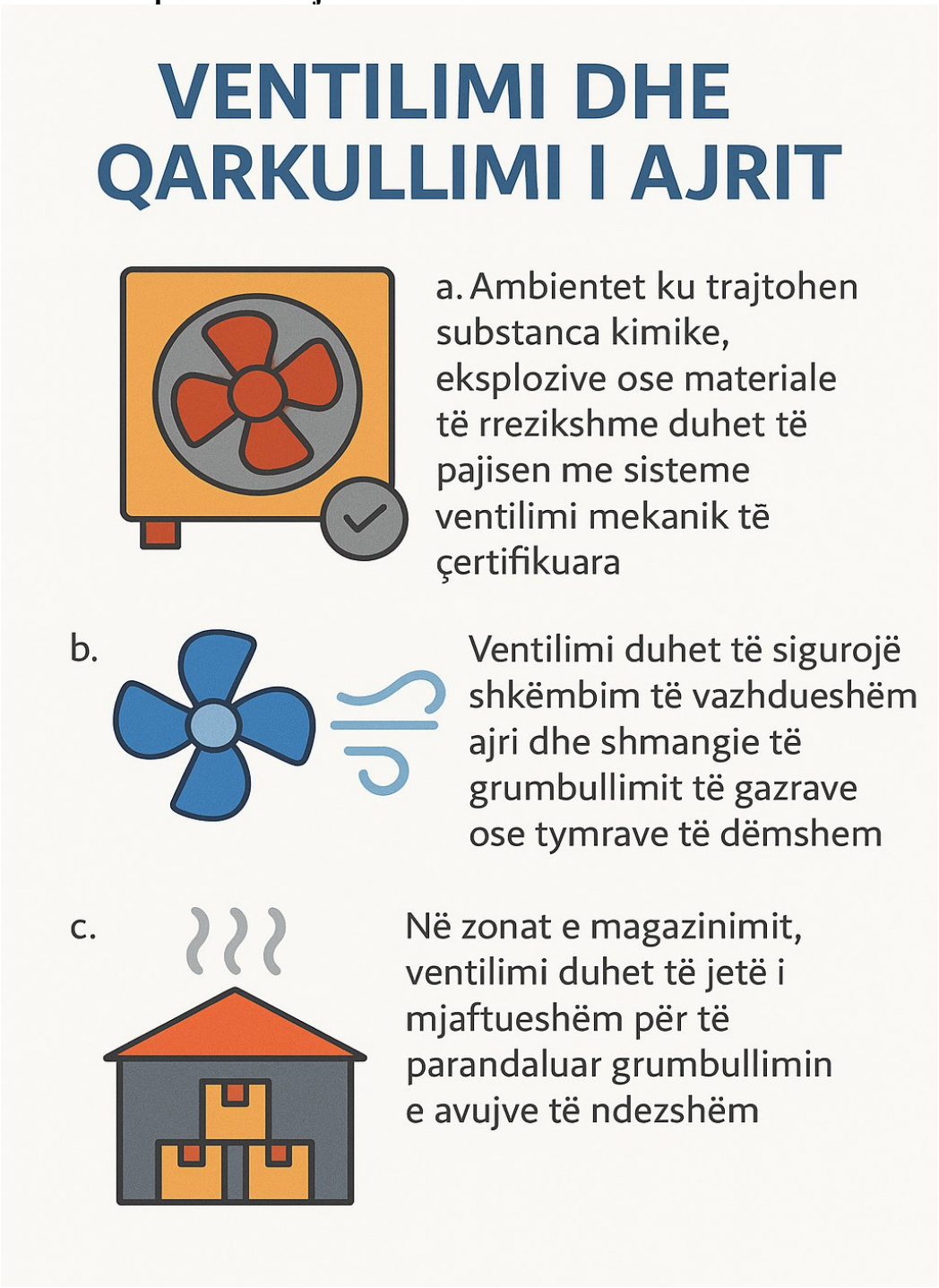


3. Detyrimi i përdorimit



ANEKS DH
Kushtet teknike të ambientit

1. Ventilimi dhe qarkullimi i ajrit

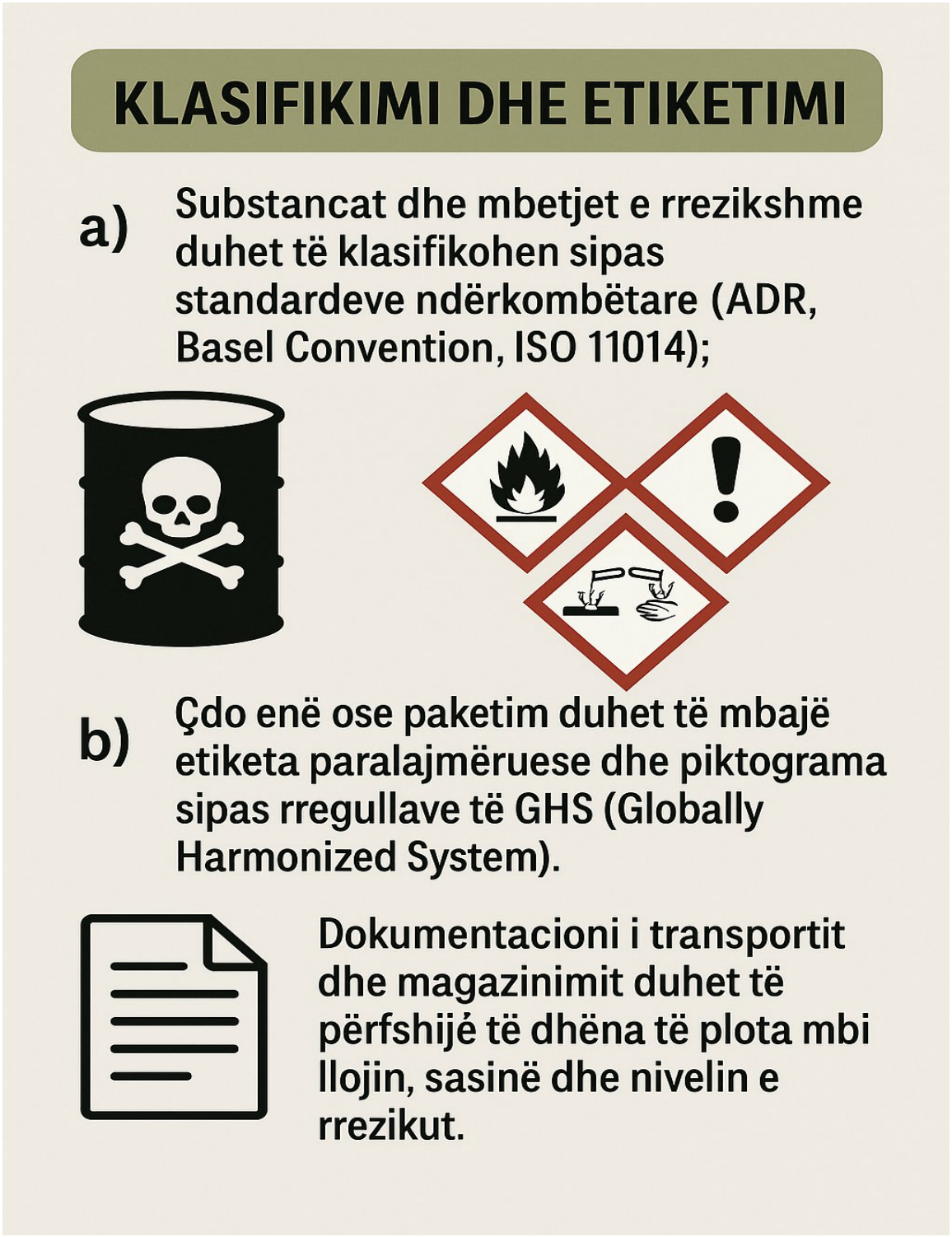


