

MEMORANDUM OF UNDERSTANDING

BETWEEN

NATIONAL AUTHORITY ON ELECTRONIC CERTIFICATION AND

CYBER SECURITY OF ALBANIA

AND

CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES

This Memorandum of Understanding (hereinafter referred to as “MoU”) is made between the following Parties:

- (a) Albanian National Authority on Electronic Certification and Cyber Security (hereinafter referred to as “NAECCS”); and
- (b) United Arab Emirates Cyber Security Council (hereinafter referred to as “CSC”);

Recognizing that Information and Communication Technologies (ICTs) have opened up new windows of opportunity and are essential tools for socio-economic development of States;

Recognizing that ICTs have also introduced new types of threats such as inter alia cyber-crime, cyber-espionage, hacktivism, cyber-terrorism, cyber-warfare, critical infrastructure attacks, disinformation campaigns; and that these threats are on rise globally, transnational, dynamic and are proving increasingly sophisticated;

Convinced of the need to join efforts and capabilities in order to develop and disseminate new technologies that promote the establishment of a secure global information society;

Both Participants have similar strategic interests and agree to cooperate in the field of information based on equal and mutual benefit, to improve cooperation in response to information security incidents.

Recognizing that public institutions have a role to play for managing cybersecurity risks and for protecting the digital environment; and that co-operation is essential at domestic, regional, and international levels.

Recognizing that the proper functioning and security of the digital environment, including the Internet, is essential to the functioning of our economies and societies and stimulates innovation.

Recognizing the role of the Parties in the field of cybersecurity in implementation of policy measures and operational responses, development of tools, and in the regulatory framework.

Both Participants intend to detail the main goals, objectives, areas, and forms of cooperation, concluded in this the MoU on the following:

Article 1

BASIC PRINCIPLES OF COOPERATION

The purposes of this MoU are:

1. to promote cooperation in the field of cybersecurity between the Parties;
2. to enhance exchange of information between both Parties pertaining to cybersecurity based on specifications in article 4 of this MoU
3. to support and cooperate on reaching the strategic goals in the field of Cyber Security.

Article 2

STATUS AND SCOPE OF THIS MOU

1. This MoU sets out the framework within which the Parties intend to work together to achieve the purposes set out in Article 1.
2. This MoU is not intended to create, maintain or govern any legally binding obligations, rights or benefits between the Parties or between the Parties and any third party. Each Party's implementation of this MoU is subject to that Party's domestic laws, regulations, policies and international obligations.
3. The Parties acknowledge that this MoU does not prejudice any existing or future arrangement, treaty, or other arrangement between the Parties.

Article 3

AREAS OF COOPERATION

To achieve the above purpose of this MoU, the Participants intend to cooperate in the following areas:

- A. Information exchange on information security risks.
- B. Joint information and response to information security incidents.
- C. Sharing information about the spread of malware.
- D. Exchange of indicators of compromise.
- E. Exchange of experience in countering information security threats.
- F. Providing information on promising solutions in the field of information security.
- G. Exchange of educational and training material related to cyber security.
- H. Mutual collaboration in organizing technical workshops, conferences, educational visits, and trainings.
- I. Mutual coordination and collaboration in organizing and implementing cybersecurity training across all sectors.
- J. Sending missions of experts and joint working groups in the field of cybersecurity.
- K. Exchange of cyber security awareness materials.

- L. Provision of advisory information assistance in the investigation and elimination of information security incidents.
- M. Attendance of representatives from each Participant for any training courses and working sessions organized by the other Participant.

Article 4

EXCHANGE AND USE OF INFORMATION

1. Both Parties may exchange information for the purposes of this MoU. The disclosure of information pursuant to this MoU will be in accordance with applicable domestic law, policies and mechanisms.
2. Neither Party will disclose information obtained from the other Party pursuant to or in connection with this MoU to any third party without prior consent of the other Party.
3. The Parties will respect any condition, restrictions or caveat indicated by the other Party in respect of the handling or disclosure of information, except for situations where disclosing such information is mandatory by law or requested by a court of law.
4. The Parties will apply data protection, according to the respective applicable national and international legal frameworks.
5. The Parties will appoint a contact person responsible for the communications between the Parties in the framework of this agreement.
6. Any joint activity involving intellectual property will be agreed upon in writing by the Parties to protect relevant interests.

