



Republika e Kosovës
Republika Kosovo - Republic of Kosovo



Autoriteti i Aviacionit Civil i Kosovës
Autoritet Civilnog Vazduhoplovstva Kosova
Civil Aviation Authority of Kosovo

Publikimi Teknik - TP 26

Sistemi i menaxhimit të sigurisë (SMS)

Udhëzues për Qendrat Aeromjekësore (AeMC)

Material udhëzues

Parathënie

Ky material udhëzues aplikohet për funksione të ndërlidhura me menaxhimin e sigurisë, apo si mbështetje e drejtpërdrejtë e Qendrave AeroMjekësore të autorizuara nga Autoriteti i Aviacionit Civil i Kosovës (AACK) konform dispozitave ligjore të Rregullores së AAC-së Nr. 5/2015 që përcakton kërkesat teknike dhe procedurat administrative në lidhje me personelin e ekuipazhit ajror të aviacionit, Shtojca IV [PJESA-MED].

Ky material udhëzues është përgatitur nga AAC si doracak për rregullimin e kësaj fushe të aviacionit civil. Për shprehjet e ideve në këtë udhëzues mund të pretendohen të drejta autoriale në rast se ekziston dyshimi për shkelje të tyre. Përgatitja e një publikimi tjetër të kësaj natyre ndalohet përveç nëse dallon substancialisht nga ky udhëzues, dhe nëse nuk është kopje e tij.

Nëse keni nevojë për informata shtesë, ju lutem të na shkruani në adresën e mëposhtme:

Autoriteti i Aviacionit Civil i Kosovës

Lagjja Arbëria; Rruga Ahmet Krasniqi nr. 208

10000 Prishtinë

Republika e Kosovës

e-mail: infocaa@caa-ks.org

Tel: +383 38 248 629

Fax: +383 38 211 009

Dritan Gjonbalaj

Drejtore i Përgjithshëm

Lista e faqeve efektive

Titulli	Faqe	Nr. Rev.	Data efektive
Parathënie	2 nga 45	Origjinal	20.11.2018
Lista e faqeve efektive	3 nga 45	Origjinal	20.11.2018
Tabela e aprovimit	4 nga 45	Origjinal	20.11.2018
Lista e distribuimit / Tabela e revidimit	5 nga 45	Origjinal	20.11.2018
Tabela e përmbajtjes	6 nga 45	Origjinal	20.11.2018
Hyrje	7 nga 45	Origjinal	20.11.2018
Politika dhe objektivat e sigurisë	10 nga 45	Origjinal	20.11.2018
Menaxhimi i rrezikut në siguri	14 nga 45	Origjinal	20.11.2018
Garantimi i sigurisë	21 nga 45	Origjinal	20.11.2018
Promovimi i sigurisë	24 nga 45	Origjinal	20.11.2018
Proceset specifike të një AeMC-je	25 nga 45	Origjinal	20.11.2018
Zbatimi efektiv i një SMS-je	27 nga 45	Origjinal	20.11.2018
Shtojca A - Shembull i politikës së sigurisë	28 nga 45	Origjinal	20.11.2018
Shtojca B - Shembull i regjistrit të riskut dhe vlerësimit të rrezikut	29 nga 45	Origjinal	20.11.2018
Shtojca C - Shembull i faqes të përmbajtjes së manualit të SMS-së	36 nga 45	Origjinal	20.11.2018
Shtojca D - Shembull i formularit të raportimit të sigurisë	37 nga 45	Origjinal	20.11.2018
Shtojca E - Shembull i objektivave të sigurisë së AeMC-së dhe treguesit e performansës së sigurisë	40 nga 45	Origjinal	20.11.2018
Shtojca F - Pyetje vlerësuese për të mbështetur analizën "GAP"	41 nga 45	Origjinal	20.11.2018

Tabela e aprovimit

	Emri dhe pozita	Data	Nënshkrimi
Përgatitur nga:	Driton Avdiu Vlerësues i autorizuar mjekësor (AMA), DSF	25.10.2018	
Autorizuar nga:	Kushtrim Musa Drejtor, DSF	13.11.2018	
Kontrolli i cilësisë:	Lendita Kika-Berisha Drejtor, DSC	16.11.2018	
Aprovuar nga:	Dritan Gjonbalaj Drejtor i përgjithshëm	20.11.2018	

Lista e distribuimit

Kopje nr.	Vendndodhja	Media	Sasia
1	Libraria e AAC-së	Origjinali	1
2	Serveri i dosjeve të AAC-së	Digjitale	1

Tabela e revidimit

Nr. Rev.	Datë	Përgatitur nga:	Autorizuar nga:
1			
2			
3			
4			
5			

Tabela e përmbajtjes

Parathënie.....	2
Lista e faqeve efektive.....	3
Tabela e aprovimit.....	4
Lista e distribuimit / Tabela e revidimit.....	5
Tabela e përmbajtjes.....	6
Hyrje.....	7
Politika dhe objektivat e sigurisë.....	10
Menaxhimi i rrezikut në siguri.....	14
Garantimi i sigurisë.....	21
Promovimi i sigurisë.....	24
Proceset specifike të një AeMC-je.....	25
Zbatimi efektiv i një SMS-je.....	27
Shtojca A.....	28
Shtojca B.....	29
Shtojca C.....	36
Shtojca D.....	37
Shtojca E.....	40
Shtojca F.....	41

1. Hyrje

Pse nevojitet një Sistem i Menaxhimit të Sigurisë (*Safety Management System (SMS)*)?

- 1.1 Në vitet e fundit njohuritë tona kanë avancuar se si ndodhin aksidentet dhe incidentet në fushën e aviacionit civil. Tani shumë më tepër theks i kushtohet faktorëve shkakësorë të përfshirë dhe faktorëve organizativë që kontribuojnë në paraqitjen e gabimeve, që çojnë në këto ngjarje të padëshiruara. Faktorët organizativë përfshijnë mënyrën se si funksionon një organizatë (*në këtë rast AeMC-ja*), si i përcakton ajo procedurat e saja, si trajnon personelin dhe çfarë niveli të rëndësisë i kushton çështjeve të sigurisë, të cilat janë identifikuar në kuadër të organizatës.
- 1.2 Sistemi i Menaxhimit të Sigurisë (SMS) lejon që ju të zhvilloni një qasje proaktive ndaj sigurisë duke i identifikuar disa prej këtyre faktorëve shkaktarë dhe duke ndërmarrë veprime, para se të ndodhë një ngjarje që cenon nivelin e sigurisë. SMS ju ndihmon që të keni një kuptim më të plotë të risqeve dhe rreziqeve që ndikojnë në sigurinë e AeMC-së tuaj. Këto risqe dhe rreziqe mund të kenë ndikim të rëndë në AeMC-në tuaj, në aspektin e kostos financiare dhe të dëmtim të reputacionit, prandaj SMS është një mënyrë efektive që ju të ngritni institucionin tuaj përtej nivelit të përputhshmërisë me legjislacionin në fuqi.
- 1.3 Agjencia Evropiane e Sigurisë së Aviacionit (*anglisht: European Aviation Safety Agency (EASA)*) mandaton Qendrat Aeromjekësore (*anglisht: AeroMedical Centres (AeMC)*) që janë në kuadër të fushëveprimtarisë së saj, që të zhvillojnë një SMS të përshtatshëm për organizata jo-komplekse. Organizata Ndërkombëtare e Aviacionit Civil (*anglisht: International Civil Aviation Organisation (ICAO)*) gjithashtu kërkon nga këto organizata që të kenë një SMS.

Çka është SMS-ja?

- 1.4 SMS është një qasje e organizuar për menaxhimin e sigurisë. Ajo përcakton strukturën e organizatës, identifikon përgjegjësitë tëanëtarëve kyçë të personelit dhe dokumenton politikat dhe procedurat për menaxhimin efektiv të sigurisë. Një SMS efektiv, lejon që risqet dhe rreziqet që potencialisht mund të ndikojnë në AeMC-në tuaj të identifikohen, vlerësohen dhe prioritetizohen me kohë, në mënyrë që të vendosen masat adekuate zbutëse për të zvogëluar rreziqet, në nivelin praktikisht sa më të ulët të arritshëm (*anglisht: as low as reasonably practicable (ALARP)*).

- 1.5 Një rrezik mund të përshkruhet si ALARP, nëse janë ndërmarrë të gjitha masat e arsyeshme për të zbutur rrezikun dhe kostoj (në aspektin e kohës, përpjekjeve dhe parave) për ndërmarrjen e veprimeve të mëtutjeshme në këtë drejtim do të ishte “krejtësisht joproporcionale”, me reduktimin e mëtejshëm të nivelit të rrezikut. Reduktimi i rrezikut në nivelin ALARP nuk nënkupton që rreziku është eliminuar në tërësi, pasi ende mbetet një nivel i rrezikut, por organizata e kapranuar nivelin e mbetur të rrezikut.
- 1.6 Ka shumë materiale këshilluese dhe udhëzuese për SMS-në që tashmë janë në dispozicion, por AeMC-të inkurajohen që gjatë përpilimit të SMS t’ju referohen rregulloreve të AAC-së (Rregullores 05/2015; Pjesa-MED dhe Pjesa-ORA), Shtojcave 1 dhe 19 të ICAO-s dhe Dokumentit Udhëzues 9859 Doracaku për Menaxhim të Sigurisë - udhëzime mbi SMS-në.
- 1.7 Zbatimi i SMS fillimisht mund të duket një detyrë e mundimshme, edhe pse ka të ngjarë që shumë prej elementeve kryesore që e përbëjnë një SMS tashmë ekzistojnë në organizatën tuaj, megjithëse jo të formalizuara apo të dokumentuara qartë. Struktura dhe përmbajtja e SMS-së duhet të jenë në thelb të njëjta për çdo organizatë, por niveli i hollësive të elementeve të veçanta duhet të reflektojnë madhësinë, kompleksitetin dhe nivelin e rreziqeve me të cilat përballlet AeMC-ja juaj. Është e rëndësishme të kuptohet se nuk ka një “model të gatshëm”, që iu përshtatet çdo organizate në kuptim të zhvillimit dhe zbatimit të SMS-së. Pra, ajo që është e rëndësishme është të zhvillohet një SMS që funksionon për AeMC-në tuaj.

Cilat janë elementet kryesore të një SMS-je?

- 1.8 Ky material udhëzues përshkruan elementet kryesore të një SMS-je. Gjithashtu kemi përfshirë pikat kryesore që do t’ju ndihmojnë të zbatoni SMS-në tuaj. Këto elemente janë:
- ❖ Politika dhe objektivat e sigurisë, ku hyjnë:
 - Përkushtimi dhe përgjegjësia e menaxhmentit;
 - Llogaridhënia përsigurinë;
 - Emërimi i anëtarëve kyç të personelit;
 - Planifikimi i reagimit emergjent (*anglisht: Emergency Response Planning*);
 - Dokumentimi i SMS-së.
 - ❖ Menaxhimi i rrezikut të sigurisë, ku hyjnë:
 - Identifikimi i riskut;
 - Vlerësimi dhe zbutja e rrezikut
 - ❖ Garantimi i sigurisë, ku hyjnë:
 - Monitorimi dhe matja e performancës së sigurisë;
 - Menaxhimi i ndryshimeve;
 - Përmirësimi i vazhdueshëm.
 - ❖ Promovimi i sigurisë, ku hyjnë:

- Trajnimi dhe edukimi;
- Komunikimi për sigurinë.