2. Parandalimi i shkarkimeve elektrike

3. Ndriçimi dhe siguria kundër zjarrit

ANEKSI E
Menaxhimi i mbetjeve dhe i substancave të rrezikshme

1. Klasifikimi dhe etiketimi



2. Ruajtja dhe depozitimi

RUAJTJA DHE DEPOZITIMI

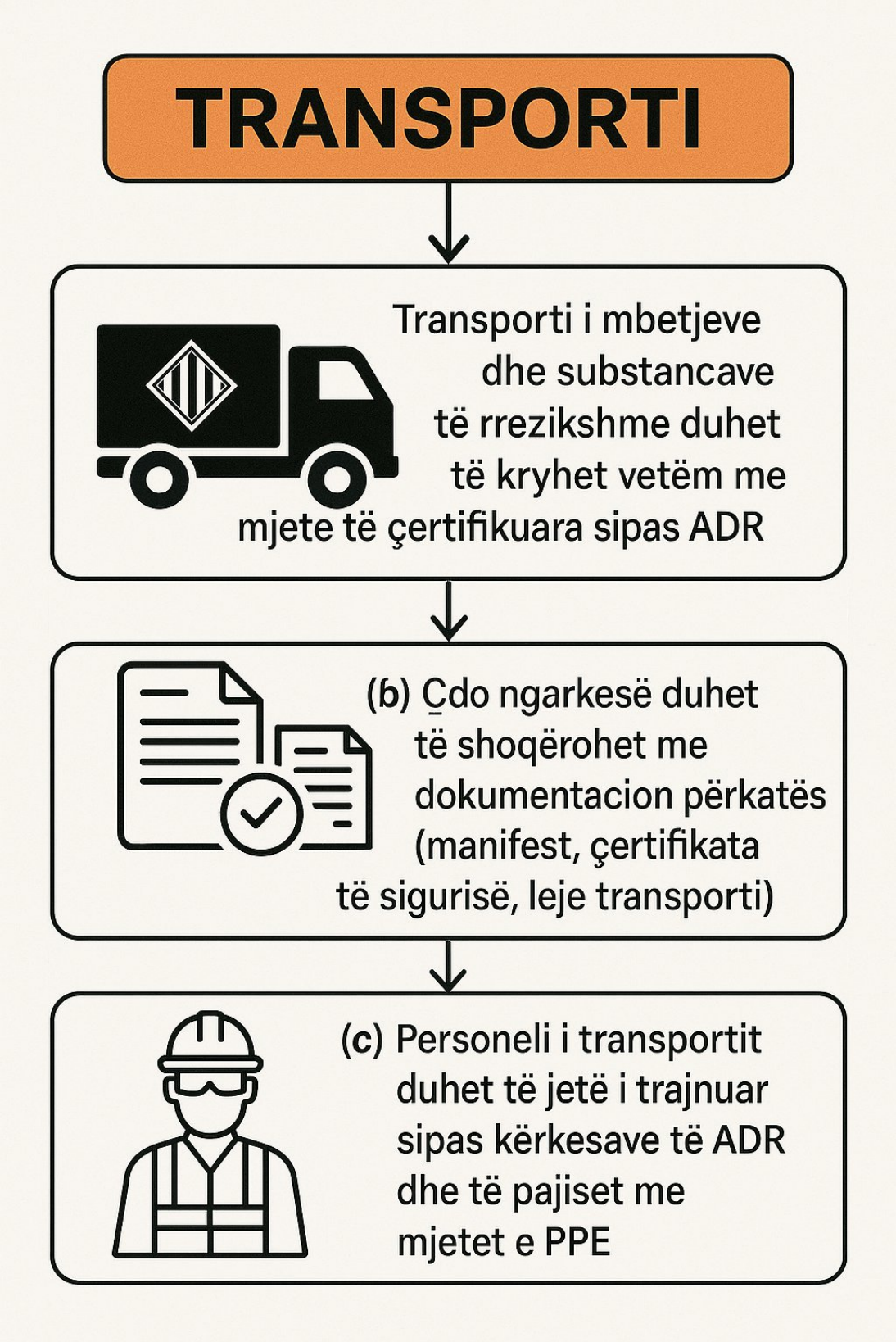
a) Mbetjet dhe substancat e rrezikshme duhet të ruhen në ambiente të veçanta, të ventiluara dhe të pajisura me masa kundër zjarrit.