Article 5

DISPUTE RESOLUTION

Any differences/disputes between the Parties concerning the interpretation and/or implementation of this MoU shall be settled amicably through consultations and/or negotiations between the Parties.

Article 6
COMMENCEMENT, DURATION AND TERMINATION

1. This MoU will come into effect on the date the MoU is signed by both Parties.
2. This MoU is intended to remain in effect for an initial period of three (3) years and automatically extended for a subsequent three (3) year period, unless the Party gives to other Party three (3) months written notice of its intention not to extend the MoU. The Parties may terminate it at any time by notifying the other Party in writing. Such termination will take effect ninety (90) calendar days from the date of the notification unless the Parties mutually consent in writing to a shorter period of time.
3. Ongoing activities at the time of termination will nonetheless be completed in accordance with the provisions of this MoU.
4. This MoU may be modified by mutual written agreement of the Parties.
5. A modification to this MoU will come into effect on the date mutually determined by both Parties.

Article 7
COST, EXPENSES AND RESOURCE

This MoU is not an obligation, and also does not entail any financial obligations for both Participants and does not give rise to legal rights and responsibilities between the Participants. Each Participant tolerates its own personal expenses and provides itself with resources for the execution of this MoU and other related expenses. All activities under this MoU will be subject to the availability of financial and human resources in accordance with the national law of the Participants.

Article 8
LANGUAGES

All communication between Parties will be in English. This MoU was compiled in three original languages: English, Arabic and Albanian. In the event of any discrepancy, the English language shall prevail.

This MoU has been signed in 06.04.... on 2023.....

Article 9

CONTACT INFORMATION

NATIONAL AUTHORITY ON
ELECTRONIC CERTIFICATION
AND CYBER SECURITY OF
ALBANIA

Name: Rexhion Qafa
Designation: NAECCS
telephone: +355697035660
Email address:
rexhion.qafa@cesk.gov.al
Call center 24/7: +355 4 22 210 39
Emergency telephone:
+355692088722
Address: Tirana - Albania

CYBER SECURITY COUNCIL OF
THE UAE

Name: Wafi Yousef Ali Fadil Binfadil
Designation: Cyber Security Council
Office telephone: +971 50 287 8888
Email address: grc@csc.ae /
ciso@csc.ae
Call center 24/7: +971 50 7231 222
Emergency telephone: +971 50
2878888
Address: Dubai - UAE

Article 10

SIGNATURES

The MOU is signed by the following representatives of the Parties:

SIGNED for and on behalf of National
Authority on Electronic Certification
and Cyber Security of Albania

General Director
Mr.Assoc.Prof. Igli TAFA

Signature

SIGNED for and on behalf of United
Arab Emirates Cyber Security Council

**Ambassador of the United Arab
Emirates to the Hellenic Republic**
H.E. Sulaiman Humad Salem

ALMazroui

Signature



**MEMORANDUM MIRËKUPTIMI
MIDIS**

**AUTORITETIT KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE
SIGURINË KIBERNETIKE NË SHQIPËRI**

DHE

**KËSHILLIT TË SIGURISË KIBERNETIKE TË EMIRATEVE TË
BASHKUARA ARABE**

Ky Memorandum Mirëkuptimi (në vijim “MM”) është dakordësuar ndërmjet palëve të mëposhtme:

- a) Autoriteti Kombëtar Shqiptar për Certifikimin Elektronik dhe Sigurinë Kibernetike (në vijim “AKCESK”); dhe
- b) Këshillit të Sigurisë Kibernetike të Emirateve të Bashkuara Arabe (më tej referuar si “CSC”);

Duke pranuar se Teknologjite e Informacionit dhe të Komunikimit (TIK) kanë hapur dritare të reja mundësish dhe janë mjete thelbësore për zhvillimin socio-ekonomik të shteteve;

Duke pranuar se TIK kanë sjellë gjithashtu lloje të reja kërcënimesh si: krimi kibernetik, spiunazhi kibernetik, haktivizmi, terrorizmi kibernetik, lufta kibernetike, sulmet ndaj infrastrukturës kritike, fushatat e dezinformimit; dhe se këto kërcënimë janë në rritje globalisht, ndërkontrollor, ndërkombëtarisht, në mënyrë dinamike dhe po shfaqen gjithnjë e më të sofistikuara;