- 1.9 Një SMS efektive kërkon vendosjen e këtyre elementeve. Deri në çfarë mase këto elemente janë në vend do të varen nga madhësia dhe kompleksiteti i AeMC-së tuaj, si dhe nga pjekuria e SMS-së tuaj. Ky material udhëzues jep vetëm orientime të përgjithshme, i dedikuar për të gjitha AeMC-të, prandaj se si do t'i zbatoni elementet kyçe të tij, do të varet nga rrethanat specifike të AeMC-së tuaj.
- 1.10 Një SMS efektive gjithashtu kërkon vendosjen e një “Kulturë të Drejtë” (“Just Culture”) të raportimit të sigurisë, që nënkupton inkurajimin dhe mbështetjen e personelit për dhënjen e informatave me rëndësi thelbësore për sigurinë, në një ambient miqësor (jo kërcënues) në organizatën tuaj, ku megjithatë ekziston një linjë e qartë në mes të sjelljes të pranueshme dhe të papranueshme.

2. Politika dhe objektivat e sigurisë

Përkushtimi dhe përgjegjësia e menaxhmentit

- 2.1 Për të qenë efektiv SMS i juaj, duhet ndarë kohën dhe resurse të mjaftueshme. Kjo kërkon nga menaxhmenti i lartë të tregojë përkushtim dhe të marrë përgjegjësi për SMS-në e AeMC-së tuaj. Pa këtë, SMS-ja nuk mund të funksionojë me efektivitet të plotë.
- 2.2 Përkushtimi i menaxhmentit ndaj sigurisë duhet të shprehet përmes një politike të shkruar të sigurisë. Kjo politikë duhet të vendosë një drejtim të qartë të nivelit të lartë i cili duhet të ndiqet nga AeMC-ja, me qëllim të menaxhimit efektiv të sigurisë dhe duhet të pranohet nga Menaxheri Përgjegjës (Accountable Manager).
- 2.3 Politika e sigurisë duhet të lexohet dhe të kuptohet nga të gjithë anëtarët e personelit dhe duhet të përkthehet në veprime konkrete, e jo vetëm fjalë mbresëlënëse që hudhen në një dokument-letër. Menaxheri Përgjegjës duhet të demonstrojë në mënyrë aktive përkushtimin e tij/saj ndaj politikës së sigurisë. Kjo do t'i kontribuojë krijimit të një kulture të drejtë në kuadër të AeMC-së, e që është me rëndësi thelbësore për suksesin e SMS-së tuaj. Përmes kulturës së drejtë të gjithë anëtarët e personelit duhet të jenë përgjegjës për sigurinë dhe do të marrin parasysh implikimet e sigurisë për çdo aktivitet që kryejnë në kuadër të organizatës.
- 2.4 **Pikë kryesore** – Politika e juaj e sigurisë duhet të jetë individuale, që reflekton gjendjen e AeMC-së tuaj. Si minimum ajo duhet të:
- Të përshkruajë qasjen themelore të AeMC-së suaj ndaj sigurisë;
 - Të tregojë përkushtimin e menaxhmentit të lartë për sigurinë;
 - Të tregojë përkushtim për të siguruar resurse adekuate për të menaxhuar sigurinë në mënyrë efektive dhe për të zvogëluar rreziqet në një nivel të pranueshëm;
 - Të inkurajojë të gjithë anëtarët e personelit që të marrin pjesë në mënyrë aktive dhe t'i zbatojnë të gjitha aspektet e SMS-së;
 - Të inkurajojë një “kulturë të drejtë të sigurisë” (*just safety culture*) në kuadër të organizatës.

Përgjegjësitë e sigurisë

- 2.5 Struktura e menaxhimit të AeMC-së tuaj duhet të definohet qartë. Për organizata të vogla kjo strukturë mund të jetë mjaft e thjeshtë dhe të përbëhet në një person përgjegjës (Accountable Manager) dhe anëtarë të tjerë të

- personelit që kanë rol kyç në mënyrën e menaxhimit të organizatës në baza ditore (prej ditës në ditë). Përgjegjësia dhe përgjegjësitë e menaxherit përgjegjës dhe anëtarëve kyç të personelit duhet të kuptohen qartë.
- 2.6 Menaxheri përgjegjës duhet të jetë normalisht personi që është përfundimisht përgjegjës për sigurinë dhe i cili është i përfshirë në menaxhimin e përditshëm të organizatës. Ka rëndësi thelbësore që menaxheri përgjegjës të ketë autoritetin dhe kontrollin buxhetor për të marrë vendimet lidhur me sigurinë dhe të ndër marrë veprimet e duhura për të ruajtur sigurinë.
- 2.7 **Pikë kryesore** – Përgjegjësia për çështje të sigurisë mund të delegohet sipas rastit, megjithatë, menaxheri përgjegjës mbetet përfundimisht përgjegjës për çështjet e sigurisë në kuadër të organizatës në çdo kohë.
- 2.8 **Pikë kryesore** – AeMC duhet të përpilojë një skemë organizative duke treguar pozitat kryesore me përgjegjësitë e tyre dhe linjat e llogaridhënies brendatë organizatës.

Emërimi i anëtarëve kyç të personelit

- 2.9 AeMC-ja kërkohet që të ketë një ekzaminues aero-mjekësor (AME) të nominuar si udhëheqës të AeMC-së. Ky mjek duhet të ketë privilegje për të lëshuar certifikata mjekësore të Klasës 1 dhe eksperiencë të mjaftueshme në mjekësinë e aviacionit. Udhëheqësi i AeMC-së është përgjegjës për koordinimin e vlerësimeve të rezultateve të ekzaminimeve mjekësore dhe nënshkrimin e raporteve, certifikatave dhe certifikatave fillestare të Klasës 1. AeMC-ja duhet gjithashtu të ketë në përbërje të personelit një numër të mjaftueshëm të AME-ve të kualifikuar plotësisht dhe personel tjetër teknik dhe ekspertë. Një individ duhet të identifikohet për pikë qendrore (focal point) për SMS. Ky person mund të jetë udhëheqësi i AeMC-së, nëse njëkohësisht është edhe menaxher përgjegjës ose sipas nevojës ky funksion mund t'i delegohet një anëtar të personelit si një funksion me orar jo të plotë.
- 2.10 **Pikë kryesore** – Një anëtar në AeMC-në tuaj duhet të ketë funksionin e menaxhimit të SMS-së dhe duhet t'i raportojë drejtpërdrejtë menaxherit përgjegjës.
- 2.11 Varësisht nga madhësia e AeMC-së, pika qendrore (focal point) mund të ketë nevojë të mbështetet nga një Komitet i Sigurisë. Për AeMC-të e vogla ky Komitet mund të përbëhet nga anëtarët kyç të personelit apo anëtarë të organizatave tjera që ndërveprojnë ngushtë me AeMC-në tuaj.
- 2.12 **Pikë kryesore** – Ka rëndësi që personat me përgjegjësi, si në kuadër të AeMC-së ashtu edhe të institucioneve që ndërveprojnë me të, të takohen dhe të diskutojnë çështjet që ndërlidhen me sigurinë, mbi bazë të intervaleve të rregullta kohore.

Planifikimi i reagimit në situata emergjente (Emergency Response Planing-ERP)

- 2.13 Planifikimi i reagimit në situata emergjente (ERP) duhet të krijohet dhe të përshkruajë veprimet që duhet të ndërmerren nga personeli në situatë emergjente.
- 2.14 Si minimum ERP-ja duhet të përshkruaj procedurat e për:
- Një tranzicion të rregullt nga operacionet normale në ato emergjente;
 - Përcaktimin e autoritetit emergjent (i cili do të marrë përsipër përgjegjësitë jashtë orarit të rregullt të punës apo gjatë fundjavës?);
 - Delegimin e përgjegjësive emergjente (çka ndodhë nëse ai person mungon apo është në pushim?);
 - Koordinimin e përpjekjeve për zgjidhjen e situatës emergjente (kush do t'i thërras shërbimet emergjente?);
 - Vazhdimin e sigurt të operacioneve (punës) ose kthimi në operacione normale, sa më shpejt që të jetë e mundur, pas përfundimit të situatës emergjente.
- 2.15 ERP-ja-ja duhet të identifikojë përgjegjësitë, rolet dhe veprimet e anëtarëve të personelit të përfshirë në ballafaqimin me emergjenca në kuadër të AeMC-së dhe të konsiderojë përfshirjen e një agjensie të jashtme apo pale të tretë, nëse është e nevojshme në përmbushjen e ERP-së.
- 2.16 **Pikë kryesore** – ERP-ja duhet të jetë në dispozicion dhe e kuptueshme nga të gjithë anëtarët e personelit dhe duhet të ushtrohet në mënyrë të rregullt, për të siguruar që të gjithë janë të vetëdijshëm për përgjegjësitë dhe veprimet e kërkuara nga ai/ajo si dhe është i aftë për të kryer veprimet e duhura në situata emergjente.
- 2.17 **Pikë kryesore** – Është e rëndësishme të koordinoni ERP-në tuaj me organizatat tjera me të cilat ndërveproni, përfshirë shërbimet emergjente që mund të marrin pjesë gjatë emergjencës dhe organizatat e palëve të treta që mund të jenë të kontraktuara nga AeMC-ja.

Dokumentimi dhe kontrolli i SMS-së

- 2.18 Të gjitha aspektet e SMS-së tuaj duhet të dokumentohen në mënyrë të qartë, me qëllim të mbajtjes së një regjistri të saktë të vendimeve dhe të veprimeve të ndërmarra dhe pse janë zbatuar ndryshimet eventuale. Dokumentacioni juaj duhet të kontrollohet dhe duhet të jetë në një format të përshtatshëm, në mënyrë që të kuptohet qartë nga anëtarët e personelit të AeMC-së, apo të

palëvet të treta të kontraktuara për të punuar me ju dhe autoritetin mbikqyrës kompetent. Në shtojcat e këtij materiali udhëzues janë dhënë modele dhe shembuj që mund të jenë të dobishme. Dokumentacioni i qartë mundëson që SMS-ja juaj të auditohet ose të vlerësohet me lehtësi.