b) Ambientet e depozitimit duhet të kenë tokëzim dhe dysheme të papërshkueshme nga lëngjet.

c) Duhet të respektohen distancat e sigurisë sipas standardeve AASTP-1 dhe AASTP-5.

ç) Sasia maksimale e lejuar për ruajtje përcaktohet në autorizimin e dhënë nga AIM.

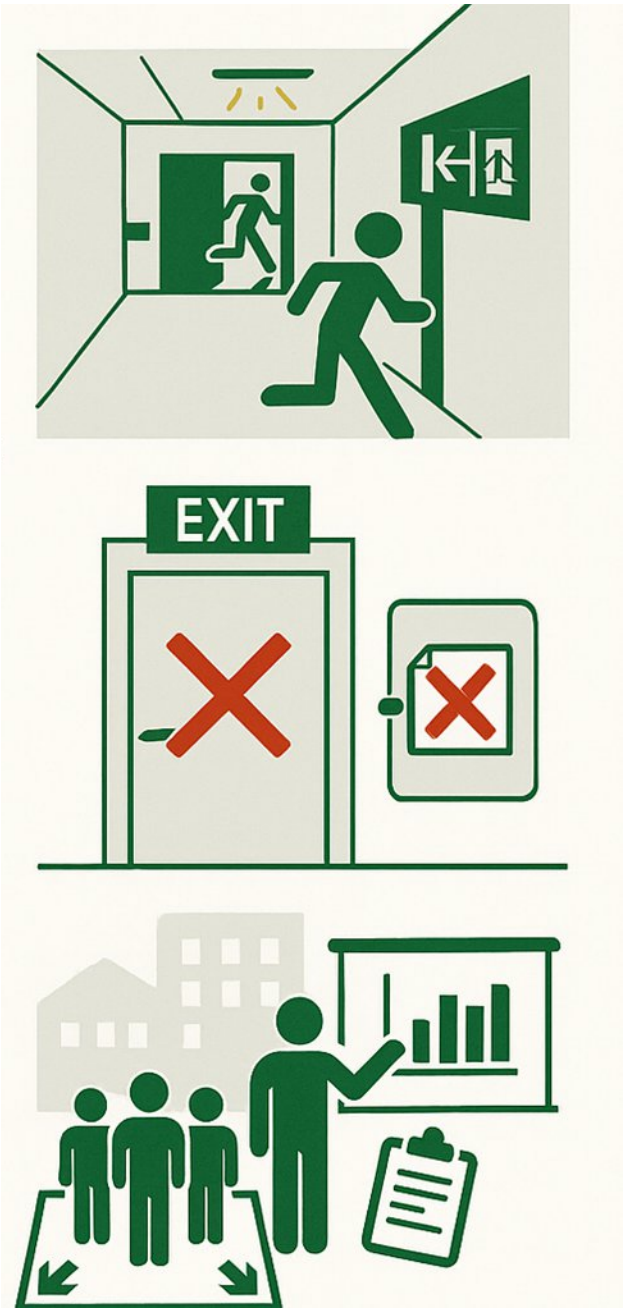
3. Transporti



ANEKSI Ë
Procedurat e reagimit ndaj emergjencave

1. Planifikimi i emergjencave

2. Evakuimi i personelit


EXIT