Të bindur për nevojën për të bashkuar përpjekjet dhe aftësitë me qëllim zhvillimin dhe përhapjen e teknologjive të reja që promovojnë krijimin e një shoqërie globale të informacionit të sigurt;

Palët kanë interesa strategjike të përbashkëta dhe bien dakord të bashkëpunojnë në fushën e informacionit bazuar në përfitime të njëjtë dhe reciproke, për të përmirësuar bashkëpunimin në përgjigje të incidenteve të sigurisë së informacionit.

Duke pranuar se institucionet publike kanë një rol te rëndësishëm për menaxhimin e rreziqeve të sigurisë kibernetike dhe për mbrojtjen e mjedisit digital; dhe se bashkëpunimi është thelbësor në nivelet e brendshme, rajonale dhe ndërkontinentale.

Duke pranuar se funksionimi i duhur dhe siguria e mjedisit digital, duke përfshirë internetin, është thelbësor për funksionimin e ekonomive dhe shoqërive tona dhe stimulon inovacionin.

Duke pranuar rolin e Palëve në fushën e sigurisë kibernetike, në zbatimin e politikave dhe reagimeve operacionale, zhvillimin e mjeteve dhe në kuadrin rregullator.

Palët synojnë të përcaktojnë qëllimet kryesore, objektivat, fushat dhe format e bashkëpunimit, të përfshira në këtë MM për sa vijon:

Neni 1

PARIMET THEMELORE TË BASHKËPUNIMIT

Parimet mbi të cilat bazohet ky MM janë:

1. të promovojë bashkëpunimin në fushën e sigurisë kibernetike ndërmjet Palëve;
2. të përmirësojë shkëmbimin e informacionit ndërmjet palëve në lidhje me sigurinë kibernetike bazuar në specifikimet sipas Nenit 4 të këtij MM

3. të mbështesë dhe bashkëpunojë në arritjen e synimeve strategjike në fushën e Sigurisë Kibernetike.

Neni 2

STATUSI DHE FUSHA E KËTIJ MM

1. Ky MM përcakton kornizën brenda të cilës Palët synojnë të bashkëpunojnë për të arritur qëllimet e përcaktuara në nenin 1.
2. Ky MM nuk ka për qëllim të krijojë, mbajë ose imponojë të drejta dhe detyrime ligjore ndaj Palëve ose ndërmjet Palëve të treta. Zbatimi i këtij MM nga Palët e përcaktuara në të, i nënshtrohet ligjeve, rregulloreve, politikave kombëtare dhe detyrimeve të tyre ndërkomëtare.
3. Palët pranojnë se ky MM nuk paragjykon asnjë marrëveshje, traktat tjeter ekzistuese apo që krijojen në të ardhmen ndërmjet Palëve.

Neni 3

FUSHAT E BASHKËPUNIMIT

Për të arritur qëllimin e mësipërm të këtij MM, pjesëmarrësit synojnë të bashkëpunojnë në fushat e mëposhtme:

- A. Shkëmbimi i informacionit mbi rreziqet e sigurisë së informacionit.
- B. Informacion i përbashkët i shkëmbyer dhe reagim ndaj incidenteve të sigurisë së informacionit.
- C. Ndarja e informacionit në lidhje me përhapjen e programeve keqdashëse.
- D. Shkëmbimi i indikatorëve të kompromisit.
- E. Shkëmbimi i përvjoes në luftën kundër kërcënimeve të sigurisë së informacionit.
- F. Dhënia e informacionit për zgjidhjet e mundshme në fushën e sigurisë së informacionit.
- G. Shkëmbimi i materialeve edukative dhe trajnuese lidhur me sigurinë kibernetike.
- H. Bashkëpunimi i ndërsjellë në organizimin e seminareve teknike, konferencave, vizitave edukative dhe trajnimeve.