2.19 Si minimum dokumentacioni i SMS-së duhet të përfshijë:

- Politikën dhe objektivat e sigurisë të SMS-së;
- Llogaridhënien dhe përgjegjësinë e menaxherit përgjegjës dhe anëtarëve kyç të personelit;
- Të gjitha proceset, procedurat apo listat e kontrollit që lidhen me sigurinë;
- Rezultatet dhe veprimet pasuese nga auditimet apo vlerësimet e sigurisë;
- Rezultatet e të gjitha vlerësimeve të rrezikut dhe të masave zbutëse, që ekzistojnë;
- Një regjistër të riskut (një shembull i regjistrit të riskut/vlerësimi të rrezikut mund të gjendet në shtojcën B të këtij materiali udhëzues);
- Pikat specifike të listuara në Kapitullin 6

2.20 Ju mund të konsideroni të përshtatshëm krijimin e një manuali të veçantë të SMS-së për AeMC-në tuaj ose dokumentimi i SMS-së tuaj brenda manualeve ekzistuese mund të jetë më i lehtë. Një shembull i faqes së përmbajtjes së një manuali për SMS-në mund të gjeni në Shtojcën C të këtij materiali udhëzues. Dokumentet e tjera mund të mbahen si kopje fizike ose elektronike. Megjithatë, shënimet e SMS-it tuaj duhet të ruhen në një sistem të besueshëm dhe sigurt, për shembull sistemet e teknologjisë informative duhet të krijojnë një kopje rezervëmbështeten dhe të mbrohen nga dëmtimi dhe të mundësojnë qasje dhe nxjerrje të lehtë të këtyre informacioneve.

3. Menaxhimi i rrezikut të sigurisë - (anglisht: Safety Risk Management)

Hyrje në menaxhimin e rrezikut të sigurisë

- 3.1 Procesi i menaxhimit të rrezikut të sigurisë fillon me identifikimin e risqeve që ndikojnë në sigurinë e AeMC-së dhe pastaj vlerësimin e rreziqeve të ndërlidhura me risqet në kuptim të mundësisë/propabilitetit-likelihood (cila është mundësia e paraqitjes së rrezikut?) dhe ashpërsisë-severity (nëse rreziku ndodhë sa i rëndë mund të jetë?). Pasi të identifikohet niveli i rrezikut, masat e përshtatshme përmirësuese apo zbutëse mund të zbatohen, për ta ulur nivelin më të ulët arsyeshëm të arritshëm të rrezikut në (ALARP) për aq sa është e mundur. Masat e zbatuara zbutësetë rrezikut pastaj duhet të monitorohen, për t'u siguruar që ato kanë arritur efektin e dëshiruar.

Figura 1: Një proces i thjeshtë i menaxhimit të rrezikut



- 3.2 Risku-Hazardi është thjesht i definuar si një gjendje, ngjarje apo rrethanë, që ka potencial të shkaktojë lëndime njerëzve apo dëmtimin e mjeteve ajrore, pajisjeve apo strukturave.
- 3.3 Rreziku definohet si rezultat i mundshëm nga risku dhe zakonisht përcaktohet si kuptim i propabilitetit të dëmtimit që të ndodhë dhe përmasës/ashpërsisë nëse ai paraqitet.

❖ Për shembull:

Gjilpëra për marrjen e gjakut paraqet risk, si për pacientin ashtu edhe për personelin mjekësor. Risk shtesë paraqet gjaku i aplikantit i prekur nga një

sëmundje transmise (si psh HIV ose Hepatiti B). Rrezik shtesë paraqet mundësia që gjilpëra e kontaminuar me gjak të këtij aplikanti/kandidati ta shpojë lëkurën e stafit mjekësor të AeMC-së dhe të inokulohet në organizmin e një pjesëtari të stafit mjekësor.

- 3.4 Në përgjithësi risku ekziston në momentin e tanishëm, përderisa rreziku ilidhur me të është një rezultat pasues i mundshëm në të ardhmen.

Sistemet e raportimit

- 3.5 Risqet mund të kontrollohen vetëm nëse ekzistenca e tyre është e ditur. Nëpërmjet sistemit konfidencial të raportimit të sigurisë, mund të identifikohen situatat apo kushtet të cilat kanë potencial për të rrezikuar sigurinë e operimeve të mjeteve ajrore.. Raportimet e sigurisë mund të jenë reaktive (për një ngjarje që tashmë ka ndodhur) ose proaktive (nga një situatë potencialisht e pasigurt që identifikohet) apo parashikuese (duke u përpjekur për të parashikuar se çfarë mund të ndodhë në të ardhmen).
- 3.6 Raportimi i brendshëm vullnetar i incidenteve me më pak peshë, që jodomosdoshmërisht kërkohen që të raportohen sipas një skeme të raportimit të detyrueshëm, por që janë shumë të dobishme për AeMC-në tuaj, duhet të inkurajohen në mënyrë aktive. Niveli më i lartë i raportimit, madje edhe për çështje që mund të konsiderohen si të vogla, do të mundësojë monitorimin e performancës së sigurisë të AeMC-së dhe identifikimin e tendencave të sigurisë në zhvillim.
- 3.7 Të gjithë anëtarët e personelit të AeMC-së dhe anëtarët e institucioneve tjera që ndërveprojnë me AeMC-në duhet të marrin pjesë në mënyrë aktive në sistemin e raportimit të sigurisë. Të gjithë hisedarët dhe përdoruesit e shërbimeve duhet ta kenë të qartë se si të raportojnë, çfarë të raportojnë dhe kujt t'i raportojnë. Informacionet e mbledhura nga këto raporte, pastaj mund të shfrytëzohen për të identifikuar rreziqet e sigurisë, në mënyrë që veprimet e duhura të ndërmerren në këtë drejtim.
- 3.8 Sistemi i raportimit duhet të përdorë informacionet e mbledhura për të rritur sigurinë, e jo për të atribuar fajin, në rast të ndonjë gabimi të bërë gjatë punës. Për të inkurajuar raportimin pa frikën e pasojave, është e rëndësishme që të gjithë anëtarët e stafit të ndjejnë së në AeMC ka një kulturë të hapur dhe të drejtë të raportimit të sigurisë. Gjithashtu është me rëndësi që personi i cili ka raportuar incidentin/gabimin t'i jepet një informacion kthyes adekuat pas raportimit të tij.
- 3.9 **Pikë kryesore** – është me rëndësi të mbahet mend se identifikimi i riskut nuk është një proces statik që kryhet vetëm një herë; ai duhet të kryhet sa herë që planifikohet një ndryshim organizativ në AeMC, sa herë institucioni juaj po kalon në rritje apo tkurrje të shpejtë të kapaciteteve, sa herë ju filloni të

përdorni pajisje apo procedura të reja, sa herëndryshohen anëtarë kyç të personelit ose në çfarëdo rasti kur vlerësoni se ekziston mundësia për zhvillimin e një rreziku të ri për sigurinë e organizatës tuaj.

- 3.10 **Pikë Kryesore** – Për të inkurajuar personelin për të raportuar risqet potenciale, AeMC e juaj duhet të ketë një sistem të raportimit të sigurisë i cili është i drejtë, konfidencial, i thjeshtë dhe i përshtatshëm për t'u përdorur. Në një sistem të drejtë të raportimit të sigurisë, punonjësit nuk duhet të ndëshkohen për gabime ose lëshime të paparamenduara ose pa dashje ose lëshimeve. Në vend të kësaj, arsyet për gabimet duhet të hetohen në mënyrë që të nxirren mësimet e sigurisë.

Identifikimi i riskut (anglisht: Hazard)

- 3.11 Procesi i identifikimit të riskut është mjet formal i grumbullimit, evidentimit, analizimit, veprimit dhe gjenerimit informacioneve kthyese(anglisht: feedback) rreth riskut që ndikojnë në sigurinë e aktiviteteve operationale të AeMC-së tuaj. Në një SMS të pjekur identifikimi i riskut është një proces i vazhdueshëm.
- 3.12 Ka shumë mënyra të identifikimit të risqeve dhe varësisht nga madhësia e AeMC-së tuaj, metodat e mëposhtme mund të jenë të dobishme:
- Shqyrtim i ideve (Brainstorming), ku Komiteti i Sigurisë apo grupe të vogla punuese takohen për të identifikuar risqet e mundshme;
 - Të dhënat nga aksidentet e mëparshme, incidentet apo aksidentet dhe analizat e rëndësishme të ngjarjeve që lidhen me to;
 - Sistemet e raportimit të detyrueshëm/vullnetar të incidenteve (të brendshme dhe të jashtme);
 - Vlerësimet / auditimet e sigurisë të kryera nga brenda ose jashtë
 - Informacionet mbi sigurinë nga burimet e jashtme, p.sh. organizata të ngjashme, media, grupet e hetimit të aksidenteve ajrore, autoritetet kombëtare të aviacionit etj;
 - Listat e përgjithshme të kontrollit të riskut.

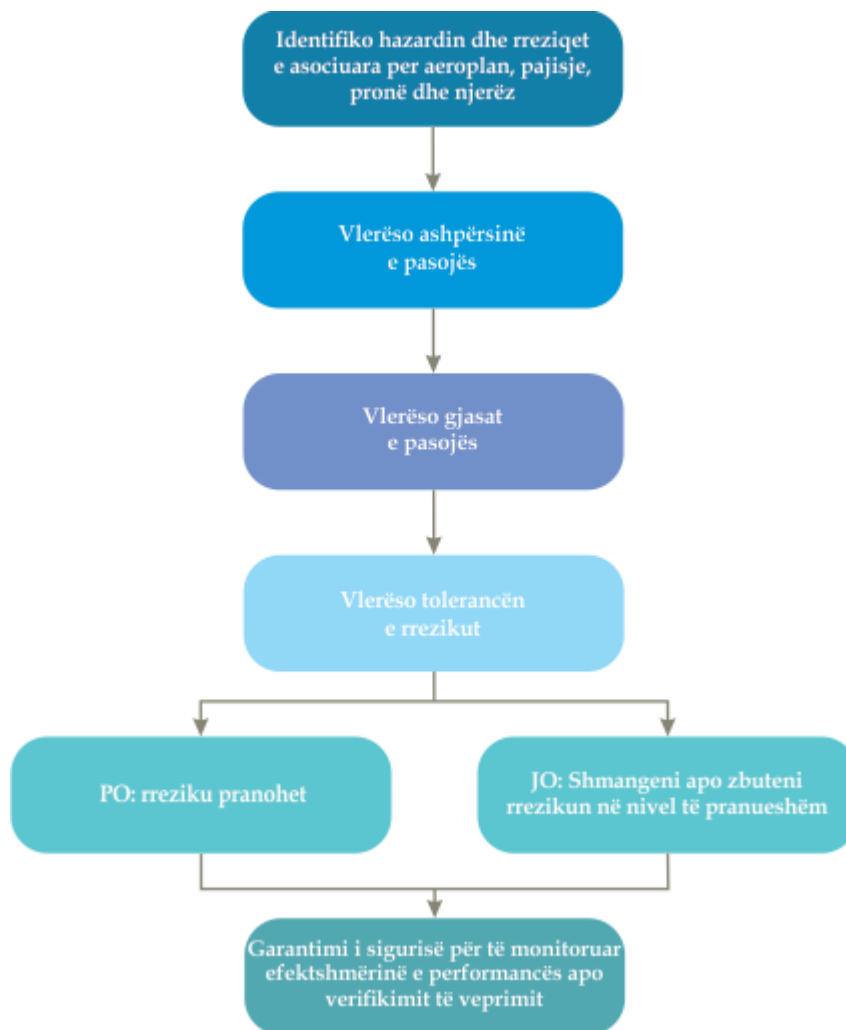
Vlerësimi dhe zbutja e rrezikut

- 3.13 Qëllimi i procesit të vlerësimit të rrezikut, është t'i mundësojë AeMC-së vlerësimin e nivelit të rrezikut të ndërlidhur me identifikimin e risqeve, në lidhje me dëmin e mundshën. Rreziqet duhet të vlerësohet në kuptimin e ashpërsisë dhe propabilitetit. Pasi të keni vlerësuar rrezikun në lidhje me ashpërsinë dhepropabilitetin, një matricë e thjeshtë e vlerësimit të riskut mund të përdoret për të përcaktuar nivelin e përgjithshëm të rrezikut. Në varësi të nivelit të rrezikut, mund të merren masa adekuate zbutëse për të eliminuar rrezikun ose për të zvogëluar rrezikun në një nivel më të ulët ose sa më të ulët që është praktikisht e arsyeshme (ALARP), në mënyrë që të jetë e pranueshme

për AeMC-në tuaj. Masat zbutëse duhet të zbatohen për të zvogëluar gjasën e paraqitjes së rrezikut, apo për të reduktuar ashpërsinë rezultuese të tij, nëse paraqitet.