- I. Koordinim dhe bashkëpunim i ndërsjellët në organizimin dhe realizimin e trajnimeve për sigurinë kibernetike në të gjithë sektorët.
- J. Dërgimi i misioneve të ekspertëve dhe grupeve të përbashkëta të punës në fushën e sigurisë kibernetike.
- K. Shkëmbimi i materialeve ndërgjegjësuese për sigurinë kibernetike.
- L. Ofrimi i asistencës informative këshilluese në hetimin dhe eliminimin e incidenteve të sigurisë së informacionit.
- M. Ndjekja nga përfaqësuesit të secilës Palë, të çdo kursi trajnimi dhe sesioni pune të organizuar nga Palët.

Neni 4

SHKËMBIMI DHE PËRDORIMI I INFORMACIONIT

1. Palët marrin përsipër të shkëmbejnë informacionin për qëllimet e këtij MM. Shkëmbimi i informacionit sipas kushteve të këtij MM, do të kryhet në përputhje me legjispcionin vendas, politikat dhe mekanizmat në fuqi të palëve.
2. Asnjëra palë nuk do të shpërndajë informacionet e marra nga Pala tjetër sipas përcaktiveve të këtij MM, asnjë pale të tretë pa pëlqimin paraprak të Palës tjetër.
3. Palët do të respektojnë çdo kusht, kufizim ose paralajmërim të vendosur nga Pala tjetër në lidhje me trajtimin ose shpëndarjen e informacionit, me përjashtim të situatave kur zbulimi i një informacioni të tillë është i detyrueshëm sipas kuadrit ligjorë vendas.
4. Palët do të zbatojnë mbrojtjen e të dhënave personale, sipas kuadrit ligjor përkatës kombëtar dhe ndërkombëtar.
5. Palët do të caktojnë një person kontakti përgjegjës për komunikimet ndërmjet Palëve në kuadrin e kësaj marrëveshjeje.
6. Çdo aktivitet i përbashkët që përfshin pronësinë intelektuale do të dakordësohet me shkrim nga Palët për të mbrojtur interesat përkatëse.

Neni 5

ZGJIDHJEN E MOSMARRËVESHJES

Çdo dallim/mosmarrëveshje ndërmjet Palëve në lidhje me interpretimin dhe/ose zbatimin e këtij MM do të zgjidhet në mënyrë miqësore nëpërmjet konsultimeve dhe/ose negociatave ndërmjet palëve.

Neni 6

FILLIMI, KOHËZGJATJA DHE PËRFUNDIMI I MM

1. Ky MM hyn në fuqi në datën e nënshkrimit të tij nga të dyja Palët.
2. Ky MM ka për qëllim që pas periudhës së vlefshmërisë fillestare prej tre (3) vjetësh, të zgjatet automatikisht për një periudhë të mëvonshme tre (3) vjeçare, përveçse kur Palët njoftojnë njëra tjetrën me shkrim tre (3) muaj përparrë përmungesën e dëshirës përzgjatjen e MM. Palët mund ta ndërpresin atë në çdo kohë duke e njoftuar Palën tjetër me shkrim. Përfundimi i MM do të hyjë në fuqi nëntëdhjetë (90) ditë kalendarike nga data e njoftimit të tij, përveç rastit kur Palët bien dakord reciprokisht me shkrim për një periudhë më të shkurtër kohore.
3. Aktivitetet që janë në proces në momentin e përfundimit të MM, do të përfundojnë në përputhje me dispozitat e këtij MM.
4. Ky MM mund të modifikohet me marrëveshje reciproke me shkrim të Palëve.
5. Një modifikim i këtij MM do të hyjë në fuqi në datën e përcaktuar reciprokisht nga Palët.

Neni 7

KOSTOT, SHPENZIMET DHE BURIMET

Ky MM nuk është një detyrim, dhe gjithashtu nuk sjell ndonjë detyrim finansiar për të dy palët dhe nuk krijon të drejta dhe përgjegjësi ligjore ndërmjet tyre. Çdo Palë merr përsipër shpenzimet e veta personale dhe i siguron vetes burime përekzekutimin e këtij MM dhe shpenzimeve të tjera të lidhura me të. Të gjitha aktivitetet sipas këtij MM, do t'i nënshtrohen disponueshmërisë së burimeve financiare dhe njerëzore në përputhje me legjislacionin kombëtar të Palëve.