- 3.14 Procesi i vlerësimit gjithashtu lejon që rreziqet të rangohen, në kuptim të potencialit të rrezikut, në mënyrë që prioritetet dhe resurset të mund të orientohen në mënyrë më efektive, në drejtim të rreziqeve të nivelit më të lartë. Figura 2 tregon një proces të thjeshtë të menaxhimit të rrezikut dhe një shembull se si mund të funksionojë ky proces është treguar në Shtojcën B të këtij materiali udhëzues.
- 3.15 **Pikë kryesore** – Është e rëndësishme të përfshihet personel me ekspertizë dhe përvojë përkatëse në procesin e vlerësimit të rrezikut, për të siguruar një proces të konsoliduar dhe të qëndrueshëm. Të gjitha vlerësimet e rreziqeve mbështeten në cilësinë e informacioneve të ofruara, me qëllim të arritjes së vlerësimit dhe në njohurinë e personelit të përfshirë në kryerjen e vlerësimit;

Figura 2: Një proces i thjeshtë i menaxhimit të rrezikut



- 3.16 Procesi i vlerësimit të rrezikut fillon me identifikimin e rrezikut/rreziqeve, të shoqëruara me risqet që janë identifikuar paraprakisht. Mund të paraqitet më shumë se një rrezik i ndërlidhur me një risk të veçantë dhe vlerësimi i rrezikut mund të ketë nevojë të kryhet për secilin rrezik.

Ashpërsia e rrezikut

- 3.17 Rreziku do të duhet të vlerësohet në bazë të ashpërsisë së tij (sa i rëndë do të jetë nëse ndodhë?). Në mënyrë që të vlerësoni ashpërsinë, duhet të merrni parasysh çdo masë lehtësuese që aktualisht është në vend për të zvogëluar ashpërsinë. Ju duhet të vlerësoni ashpërsinë në kuptim të skenarit më të keq të mundshëm realist, por mund të vëreni se duke shikuar në rezultatin më të besueshëm është më e lehtë të klasifikoni nivelet e ashpërsisë..
- 3.18 Për të ndihmuar në vlerësimin e ashpërsisë së rrezikut ju duhet të bëni pyetjet e mëposhtme:
- A do të humben jetërat me këtë rast (të punonjësve, të aplikuesve, të udhëtarëve etj.)?
 - Cila është shkalla e mundshme dëmtimit të pajisjeve, pasurisë apo dëmtimit financiar?
 - Cili është propabiliteti indikimit në mjedis?
 - Cilat janë implikimet e mundshme komerciale apo interesi i medias?
 - A do të ketë humbje të reputacionit të organizatës?
- 3.19 Për të përcaktuar ashpërsinë, figura 4 e Shtojcës B jep një shembull të tabelës së ashpërsisë që mund të përdoret, ose mund të vendosni këtë përcaktori ashpërsinë në një mënyrë tjetër.

Gjasat e rrezikut

- 3.20 Rreziku gjithashtu do të duhet të vlerësohet në lidhje me gjasat e tij (sa është mundësia e rrezikut që ndodhë?) Me qëllim të vlerësimit të gjasave duhet të merrni parasysh çdo masë lehtësuese që është aktualisht në vend për të reduktuar gjasat. Përcaktimi i gjasave është ndonjëherë më i vështirë pasi nuk është një shkencë e saktë. Duhet të mbështetet në një analizë logjike dhe të përbashkët të rrezikut për të arritur në një përgjigje të arsyeshme
- 3.21 Për të ndihmuar në vlerësimin e propabilitetit, ju duhet të bëni pyetjet e mëposhtme:
- A ka ndonjë histori të ngjarjeve të ngjashme (qoftë në AeMC ose në organizata të tjera të njohura për ju) për rastin në fjalë, apo a është kjo një dukuri/ngjarje e izoluar?

- Cilat pajisje ose komponente të tjera të të njëjtit lloj mund të kenë të meta të ngjashme?
 - Cilat procese të tjera mund të preken në të njëjtën mënyrë?
 - Sa njerëz janë të përfshirë dhe sa i shpeshtë është aktiviteti?
 - Cili grup (tjetër) i aplikantëve mund të ndikohet?
- 3.22 Për të ju ndihmuar në përkufizimin e gjasave, figura 5 e Shtojcës B jep një shembull të një tabele tëpropabilitetit/gjasës, që mund të përdoret, ose mund të vendosni të përcaktoni propabilitetin në një mënyrë tjetër.

Toleranca e rrezikut

- 3.23 Kur ashpërsia dhe gjasat e paraqitjes së rrezikut janë përcaktuar, atëherë mund të përdoret matrica e tolerancës së rrezikut për të vlerësuar se sa i tolerueshëm është rreziku. Një shembull i matricës së tolerancës së rrezikut mund të gjendet në figurën 6 të Shtojcës B.
- 3.24 Duke përdorur një matricë të tolerancës së rrezikut, rreziku mund të klasifikohet ose si i pranueshëm, i rishikuar ose i papranueshëm, duke lejuar që të zhvillohet një strategji e përshtatshme për zbutjen e rrezikut nëse kërkohet.
- 3.25 **I Papranueshëm:** Nëse rreziku është i papranueshëm, veprimi apo aktiviteti duhet të ndërpritet menjëherë apo nuk duhet të zhvillohet fare. Zbutje e madhe e rrezikut nevojitet në këtë rast, me qëllim të reduktimit të ashpërsisë së rrezikut, nëse ai realisht ndodh, apo duhet të zvogëlohet gjasa e paraqitjes së rrezikut. Normalisht, mund të zvogëlohet gjasa e paraqitjes së rrezikut më shumë se sa ashpërsia e rrezikut.
- 3.26 **I Rishikuar:** Nëse rreziku kategorizohet këtu, atëherë ashpërsia ose gjasa e paraqitjes së tij përbën një shqetësim; Duhet të kërkohet masa për të zbutur rrezikun për aq sa është e arsyeshme (ALARP). Nëse pas ndërmarrjes së këtyre masave, rreziku vazhdon të mbetet në këtë kategori, atëherë kostoja e veprimeve të nevojshme për të ulur më tej rrezikun është shumë penguese. Rreziku mund të pranohet, me kusht që rreziku të kuptohet dhe të ketë miratimin e Menaxherit Përgjegjës.
- 3.27 **I Pranueshëm:** Nëse rreziku është i pranueshëm, atëherë pasoja e tij është me pak mundësi të ndodhë apo me përmasa jo aq të mëdha që të përbëjë një shqetësim dhe në këtë rast, toleranca ndaj rrezikut është e pranueshme. Sidoqoftë, duhet t'i kushtohet vëmendje zvoglimit të mëtejshëm të rrezikut.

Zbutja e rrezikut

- 3.28 Nëse niveli i rrezikut bie në kategorinë e papranueshme apo në atë të rishikuar, atëherë masat e zbutjes së rrezikut do të kërkohen për të zvogëluar rrezikun në një nivel sa më të ulët të mundshëm të arritshëm (ALARP).
- 3.29 Masat e zbutjes të rrezikut janë veprime ose ndryshime, siç janë ndryshimet në procedurat operative, në pajisje apo në infrastrukturë, për të zvogëluar si ashpërsinë ashtu edhe gjasat/propabilitetin e paraqitjes së rrezikut.
- 3.30 Në përgjithësi strategjitë për zbutjen e rrezikut klasifikohen në tri kategori:

Shmangia: Operacioni apo aktiviteti anulohet ose shmanget, sepse rreziku i sigurisë tejkalonë dobhtë e vazhdimit të aktivitetit, duke eliminuar kështu rrezikun në tërësi.

Zvogëlimi: Frekuenca e operacionit apo e aktivitetit zvogëlohet ose merret masë për zvogëlimin e përmasave/ashpërsisë të pasojave të rrezikut.

Segregimi/Ndarja: Veprimi merret për të izoluar efektet e pasojave të rrezikut ose për të ndërtuar masa të shumta mbrojtëse kundër tij.

Regjistri i riskut *(anglisht: Hazard log)*

- 3.31 Çfarëdo risku i identifikuar i sigurisë, vlerësimet e rrezikut dhe veprimet pasuese duhet të dokumentohen në mënyrë të qartë. Një mënyrë e pranueshme për t'a arritur këtë është krijimi i një regjistri të riskut apo ditari të rrezikut. Këto dy dokumente duhet të përshijnë secilin risk të identifikuar, rrezikun/rreziqet e ndërlidhura me të, rezultatet e vlerësimit të rrezikut, duke marrë parasysh çfarëdo mase aktuale zbutësetë vendosur, masat tjera për zbutjen e rrezikut nëse janë të nevojshme dhe një rivlerësim të rrezikut, sapo të merren masat zbutëse të zbatuara, për të vlerësuar nëse ato kanë arritur rezultatin e dëshiruar. Regjistri i riskut është dokument pune dhe duhet të rishikohet rregullisht, veçanërisht gjatë çdo takimi të Komitetit të Sigurisë. Regjistri i riskut është pjesë e dokumentacionit të SMS për AeMC-në tuaj. Shembuj të një regjistri të përshtatshëm të riskut dhe vlerësimit të rrezikut mund të gjenden në Shtojcën B të këtij materiali udhëzues.

4. Garantimi i sigurisë

Hyrje në garantimin e sigurisë

- 4.1 Garantimi i sigurisë monitoron performancën e sigurisë të AeMC-së tuaj dhe efektivitetin e SMS-së tuaj. Kjo do të sigurojë që identifikimi i riskut, vlerësimi i rrezikut dhe procesi i zbutjes së tyre të ndiqen në mënyrë efektive dhe se masat e duhura zbutëse po zbatohen dhe veprojnë sipas qëllimit.
- 4.2 **Pikë kryesore** - Elementi i garantimit të sigurisë jep besueshmëri se për të gjitha risqet e identifikuara aplikohen masat zbutëse dhe arrijnë objektivat e tyre të synuara.