Neni 8

GJUHËT

I gjithë komunikimi ndërmjet Palëve do të jetë në gjuhën angleze. Ky MM është hartuar në 3 (tre) gjuhë origjinale: Anglisht, Arabisht, Shqip. Në rast mosmarrëveshjeje, prevalon gjuha angleze.

Ky MM është nënshkruar më 26. 04. 2023.

Neni 9

INFORMACIONET E KONTAKTIT

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE I SHQIPËRISË	KËSHILLI I SIGURISË KIBERNETIKE I EMIRATEVE TË BASHKUARA ARABE
Emër: Rexhion Qafa	Emër: Wafi Yousef Ali Fadil Binfadil
Institucioni: AKCESK	Institucioni: Këshilli i Sigurisë Kibernetike
Telefon: +355697035660	Telefon: +971 50 287 8888
Adresë email : Rexhion.qafa@cesk.gov.al	Adresë email: grc@csc.ae / ciso@csc.ae
Telefon 24/7: +355 4 22 210 39	Telefon 24/7: +971 50 7231 222
Telefon emergjencash: +355 69 20 88 722	Telefon emergjencash: +971 50 2878888
Adresa: Tirane, Shqipëri.	Adresa: Dubai, Emiratet e Bashkuara Arabe

Neni 10

NËNSHKRIMI

Marrëveshja e Mirëkuptimit nënshkruhet nga përfaqësuesit e mëposhtëm të palëve:

NËNSHKRUAR për dhe në emër të
Autoritetit Kombëtar për Certifikimin
Elektronik dhe Sigurinë Kibernetike të
Shqipërisë

Drejtor i Përgjithshëm
Z. Ass.Prof. Igli TAFA

NËNSHKRUAR për dhe në emër të
Këshillit të Sigurisë Kibernetike të
Emirateve të Bashkuara Arabe

Ambasador i Emirateve të Bashkuara
Arabe në Republikën Helenike
Sh.T.Z Sulaiman Humad Salem
ALMazroui

Igli Tafa _____ ALMazroui
Nënshkrimi Nënshkrimi



અંગરી | ગુજરાતી | કૃતી | એણ્ઝે | એણ્ઝી | માર્ગની | જીવિતી

૬

શિપ્રા

અંગરી | માર્ગની | જીવિતી | એણ્ઝે | એણ્ઝી | કૃતી | ગુજરાતી

કેદી

અંગરી | માર્ગની | જીવિતી |

የኢትዮጵያ የሰውን ተቋማዊ ስራውን እና ተቋማዊ ስራውን

የዕድገት በዚህ የሚከተሉት ስልክ እንደሚታረም ነው፡፡

ዕና ተግባር የትምህር ስራውን አገልግሎት ተስፋል ነው ይህንን የሚከተሉት ደንብ እንደሚታረም ይመለከታል;

የኢትዮጵያውያንድ የሚከተሉት ቀን ነው፡፡

የንግድ የሚገኘውን ስም በመስቀል እንደሆነ ተከተሉ ይገባል እና የሚከተሉት ስም ተከተሉ ይገባል

۱۷۰

የመንግሥት የዕለታዊ ስምምነት እና ተቋማዊ ስምምነት የሚያስፈልግ ይችላል

(ጥ) በዚህን የሆኑን ስምምነት ተብሎ እንደገኘ ይችላል፡፡

የኢትዮ-ፖ.ሪ.ዳ. (ፖ.ሪ.ዳ. የኢትዮ-ፖ.ሪ.ዳ. አዲስ አበባ) በተመለከተ ስ.፩.፪.፭.፻፲፭

(၁၃) မြန်မာ လူများ ပေါ်လုပ်မှု ရွှေ့ချေမှု ပိုမို တော်ကြော် ပေါ်လုပ်မှု ပိုမို တော်ကြော်