Monitorimi dhe matja e performansës së sigurisë

- 4.3 Me qëllim të menaxhimit të performansës së sigurisë të AeMC-së, këtë performancë ju duhet ta matni në një mënyrë, dhe për këtë ju keni nevojë për të dhëna të sigurisë. Hapi i parë në këtë drejtim është identifikimi i treguesve të performansës së sigurisë (*anglisht: Safety Performance Indicators – (SPI)*). SPI-ja është një tregues që tregon se sa është e sigurtë AeMC-ja e juaj. Se çfarë SPI ju përdorni do të varet nga AeMC-ja e juaj dhe niveli i të dhënave që mbledhni, sidoqoftë disa shembuj të përgjithshëm janë dhënë në Shtojcën E.
- 4.4 **Pikë kryesore** -Treguesit e performancës jo gjithmonë duhet të bazohen në ngjarje; ia vlen të konsideroni frekuencën dhe pjesëmarrjen e takimeve të sigurisë dhe niveleve të raportimit të sigurisë, Kjo mund të përparojë me të dhëna të mjaftueshme për një rishikim të raporteve të sigurisë, të cilat mund të përfshijnë kategorizimin e raporteve të sigurisë në fushën e veprimit të raportuesit, llojet e ngjarjeve dhe llojet e pajisjeve ose aplikuesit.

Burimet e të dhënave të sigurisë

- 4.5 Burimet e të dhënave të sigurisë në kuptim të SPI-së mund të përfshijnë:
- Raportet e incidenteve dhe risqeve;
 - Ankesat e palëve të shërbyera;
 - Raportimet e detyrueshme, siç kërkohen me legjislacionin në fuqi;
 - Anketat e konsumatorëve apo të kontraktorëve;
 - Hulumtimet e sigurisë apo gjetjet e auditimeve në fushën e sigurisë.
- 4.6 Objektivat e performancës së sigurisë mund të jenë më të vështira për t'u definuar dhe mund të jetë më e rëndësishme të hulumtohen ngjarjet e veçanta dhe të shikohen trendet në kuadër të të dhënave të kufizuara që kemi në dispozicion, p.sh

shqyrtimi i raporteve të incidenteve/aksidenteve në organizatat tjera të ngjajshme, gjithashtu mund të rezultojnë me dobi.

Menaxhimi i ndryshimit

- 4.7 Aktivitetet e AeMC-së janë dinamike dhe ndryshimet mund të ndodhin shpesh. Një proces i thjeshtë duhet të vendoset për të identifikuar risqet potenciale dhe të vlerësojë ndikimin potencial në sigurinë e aktiviteteve, që mund të rezultojnë pas këtyre ndryshimeve. Ndryshimet përfshijnë futjen e pajisjeve të reja, ndryshimet në infrastrukturë apo fushëveprimtari, shërbimet e reja të kontraktuara, procedurat e reja ose ndryshimet në anëtarët kyç të personelit. A janë procedurat dhe dokumentacioni juaj ekzistues i përshtatshëm apo duhet të ndryshohen? A janë anëtarët e personelit të trajnuar mjaftueshëm dhe a janë të vetëdijshme grupet që ju shërbeni për këto ndryshime?
- 4.8 Duke marrë parasysh parimet e ALARP, qëllimi i procesit të menaxhimit të ndryshimit duhet të jetë që rreziku i ndërlidhur me ndryshimin e planifikuar, nuk do të ketë ndikim në aktivitetet e ardhshme dhe të tanishme të AeMC-së.
- 4.9 **Pikë kryesore** – Procesi i menaxhimit të ndryshimit duhet të përcillet me një qasje të njëjtë të strukturuar, sikurse procesi normal i vlerësimit të rrezikut i përdorur nga AeMC-ja.

Menaxhimi i incidenteve

- 4.10 Incidentet do të ndodhin në mënyrë të pashmangshme dhe kjo mund të paraqesë një mundësi të çmuar për të nxjerrë mësim për AeMC-në. Në një SMS efektiv duhet të ekzistojë një proces për të mësuar nga çdo incident dhe për të zbatuar çdo ndryshim që mund të kërkohet nga ky incident. Prandaj, AeMC-ja duhet ta ndërtojë një proces për të siguruar që çdo incident/aksident që ndodhë të hetohet, në mënyrë të duhur. Niveli i hetimit duhet të reflektojë rëndësinë e ngjarjes. Hetimi duhet të përfshijë çka ka ndodhur, kur, ku, si dhe kush është i përfshirë në të. Gjithashtu, duhet përpjekur të kuptohet se pse ka ndodhur kjo ngjarje. Gjatë këtij veprimi është me rëndësi të përcaktohen faktet dhe të shmangen spekulimet.
- 4.11 **Pikë kryesore** – Duhet të përpiqeni të jeni objektiv: hetimi duhet të gjejë se pse ndodhi ngjarja, me qëllim të parandalimit të përsëritjes së saj dhe jo për të gjetur dikë që duhet fajësuar.
- 4.12 **Pikë kryesore** – Komiteti i Sigurisë ose grupet punuese duhet të shqyrtojnë të gjitha gjetjet nga incidentet ose aksidentet dhe të rekomandojnë përmirësime nëse është e nevojshme. Mësimet e nxjerrura duhet të ndahen me anëtarët e tjerë të personelit dhe me organizatat tjera relevante me të cilat AeMC është në ndërveprim.

Përmirësimi i vazhdueshëm i SMS-së

4.13 SMS i juaj duhet të jetë pjesë përbërëse e AeMC-së tuaj. Ajo duhet të jetë dinamike, dhe jo statike, dhe duhet të ketë për qëllim që të përmirësojë në mënyrë të vazhdueshme performansën e sigurisë të AeMC-së tuaj.

Garantimi i sigurisë dhe mbikqyrja e përputhshmërisë së SMS

4.14 Si pjesë e SMS tuaj do të jetë e nevojshme themelimi i funksionit të mbikqyrjes së përputhshmërisë (për disa organizata kjo mund të jetë pjesë e sistemit të menaxhimit të cilësisë). Idealisht, funksioni i mbikqyrjes së përputhshmërisë është një vlerësim i pavarur që garanton se SMS-ja, është efektive dhe funksionale.

4.15 Kjo kërkon monitorimin për:

- Rishikimin se si AeMC juaj përputhet me kërkesat e publikuara për një SMS;
- Verifikimin që lehtësimet dhe kontrollet që janë vënë në vend për të kontrolluar risqet e identifikuar janë të qëndrueshme dhe efektive;
- Vlerësimin e efikasitetit të procedurave dhe proceseve në doracakun tuaj të SMS siç përshkruhet në të, dhe si ato zbatohen dhe praktikohen.

4.16 Duhet të ekzistojë një proces i mbyllur për të siguruar që problemet e identifikuar të korrigjohen. Auditimet duhet gjithashtu të përfshijnë vlerësimet e organizatave të tjera që lidhen me AeMC tuaj dhe që mund të ndikojnë në sigurinë.

4.17 **Pikë kryesore** - Në një AeMC të vogël ku të gjithë mund të përfshihen në SMS, do të jetë sfiduese të krijohet një rishikim apo auditim i pavarur. Në raste të tilla mund të kërkohet auditor i jashtëm i pavarur ose aranzhime të bëra me organizata të tjera të jashtme.

4.18 **Pikë kryesore** - Meqenëse sistemi i mbikqyrjes të përputhshmërisë ndihmon në monitorimin e performancës së sigurisë së AeMC-së, është e rëndësishme që Menaxheri i Përgjegjës të përfshihet dhe të monitorojë sistemin dhe atë që zbulohet.

4.19 **Pikë kryesore** - Si një AeMC e aprovuar mund të ketë kërkesa specifike që diktojnë atë që është e pranueshme si një sistem i mbikqyrjes së përputhshmërisë dhe ky udhëzim duhet të lexohet në kontekst me ato kërkesa specifike.

5. Promovimi i sigurisë

Edukimi dhe trajnimi për siguri

- 5.1 I personeli i AeMC-së ka përgjegjësi për sigurinë e aviacionit. Është e rëndësishme që i gjithë personeli të jetë kompetent për të ushtruar përgjegjësitë dhe detyrat e veta në kuadër të sigurisë. Kjo arrihet përmes trajnimit dhe vlerësimit të vazhdueshëm të personelit. Ky trajnim duhet të përfshijë SMS-në e AeMC-së, politikën e sigurisë, procedurat e raportimit, përgjegjësitë e sigurisë dhe mënyrën se si individët mund të kontribuojnë në të gjitha nivelet. Trajnimi i sigurisë duhet të përfshijë trajnimet periodike freskuese apo të ripërtëritjes së njohurive.
- 5.2 **Pikë kryesore** – Dosjet e trajnimit për të gjithë anëtarët e personelit duhet të ruhen.
- 5.3 **Pikë kryesore** – Promovimi efektiv i sigurisë duhet të rezultojë në inkurajimin aktiv të të gjithë personelit për identifikimin dhe raportimin e risqeve.
- 5.4 **Pikë kryesore** – Të gjithë anëtarët e personelit duhet të jenë të vetëdijshëm për risqet dhe rreziqet e sigurisë, të ndërlidhura me detyrat e tyre.
- 5.5 **Pikë kryesore** – Mësimet e nxjerra nga investigimet/hetimet duhet të shpërndahen në mënyrë efektive tek të gjithë anëtarët e personelit.

Komunikimi për sigurinë

- 5.6 Është e rëndësishme që të gjithë anëtarët e personelit të jenë plotësisht të vetëdijshëm për SMS-në dhe çfarëdo çështjesh që prekin sigurinë e AeMC-së tuaj. Informatat tjera përkatëse për sigurinë duhet të shpërndahen tek përdoruesit e shërbimeve tuaja dhe palët tjera me të cilat keni raporte kontraktuale.
- 5.7 Komunikimi efektiv siguron që të gjithë anëtarët e personelit të jenë plotësisht të vetëdijshëm për SMS-në, përfshirë informacionin me rëndësi kritike për sigurinë, të ndërlidhura me risqet e vlerësuara apo të analizura. Të gjithë anëtarët e personelit duhet ta kuptojnë se pse ndërmerren veprime të veçanta dhe pse procedurat e sigurisë paraqiten apo ndryshohen.
- 5.8 Takimet e rregullta të stafit ku diskutohen informatat, veprimet dhe procedurat mund të përdoren për qëllim të komunikimit në çështjet e sigurisë.
- 5.9 **Pikë kryesore** – Kjo mund të arrihet me lehtësi përmes takimeve, buletineve të sigurisë, fletë-informacioneve apo shpalljeve që vendosen në hapësirat e institucionit ose shpërndahen përmes postës elektronike dhe në faqen e internetit të AeMC-së. Duhet të bëhen përpjekje serioze për të shkëmbyer praktikat më të mira

lidhur me informacionet përkatëse që kanë të bëjnë me sigurinë me organizata të tjera të ngjashme.

6. Proceset specifike të një AeMC-je

Çfarë duhet të mbulojë SMS i juaj?

6.1 Deri në këtë pikë ky dokument ka trajtuar pjesët e një SMS-je që janë të përgjithshme për organizata jo-komplekse. Por, ekzistojnë aktivitete dhe procese që janë të veçanta për AeMC-në që gjithashtu duhet të përfshihen në SMS-në tuaj dhe të cilat janë:

- Certifikimi mjekësor në përputhje me Part-MED;
- Sigurimi i konfidencialitetit mjekësor;
- Hulumtimi mjekësor.

Certifikimi mjekësor në përputhje me Part-MED

6.2 Duhet të keni parasysh risqet dhe rreziqet që dalin nga proceset që përdoren në AeMC-në tuaj për vlerësimin dhe lëshimin e certifikatave mjekësore në përputhje me Part-MED.

6.3 Posaçërisht duhet ta keni në konsideratë:

- Mënyrën se si i menaxhoni rastet në përputhje me materialet udhëzuese që ju jipen nga autoriteti kompetent, me qëllim që të kuptoni më lehtë rregulloret zbatuese të EASA-s (Agjensia Evropiane e Sigurisë në Aviacion).
- Procesin e konsultimeve të brendshme apo mënyrën e referimit të një rasti drejt autoritetit kompetent ose të autoritetit të shtetit i cili e lëshon licencën/certifikatën të aplikuesit në fjalë.
- Mënyrën e verifikimit të certifikatave paraprake mjekësore dhe të dhënat e certifikatave të reja në mënyrë që ato të përmbajnë hollësi të sakta të aplikuesve, përfshirë edhe kufizimet përkatëse që ato mund të kenë.
- Mënyrën e vlerësimit të EKG-ve, në mënyrë që çfarëdo karakteristike me sinjifikancë klinike që ato mund të tregojnë, të mos interpretohen si normale, pa u marrë në shqyrtim dhe konsideratë të duhur.

6.4 Ka gjasë që ju veçse keni kryer auditime të rezultateve nga ekzaminimet mjekësore me qëllim të zbulimit të gabimeve dhe kjo mund të përfshihet në masat zbutëse për vlerësimin tuaj të rrezikut.

6.5 Shtojca 1 e ICAO-së rekomandon që të gjeturat të cilat dalin nga vlerësimet mjekësore të shqyrtohen me qëllim të identifikimit të fushave me rrezik të rritur për certifikim aeromjekësor dhe të paaftësisë mjekësore gjatë fazës së

fluturimit. Kjo mund të bëhet pjesë e SMS-së në bashkëpunim me autoritetin kompetent.

Garantimi i konfidencialitetit mjekësor

- 6.6 AeMC-së i kërkohet të krijojë një sistem të mbajtjes së të dhënave mjekësore, që lejon ruajtjen adekuate dhe gjurmueshmërinë e besueshme të të gjitha aktiviteteve në lidhje me to. Përveç kësaj, AeMC-ja duhet të krijojë një sistem të ruajtjes së dosjeve, me detajet e ekzaminimeve dhe vlerësimeve mjekësore, të kryera me qëllim të lëshimit, të vazhdimit apo të ripërtëritjes së certifikatave mjekësore, për një periudhë kohore prej së paku 10 vitesh, pas datës së ekzaminimit të fundit mjekësor.
- 6.7 Të gjitha të dhënat mjekësore duhet të mbahen në atë mënyrë që mbron ato nga dëmtimi, ndryshimi në përmbajtje ose vjedhja dhe siguron ruajtjen e konfidencialitetit mjekësor gjatë gjithë kohës të mbajtjes së tyre. Mbrojtja do të ndryshojë në varësi të faktit nëse të dhënat ruhen si kopje letre ose duke përdorur mediat elektronike. Në të dyja rastet, siguria nga qasja e paautorizuar do të sigurohet p.sh. duke kufizuar hyrjen në zonat ku ruhen dokumentet e letrës ose sigurinë e qëndrueshme me TI-së për të dhënat elektronike.

Hulumtimi mjekësor

- 6.8 Në rast kur hulumtimi në fushën e mjekësisë së aviacionit kryhet në ose nga ana e AeMC-së tuaj, atëherë SMS-ja duhet të përfshijë proceset për kryerjen e këtyre hulumtimeve, publikimin e rezultateve të tyre, duke marrë parasysh risqet dhe rreziqet e ndërlidhura me to, ashtu që hulumtimi të kryhet në mënyrë të sigurtë dhe në bazë të parimeve etike.

7. Zbatimi efektiv i një SMS-je

Analiza "GAP"

- 7.1 Ky dokument përshkruan elementet bazike që përbëjnë SMS-në për një AeMC. Shumica e organizatave tashmë mund të kenë disa nga këto komponente në fuqi. Gjithashtu nuk është e pritshme që SMS-ja e AeMC-së suaj të jetë plotësisht funksionale menjëherë; do të duhet kohë dhe përpjekje për të integruar këto komponente të SMS-së në AeMC-në tuaj, në mënyrë që ato të jenë plotësisht efektive.
- 7.2 Rekomandohet që ju të vlerësoni AeMC-në dhe të identifikoni elementet/komponentet që tashmë ekzistojnë dhe cilat komponentë duhet të zbatohen apo të fuqizohen. Një metodë e dobishme për të arritur këtë është analiza GAP. (Analiza GAP përfshin krahasimin e performancës aktuale me performancën e mundshme ose të dëshiruar). Për t'ju ndihmuar të vlerësoni secilën komponentë brenda AeMC-së tuaj, një grup pyetjesh vlerësimi për një AeMC është dhënë në Shtojcën F.

Plani Zbatues (Implementues)

- 7.3 Duke u nisur nga analiza "GAP" ju mund të zhvilloni një plan implementues për të zbatuar pjesët e mbetura të komponenteve relevant të SMS-së, brenda një periudhe kohore në mënyrë logjike dhe të strukturuar. Ndonëse plani juaj duhet të ketë një afat kohor të zbatimit, ju duhet të jeni realist pasiqë disa komponente janë më të vështira të zbatohen sesa të tjerat.
- 7.4 Mbani mend:
- Një SMS i maturuar do të merr kohë të zbatohet plotësisht;
 - Është e rëndësishme që të gjithë anëtarët e personelit të kenë mundësinë për të kontribuar në zhvillimin e SMS-së;
 - Nëse keni çfarëdo dyshimi kontaktoni autoritetin kompetent për këshilla apo
sygjerime;

Shtojca A

Shembull i politikës së sigurisë

Siguria ka konsideratë parësore në kuadër të organizatës [emri i organizatës tuaj].

Si Menaxher Përgjegjës është në përgjegjësi time për të garantuar siguri në kuadër të shërbimeve tona dhe operimeve të organizatës.

Unë garantoj që resurset përkatëse dhe trajnime të mjaftueshme do të ofrohen, me qëllim të menaxhimit efektiv të sigurisë.

Ne inkurajojmë të gjithë punonjësit dhe palët e interesuara që të raportojnë ngjarjet që ndërlidhen me sigurinë apo rreziqet potenciale, sado të parëndësishme që ato mund të vlerësohen në kohën e paraqitjes së tyre.

Kemi një kulturë të hapur të raportimit që inkurajon raportim të lirë dhe të sinqertë, nëpërmjet një kulture të drejtë të raportimit.

Ne përpiqemi të arrijmë:

- Një ambient pa aksidente;
- Një sistem efektiv të menaxhimit të sigurisë dhe përmirësimin e vazhdueshëm të tij;
- Përputhshmëri të plotë me të gjitha rregulloret kombëtare dhe ndërkombëtare që aplikohen për ne.

Këto objektiva janë për të mirën e organizatës, të punonjësve dhe të klientëve. Për këtë qëllim kemi përgjegjësi të përbashkët për të arritur këto qëllime.

Siguria është përgjegjësi e të gjithëve.

Nënshkruar nga Menaxheri Përgjegjës.

Nënshkrimi:

Shtojca B

SHEMBULL I REGJISTRIT (LOG-ut) TË RISKUT DHE VLERËSIMIT TË RREZIKUT

Datë:

Personi përgjegjës:

Nr. kontaktues:

Pjesëmarrësit:

Raportuar nga:

Nr. kontaktues:

Data e raportimit:

Data e shqyrtimit të hapave pasues:

Risku i identifikuar	Rreziku i shoqëruar/ pasojat	Masat ekzistuese zbutëse të rrezikut	Niveli aktual i rrezikut	Masat e mëtejme zbutëse	Rishikimi i nivelit të rrezikut	Veprimi i ndërmarrë, dhe kur ?
Ushtrim për elektrokardiografi duke përdorur trakë të vrapimit	Rrëshqitja, pengimi (marr në thua) dhe rrëzimi në trakë të vrapimit	Mbajtëset anësore në trakë të vrapimit ----- Të sigurohet që asnjë objekt të mos jetë i vendosur pas trakës së vrapimit ----- Mirëmbajtja dhe testimi vjetor i pajisjes	Ashpërsia 3 ----- Gjasat 3 ----- Rishikim i rregullt		Ashpërsia 3 ----- Gjasat 3 ----- Rishikim i rregullt	
	Provokim i aritmisë dhe ishemië kardiake gjatë testit	Proces i dokumentuar qartësi për ndërmarrjen e testeve për të cilat janë të familjarizuar anëtarët e personelit ----- Vlerësimi nga kardiologu para fillimit të testit	Ashpërsia 4 ----- Gjasat 3 ----- Rishikimi i rregullt	Të sigurohet që i gjithë stafi i AeMC-së të kryejë trajnim në reanimacion kardio-pulmonar dhe të mirëmbajë këtë kompetencë ----- Të kenë pajisjet e duhura për RKP përfshirë defibrilatorin e jashtëm ----- Të kryhen trajnime të simuluar dy herë në vit	Ashpërsia 3 ----- Gjasat 2 ----- Rishikim i rregullt	Menaxheri për siguri ----- korrik 2019

Shembull i identifikimit të riskut dhe procesi i vlerësimit të rrezikut në AeMC

Identifikimi i riskut

Instituti i Mjekësisë së Punës së Kosovës (IMPK) është një Qendër Aeromjekësore (AeMC) e cila kryen vlerësime shtesë të aplikantëve për certifikim mjekësor me anomali të EKG-së në qetësi dhe me sëmundje të dyshuar apo të vërtetuar koronare të zemrës. Risku i identifikuar në këtë rast është EKG duke përdorur trakën e vrapimit.

Rreziku përcjellës (i shoqëruar)

Këshilli i Sigurisë në kuadër të AeMC-së i përbërë na Drejtori i AeMC-së (Menaxheri Përgjegjës), një AME tjetër i cili është i punësuar poashtu në AeMC në cilësinë e Menaxherit të Sigurisë kanë vlerësuar një numër të risqeve të ndryshme brenda AeMC-së dhe në mesin e veprimeve të nevojshme për të adresuar këto është përcaktuar që duhet të ketë një vlerësim të duhur të rrezikut për EKG-të në ngarkesë (*Figura 1*). Komiteti i Sigurisë konstatoi se pasojat më të rëndësishme negative të ndërmarrjes së të elektrokardiografisë në ngarkesë janë rrëshqitjet dhe pengimet (marrja në thua) në trakë të vrapimit, që mund të provokojnë një aritmi të theksuar ose ishemi kardiake gjatë testimit.