(၁) ပုဂ္ဂန်မြို့၏ အကျဉ်းချုပ်မှု ပုဂ္ဂန်မြို့၏ အကျဉ်းချုပ်မှု

(6) ສາມ ລາວ ຊັນຕະ ຖີ່ | ແລ້ວ | ພິກາດ ຕີ່ ຂ່າງ | ຫີ້ | ຊັນຕະ

(۹) گردنی چشمی چشمی چشمی چشمی چشمی چشمی چشمی

(c) የኩርሻ ተቋም በማዕከራዊ

(ג) אוניברסיטה גנט הולנד ? אוניברסיטה

(1) ପ୍ରଦର୍ଶନ କାର୍ଯ୍ୟ ଏବଂ ପରିମାଣ

11. ດາວໂຫຼນ ແລ້ວ ຕົກລົງ ພຣະ ລົມ ພຣະ ພຣະ ພຣະ ພຣະ ພຣະ ພຣະ ພຣະ ພຣະ

፳፻፲፭

1758 (5)

၃၁။ အောက်ပါတိမျက်နှာမှာ ဖော်လုပ်ခြင်း၊ အောက်ပါတိမျက်နှာမှာ ဖော်လုပ်ခြင်း၊ အောက်ပါတိမျက်နှာမှာ ဖော်လုပ်ခြင်း၊

ଶ୍ରୀ ରାଜମାନ୍ | ପାତ୍ରମାନ୍ | କର୍ମଚାରୀ

ପ୍ରାଚୀନ ଲୋହ କର୍ମକାଳେ କର୍ମକାଳେ କର୍ମକାଳେ କର୍ମକାଳେ କର୍ମକାଳେ

- 5 -

અનુભૂતિ

۱۷۸۹ (۷)

၃။ အာသနရေးကို ပြန်လည်ပေါ်လေ့ရှိခဲ့သူများ၏ အာသနပေါ်လေ့ရှိခဲ့ခြင်း

۱۰۷

၃. အောင် မြန်မာ ပို့ကြခဲ့သော တော်မြတ်ရှိ ပေါ်လောက်မှုများ ဒေါ်မြတ်ရှိ ပေါ်လောက်မှုများ

11. නිර්වචන ව්‍යුත්ති පෙනී යොමු කිරීමේදී මෙම ප්‍රතිච්ඡලයි

వ్యక్తిగతి ప్రాణు పూర్వి

ପ୍ରକାଶକ ମେଳି

| ८८ (१)

- (ج) تقديم المساعدة الإعلامية الاستشارية في التحقيق والقضاء على حوادث أمن المعلومات.
(خ) حضور ممثلين من كل موقع لأي دورات تدريبية وجلسات عمل ينضمها الموقع الآخر.

المادة (4)
تبادل المعلومات

1. يجوز للطرفين تبادل المعلومات لأغراض مذكورة التفاهem هذه. سيتم الكشف عن المعلومات وفقاً مذكورة التفاهem هذه وفقاً للقانون والسياسات والآليات المحلية المعهود بها .
2. لا يجوز لأي طرف الإفصاح عن المعلومات التي تم الحصول عليها من الطرف الآخر بموجب أو فيما يتعلق بمذكورة التفاهem هذه إلى أي طرف ثالث دون موافقة مسبقة من الطرف الآخر .
3. يحترم الطرفان أي شرط أو قيود أو تحذير يحدده الطرف الآخر فيما يتعلق بالتعامل مع المعلومات أو الكشف عنها ، باستثناء الحالات التي يكون فيها الكشف عن هذه المعلومات إلزامياً بموجب القانون بناء على طلب محكمة قانونية.
4. سيطبق الطرفان حماية البيانات ، وفقاً للأطر القانونية الوطنية والدولية المعهود بها .
5. يعين الطرفان جهة اتصال مسؤولة عن الاتصالات بين الطرفين في إطار هذه الاتفاقية.
6. سيتم الاتفاق على أي نشاط مشترك ينطوي على الملكية الفكرية كتابة من قبل الأطراف لحماية المصالح ذات الصلة .

المادة (5)
حل النزاعات

تم تسوية أي خلافات / نزاعات بين الطرفين بشأن تفسير و / أو تنفيذ مذكورة التفاهem هذه ودياً من خلال المشاورات و / أو المفاوضات بين الطرفين.