Masat e zbutjes së rrezikut

Masat e zbutjes së rrezikut që zbatohen në këtë rast me qëllim parandalimi të rrëshqitjes dhe pengimet (marrja në thua) në trakë të vrapimit, përfshijnë mbajtëset anësore për duar ku i ekzaminuari mbahet përderisa ecë me intensitet të caktuar, dhe duke siguruar që nuk ka objekte të cilat gjenden pas trakës së vrapimit që do të mund të shkaktonin lëndime për të ekzaminuarin, në rast të rrëzimit prapa. Përveç kësaj, gjithashtu duhet të zbatohet mirëmbajtja vjetore e pajisjes nga ana e një pale kontraktuese të jashtme, me qëllim të zvogëlimin të rrezikut për ndalimin e papritur të trakës së vrapimit gjatë punës me të. Masat zbutëse të rrezikut të aplikuara, me qëllim të reduktimit të tij në raport me nxitjen e një aritmie apo ishemie kardiake gjatë testit përfshijnë një proces të dokumentuar të vlerësimit paraprak të rrezikut dhe të familjarizimit të personelit me pajisjen, procedurë kjo që mund të rishqyrtohet në bazë vjetore apo në çdo rast, nëse gjatë punës paraqitet ndonjë çështje me ndikim në sigurinë e testit. Para testit të gjithë të

ekzaminuarit vlerësohen nga kardiologu për të zvogëluar rrezikun e nxitjes së ndonjë efekti të padëshiruar gjatë zhvillimit të testimit.

Përcaktimi i nivelit aktual të rrezikut

Hapi i radhës është përcaktimi i nivelit të rrezikut që ndërlidhet me mundësinë e rrëzimit apo të një zhvillimi të padëshiruar kardial. Sa i ashpër do të jetë nëse ndodhë dhe cilat janë gjasat që ky zhvillim të ndodhë?

Ashpërsia (Shkalla e rrezikut)

Ashpërsia (shkalla e rrezikut) përcaktohet duke përdorur tabelën nr. 4 si më poshtë. Këshilli i Sigurisë ka vlerësuar se rrëshqitjet, pengimet (marrja në thua) dhe rrëzimet mund të rezultojnë me lëndime të rënda në kokë, të llogariten në ashpërsinë (shkallën e rrezikut) me vlerë 3. Nëse gjatë kryerjes së testit nxitet një ngjarje (efekt) e padëshiruar kardiale, e njëjta vlerësohet në ashpërsi (shkallë të rrezikut) me vlerë 4.

Figura 4. Klasifikimi i ashpërsisë (shkallës së rrezikut) sipas pasojave që mund të sjellë

Definicioni	Domethënia	Vlera
Katastrofik	Rezulton me aksident, vdekje apo dëmtim të pajisjes	5
I rrezikshëm	Lëndim i rëndë apo dëmtim madhor të pajisjes	4
Madhor	Incident serioz apo lëndim	3
Minor	Rezulton në incident minor	2
I papërfillshëm	Telashe me pasoja të vogla	1

Përcaktimi i gjasës (mundësisë së rrezikut)

Tabela në Figurën 5 përcakton mundësinë e rrëshqitjes, pengimit (marrja në thua), rrëzimit apo ndonjë ndodhie të veçuar kardiale gjatë ushtrimit të EKG-së në ngarkesë. Përcaktimi i gjasës (mundësisë së rrezikut) duhet të mbështetet në masat zbutëse ndaj rrezikut, të cilat janë aktualisht në fuqi dhe të efektivitetit të tyre në raport me rrezikun

e identifikuar. Me vlerësimin paraprak nga kardiologu dhe pastaj me monitorimin e vazhdueshëm përgjatë procesit të ekzaminimit, dhe shqyrtimit të literaturës së kësaj fushe është përcaktuar se gjasa (mundësia e rrezikut) e një ndodhie të veçuar kardiake do të ishte shumë e rrallë dhe e përcaktuar si “e pamundur”.

Është më e mundur që i ekzaminuari të pengohet (marrë në thua) apo të rrëzohet. Kjo rrallë ndodhë, prandaj rreziku i paraqitjes së kësaj ndodhie është vlerësuar të jetë “i vetmuar” (i izoluar).

Figura 5: Klasifikimi i gjasës (mundësisë së rrezikut) së ndodhies

Definicioni	Domethënia	Vlera
I shpeshtë	Gjasa (mundësia e rrezikut) është që të ndodhë shumë herë (ka ndodhur shpesh)	5
I kohëpaskohshëm	Me gjasë (mundësia e rrezikut) që të ndodhë ndonjëherë (ka ndodhur jo shpesh)	4
I vetmuar	Vështirë të ndodhë, por i mundshëm (ka ndodhur rrallë)	3
I pamundur	Shumë pak mundësi që të ndodhë (nuk dihet që ka ndodhur)	2
Skajshmërisht i pamundur	Pothuajse e pakonceptueshme që ngjarja do të ndodhë	1

Shënim: Definicionet e paraqitura në këtë tabelë janë vetëm shembull ilustrues. Mund të jetë më e dobishme për ju të përcaktoni definicionet cilësore, siç janë numri i ndodhjeve në një periudhë të caktuar kohore për numrin e aplikuesve/kandidatëve të vlerësuar/ekzaminuar.

Përcaktimi i tolerancës së rrezikut

Duke përdorur matricën e vlerësimit të rrezikut në Figurën 6, nëse rreziku përcaktohet si Katastrofik (5) dhe i Veçuar (3), atëherë rreziku do të klasifikohet në kategorinë e **Papranueshme**.

Figura 6: Matriksi i tolerancës së rrezikut

		Përmasa/ Shkalla e rrezikut				
Gjasa e rrezikut		Katastrofal 5	I Rrezikshëm 4	Madhor 3	Minor 2	I Parëndësishëm 1
I shpeshtë 5	E papranueshme	E papranueshme	E papranueshme	E papranueshme	E shqyrtueshme	E shqyrtueshme
I kohëpaskohshëm 4	E papranueshme	E papranueshme	E shqyrtueshme	E shqyrtueshme	E shqyrtueshme	E shqyrtueshme
I veçuar 3	E papranueshme	E shqyrtueshme	E shqyrtueshme	E shqyrtueshme	E shqyrtueshme	E pranueshme
Me pak gjasë që të ndodhë 2	E shqyrtueshme	E shqyrtueshme	E shqyrtueshme	E shqyrtueshme	E pranueshme	E pranueshme
Skajshmërisht pak gjasa që të ndodhë 1	E shqyrtueshme	E pranueshme	E pranueshme	E pranueshme	E pranueshme	E pranueshme

E papranueshme:	Shkalla e rrezikut është e papranueshme dhe masa të mëdha zbutëse kërkohen për të zvogëluar shkallën e rrezikut në nivelin më të ulët praktikisht të arsyeshëm.
E shqyrtueshme:	Niveli i rrezikut është shqetësues dhe masat zbutëse ndaj tij kërkohen me qëllim të reduktimit në nivelin më të ulët praktikisht të arsyeshëm (ALARP). Në rastet kur reduktimi/zbutja e mëtejme e rrezikut nuk është praktike apo e zbatueshme, rreziku mund të pranohet, me kusht që ky rrezik është kuptuar drejt dhe ka miratimin e Menaxherit Përgjegjës.
E pranueshme:	Rreziku konsiderohet me shkallë të pranueshme, por duhet të shqyrtohet nëse vazhdon të rishfaqet.

Masat të tjera për zbutjen e rrezikut

Shqyrtimi i mëtejshëm i rrezikut, përcakton që Menaxheri i Sigurisë duhet të sigurojë që i gjithë personeli të jetë i aftë të menaxhojë një ndodhi të padëshiruar kardiake nëse

shfaqet dhe se kjo mund të përmirësohet duke siguruar që personeli të jetë i trajnuar në reanimimin kardiopulmonar (RKP) dhe trajnimeve të vazhdueshme për rifreskimin e njohurive dhe aftësive të tyre. Pajisjet e përshtatshme për të menaxhuar këto ndodhi duhet të vendosen në hapësirë për qasje të lehtë nga traka e vrapimit, dhe të vlerësohen në baza periodike përmes ushtrimeve të paparalajmëruara, me qëllim të menaxhimit sa më të mirë të kësaj ndodhie.

Rishikimi i nivelit të rrezikut

Këshilli i Sigurisë konstaton se masat e ndërmarra kanë reduktuar shkallën/ashpërsinë e ndonjë lëndimi që do të mund të ndodhte gjatë ushtrimit të EKG-së në ngarkesë, megjithëse mbajti nivelin e tolerancës së gjithmbarshme të rrezikut në nivelin e “Shqyrtueshëm”.

Shtojca C

SHEMBULL I FAQES TË PËRMBAJTJES SË MANUALIT TË SMS-së

1. Tabela e përmbajtjes
2. Lista e faqeve efektive
3. Lista e shpërndarjes
4. **Politika e sigurisë dhe objektivat** - *(duhet të përfshijë edhe politikën e sigurisë të nënshkruar nga Menaxheri Përgjegjës)*
5. **Organizimi i sigurisë** - *(duhet të përshkruaj strukturën menaxheriale të AeMC-së)*
 - a) **Fushëveprimi i SMS-it dhe aktivitetet e kontraktuara** - *duhet të përshkruaj atë që SMS mbulon dhe si ndërlidhet me palët e tjera të lidhura me sigurinë.*
 - b) **Përgjegjshmëria e sigurisë dhe përgjegjësitë** - *duhet të përshkruaj anëtarët kyç të personelit të sigurisë, anëtarët e komisionit për siguri dhe përgjegjshmërinë e sigurisë dhe përgjegjësitë e të gjithë anëtarëve kyç të personelit.*
 - c) **Dokumentimi i SMS-it** - *duhet të përshkruaj mënyrën se si dokumentohet dhe regjistrohet SMS.*
6. **Identifikimi riskut dhe procesi i menaxhimit të rrezikut** - *duhet të përfshijë raportimin e sigurisë dhe procesin e identifikimit të riskut dhe vlerësimin e rrezikut dhe menaxhimin dhe kontrollimin e tij.*
7. **Garantimi i sigurisë** - *duhet të përfshijë mënyrën se si SMS dhe rezultatet e tij janë të audituara, si dhe duhet të përfshijë gjithashtu edhe monitorimin e performancës së sigurisë dhe procesin e matjes.*
8. **Menaxhimi i ndryshimeve** - *duhet të përshkruaj se si AeMC-ja përdor sistemin e SMS-së për të menaxhuar ndryshimet.*
9. **Plani i reagimit emergjent** - *duhet të përshkruaj se si AeMC-ja do të veproj në një situatë emergjente dhe të sigurojë një udhëzues të shpejtë për anëtarët kyç të personelit.*

Shtojca D

SHEMBULL I FORMULARIT TË RAPORTIMIT TË SIGURISË

Pjesa A: Të plotësohet nga personi i cili identifikon ngjarjen ose riskun

Data e ngjarjes: _____ Koha: _____

Lokacioni: _____

Emri i raportuesit: _____

Sektori/Organizata: _____

Ju lutem përshkruani ne tërësi ngjarjen ose riskun e identifikuar:

I përfshini edhe rekomandimet e juaja si të parandaloni ndodhitë e njëjta

Sipas mendimit tuaj, cila është mundësia e një ngjarjeje të tillë apo të ngjashme të ndodh përsëri?

Jashtëzakonisht e pamundur

E shpeshtë

1

2

3

4

5

Çfarë konsideroni mund të jetë pasoja më e keqe e mundshme nëse kjo ngjarje ndodhë përsëri

E parëndësishme

Katastrofike

1

2

3

4

5

Pjesa B: Të plotësohet nga Zyrtari / Menaxheri i Sigurisë

Ky raport është de-identifikuar dhe është futur në bazën e të dhënave të kompanisë.

Referenca e raportit: _____

Emri dhe mbiemri: _____ Datë: _____

Nënshkrimi: _____

Pjesa C: Të plotësohet nga Këshilli i Sigurisë

Vlerësoni gjasat e përsëritjes së ndodhisë ose ri-përsëritjes:

Jashtëzakonisht e pamundur					E shpeshtë
1	2	3	4	5	

Vlerësoni pasojat më të këqija:

E parëndësishme					Katastrofike
1	2	3	4	5	

Cilat veprime janë të nevojshme për të ELIMINUAR, ZVOGËLUAR (ZBUTUR) ose KONTROLLUAR riskun në një nivel të pranueshëm të sigurisë?

Burimet e kërkuara: _____

Përgjegjësia për veprim: _____

Pajtuar dhe pranuar nga:	Zyrtari/Menaxheri i Sigurisë	Datë: _____
	Menaxheri Kryesor	Datë: _____
	Menaxheri Përgjegjës	Datë: _____

Informatat e përshtatshme dhënë stafit nga Zyrtari i Sigurisë / Menaxheri i Sigurisë

Nënshkruar: _____ Datë: _____

Veprimet e kërkuara: Kur: _____
Kush: _____

Regjistri i riskut i përditësuar: Kur: _____

Shtojca E

SHEMBULL I OBJEKTIVAVE TË SIGURISË SË AeMC-së DHE TREGUESIT E PERFORMANSËS SË SIGURISË

TREGUESIT E PERFORMANSËS	OBJEKTIVI	PERFORMANSA											
		1	2	3	4	5	6	7	8	9	10	11	12
		TM 1			TM 2			TM 3			TM 4		
Numri i incidenteve klinike të rrezikut të madh	1 apo më pak												
Numri i rasteve të certifikatave mjekësore lëshuar me gabime	1												
Numri i EKG-ve të keqkuptuara si të pranueshme	2 apo më pak												
Numri i auditimeve të brendshme	4												
Numri i gjetjeve të auditimit	2 apo më pak												
Numri i mbledhjeve të Komitetit të sigurisë	6												
Pjesëmarrja e personelit kyç në komitetin e sigurisë	Minimumi												
Numri i raporteve të rrezikut / sigurisë	20 apo më tepër												
Numri i fletushkave të lëshuara për siguri	2												
Numri i vlerësimeve formale të rrezikut	5 apo më tepër												
Numri i sondazheve të sigurisë	1												
Numri i raporteve të detyrueshme siç kërkohet me Ligj komb.	1 apo më pak												

SHËNIM: Objektivat e sugjeruara janë vetëm shembull. Organizatat duhet të përcaktojnë qëllimet të cilat janë relevante për llojin e tyre specifik të operimeve.

Shtojca F

PYETJE VLERËSUESE PËR TË MBËSHTETUR ANALIZËN “GAP”

Të plotësohet dhe nënshkruhet nga Menaxheri i Sigurisë apo Menaxheri Përgjegjës

Organizata:

Numri referent:

Nënshkrimi:

Pozita:

Emri dhe mbiemri:

Datë:

Revidimi i manualit të SMS-së:

		Në përputhje Po / Jo Pjesërisht	Komentet Referenca në përputhshmëri
PËRKUSHTIMI I MENAXHMENTIT DHE PËRGJEGJSHMËRIA	A ekziston një politikë e shkruar e sigurisë e miratuar nga Menaxheri Përgjegjës?		
	A promovohet dhe demonstron në mënyrë të vazhdueshme përkushtimi për politikën e sigurisë nga menaxhmenti drejtues?		
	A është komunikuar në mënyrë efektive politika e sigurisë në të gjitha nivelet e AeMC-së?		
	A përfshihen pikat e këtij materiali udhëzues në politikën e sigurisë?		
PËRGJEGJËSITË PËR SIGURI	A janë definuar qartë përgjegjësitë dhe llogaridhënia e Menaxherit Përgjegjës dhe pjesëtarëve tjerë kyç të personelit dhe a janë të publikuara që të shihen nga personeli dhe kontraktorët e organizatës?		
	A ka Menaxheri Përgjegjës përgjegjësi të plotë për SMS-në dhe autoritet për të vendosur për buxhetin e organizatës?		
	A është e definuar struktura menaxheriale e AeMC-së?		
	A janë të vetëdijshëm të gjithë anëtarët e personelit për detyrat dhe përgjegjësitë e tyre të sigurisë?		
EMËRIMI I ANËTARËVE KYÇ TË SIGURISË	A është emëruar një pikë kontakti / Menaxher i Sigurisë për SMS-në?		
	A ekziston një linjë e drejtpërdrejtë e raportimit ndërmjet pikës të kontaktit për SMS, Menaxherit të Sigurisë dhe Menaxherit Përgjegjës?		
	A ka njohuri të përshtatshme dhe të duhur për SMS pika e kontaktit për SMS / Menaxheri i Sigurisë?		
	A ka AeMC-ja një Komitet të Sigurisë apo një organ ekuivalent?		
	A monitoron Komiteti i Sigurisë apo organi ekuivalent performancën e sigurisë dhe efikasitetin e SMS-së?		
	A mbledhet Komiteti i Sigurisë apo organi ekuivalent të paktën një herë në vit dhe a mbahen procesverbalet e takimeve?		

PLANIFIKIMI I REAGIMIT EMERGJENT	A është zhvilluar një plan reagimi ndaj emergjencave (PRE) dhe është i azhurnuar?		
	A janë rolet, përgjegjësitë dhe veprimet e anëtarëve kyç të personelit të definuara në PRE?		
	A janë përfshirë në PRE të gjitha elementet e këtij materiali udhëzues, nëse aplikohen?		
	A është rishikuar dhe testuar rregullisht PRE?		
DOKUMENTACIONI I SIGURISË	A përmban manuali i menaxhimit të sigurisë ose dokumentacioni i sigurisë, të gjitha elementet e detajuara në këtë material udhëzues?		
	A rishikohet rregullisht?		
	A ekziston një sistem për regjistrimin dhe ruajtjen e dokumentacionit dhe dosjeve të SMS-së, si p.sh. regjistrat e riskut, vlerësimet e rrezikut, raportet e sigurisë, të rasteve të raportuara të sigurisë nga ana e stafit / kontraktuesve?		
IDENTIFIKIMI I RISKUT	A ekziston një sistem konfidencial i raportimit të sigurisë?		
	A i janë deleguar një "pronari" raportet e sigurisë dhe a janë shqyrtuar nga Komiteti i Sigurisë apo organi ekuivalent?		
	A ka informatë kthyesë për raportuesin e ndodhisë?		
	A ka një procedurë të shkruar e cila përshkruan mënyrën e identifikimit të risqeve?		
	A janë identifikuar risqet kryesore të ndërlidhura me AeMC?		
VLERËSIMI DHE ZBUTJA E RREZIKUT	A ekziston një proces i vlerësimit të rrezikut?		
	A është matrica e tolerancës së rrezikut e përshtatshme dhe a mund të aplikohet vazhdimisht?		
	A ka ndonjë proces për të vendosur masa zbutëse të rrezikut?		
	A janë verifikuar / audituar masat për zbutjen dhe kontrollin e rrezikut për të konfirmuar efektshmërinë e zbatimit të tyre?		

	A janë të menaxhuara rreziqet në një nivel të arsyeshëm?		
	A janë risqet dhe rreziqet e regjistruara, në librin e regjistrit përkatës?		
MONITORIMI I PERFORMANSËS SË SIGURISË	A janë përcaktuar treguesit e performansës së sigurisë?		
	A janë rishikuar rregullisht treguesit e performansës së sigurisë, për të identifikuar ndonjë trend?		
MENAXHIMI I NDRYSHIMIT	A ka një proces për të identifikuar risqet në mënyrë proaktive dhe për të zbutur rreziqet kur ndodhin ndryshime të rëndësishme në AeMC?		
MENAXHIMI I INCIDENTEVE	A janë kryer hetimet e sigurisë pas incidenteve apo aksidenteve për të përcaktuar shkakun rrënjësor të paraqitjes së tyre?		
	A janë adresuar dhe komunikuar me pjesën tjetër të AeMC-së, risqet e identifikuara nga hetimet e sigurisë?		
FUSHAT SPECIFIKE TË AeMC-së	A janë zbatuar elementet e SMS, të përshkruara në Kapitujt 6 dhe 7 në atë mënyrë që të sigurohet që certifikimi mjekësor është kryer në përputhje me Part-MED?		
	A janë zbatuar elementet e SMS të përshkruara në Kapitujt 6 dhe 7 në proceset e juja për të garantuar konfidencialitetin mjekësor?		
	A janë zbatuar elementet e SMS të përshkruara në Kapitujt 6 dhe 7 në proceset për hulumtime mjekësore?		
PËRMIRËSIMI I VAZHUESHËM	A është arritur përmirësimi i vazhdueshëm në performancën e sigurisë?		
AUDITIME TË SIGURISË	A janë kryer auditime dhe anketime të sigurisë?		
	A ekziston një sistem i pavarur i cilësisë apo agjenci e palës së tretë që kontrollon SMS-në?		

TRAJNIME TË SIGURISË	A është personeli i trajnuar në mënyrë adekuate lidhur me SMS si dhe rolet dhe përgjegjësitë e tyre në siguri?		
KOMUNIKIMI	A komunikohen informatat lidhur me sigurinë tek i gjithë personeli sipas nevojës?		
	A arrin informacioni përkatës i sigurisë tek shfrytëzuesit / klientët e jashtëm?		
ZBATIMI I SMS-së	A është kryer një analizë "GAP"?		
	A ekziston një plan për zbatimin e SMS-së?		
	A pasqyron plani i zbatimit analizën "GAP"?		
	A është plani i zbatimit i orientuar drejt një objektivi?		