المادة (6)
البدء والمدة والإنهاء

1. تدخل مذكورة التفاهem هذه حيز التنفيذ من تاريخ توقيع مذكورة التفاهem بين الطرفين.
2. من المفترض أن تظل مذكورة التفاهem هذه سارية المفعول لفترة أولية مدتها خمس (3) سنوات ويتم تجديدها تلقائياً لمدة خمس (3) سنوات لاحقة، ما لم يقدم الطرف الآخر إشعاراً كتابياً مدمجاً مدة ثلاثة (3) أشهر بنيته عدم تمديد مذكورة التفاهem. يجوز للطرفين إنهاءه في أي وقت عن طريق إخطار الطرف الآخر بكتاب يسري هذا الإنهاء تسعين (90) يوماً تقويمياً من تاريخ الإخطار ما لم يوافق الطرفان كتابة على فترة زمنية أقصر .
3. سيتم الانهاء من الأنشطة الجارية في وقت الإنهاء وفقاً لأحكام مذكورة التفاهem هذه.
4. يجوز تعديل مذكورة التفاهem هذه باتفاق خطوي متبادل بين الطرفين .

.5. يدخل تعديل مذكرة التفاهم هذه حيز التنفيذ في التاريخ الذي يحدده الطرفان بشكل متبادل.

المادة (7)
التكاليف والمصاريف والموارد

لا تعد هذه المذكرة إلزامية، ولا تنطوي على أي التزامات مالية لكلا الطرفين، ولا تترتب عليها أي حقوق أو التزامات قانونية بين الموقعين ويتحمل كل طرف مصاريفه الشخصية الخاصة ويزود نفسه بالموارد اللازمة لتنفيذ هذه المذكرة وغيرها من المصاريف ذات الصلة. تخضع الأنشطة التي يقام بها بموجب هذه المذكرة لتوفير الموارد المالية والإنسانية وفقاً لقوانين الموقعين الوطنية.

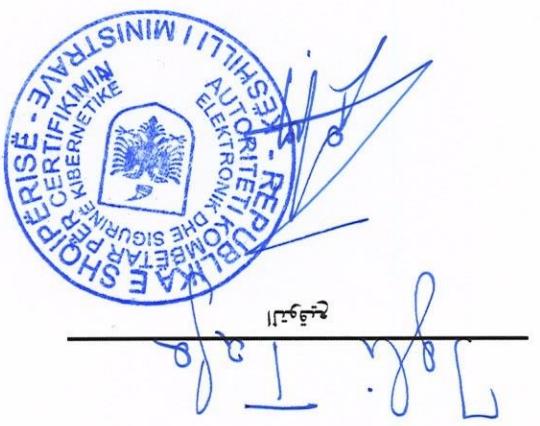
المادة (8)
اللغة

ستكون جميع الاتصالات بين الأطراف باللغة الإنجليزية. حيث تجمع مذكرة التفاهم هذه باللغات الأصلية: الإنجليزية والعربية والألبانية في حالة وجود أي تعارض في الفهم فإن اللغة الإنجليزية تسود.

تم توقيع مذكرة التفاهم هذه في 06.04.2023 بتاريخ ٢٠٢٣.

المادة (9)
معلومات الاتصال

مجلس الأمن السيبراني	البيئة الوطنية للتصديق الإلكتروني والأمن السيبراني
<p>الاسم: وافي يوسف علي فاضل بن فاضل المسمى الوظيفي: مجلس الأمن السيبراني</p> <p>رقم الهاتف: +971 50 287 8888 البريد الإلكتروني: ciso@csc.ae / grc@csc.ae رقم الهاتف: +971 50 7231 222 رقم هاتف الطوارئ: +971 50 2878888 العنوان: دبي - الإمارات العربية المتحدة</p>	<p>الاسم: روكيسيون كافا المسمى الوظيفي: البيئة الوطنية للتصديق الإلكتروني والأمن السيبراني</p> <p>رقم الهاتف: +355697035660 البريد الإلكتروني: rexhion.qafa@cesk.gov.al رقم الهاتف: +355 4 22 210 39 رقم هاتف الطوارئ: +35569208722 العنوان: تيرانا - ألبانيا</p>



2018

2018

સર્વેની પાત્રાની દાખલી કરી રહી છે।

અધ્યક્ષ

સર્વેની પાત્રાની દાખલી કરી રહી છે।

અધ્યક્ષ

સર્વેની પાત્રાની દાખલી કરી રહી છે।

સર્વેની પાત્રાની દાખલી કરી રહી છે।

2018

(10) જાન્યુઆરી