حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

Dubai Electronic Security Center

Cyber Force Program Guidelines

Version 1.1 | July 2024

Table of Contents

1. Introduction

Dubai Electronic Security Center (DESC) is committed to establishing Dubai as a global leader in innovation, safety, and security. In line with the vision of the Vice President and Prime Minister and Ruler of Dubai, His Highness Sheikh Mohammed bin Rashid Al Maktoum, to place Dubai among the most secure cities electronically in the world, the Dubai Cyber Security Strategy was launched in 2017, with a new version released in 2023, which defines Dubai's vision and objectives in this regard. The strategy provides rules protecting the data and electronic services from threats and attacks, as well as protecting companies, individual users, or any information technology–related activities.

A vital strategy domain is creating a Cyber Secure Society—achieving awareness, skills, and capabilities to manage cyber security risks for Dubai's public and private sectors and individuals. This will therefore support Dubai to become an established cyber hub in the region and to influence regional and global cyber security standards.

To achieve these strategic objectives, we need to develop:

- **Capacity** – The availability of knowledgeable, experienced, and trained personnel specialized in cyber security for public and private sector organizations;
- **Capability** – Raising the skills of cyber security experts.

Another fundamental domain from the strategy is Active Cyber Collaboration. The following areas of focus are identified to achieve the objectives of this domain:

- Establishment of international collaboration – setting internationally recognized standards and enabling Dubai to build a cyber eco–system that aligns with the best practices globally;
- Collaboration between organizations forming part of the Critical Information Infrastructure (CII) and establishing partnerships with the public and private sectors – connecting the public sector to the private sector cyber service providers through collaboration with global certification bodies;
- Establishment of cyber security legislation and regulations – the implementation of rules that drive capacity, capability, and consistency aligned with international standards.

1.1 Purpose

This document serves as an implementation guideline for the Cyber Force Program with its scope of cyber security services. It covers the compliance requirements for the cyber security service providers, details the certification pathways, and providers guidelines to the cyber security service consumers.

The Cyber Force Program ensures the following:

- **Skills and competence:** Companies providing services under the program will employ individuals with DESC–approved qualifications and suitable experience;

- **Methodologies:** Services will be conducted using DESC–recognized and internationally accepted best practices and approaches which are according to the specific scope of activity. Each in–scope disciplines will have corresponding detailed methodologies and approaches;
- **Reporting:** Reports and recommendations are produced in a recognized standard, each having its own format according to the scope of activity and discipline requirement.

The program aims to define processes and principles to ensure consistency, capability, and capacity in the marketplace.

It provides reassurance that:

- The processes and procedures of the service providers have been subject to independent audit;
- Systems and data will be handled safely and according to the ISR V3 Controls 2.7.1, 2.7.2, 11.1.1 and 13.2.1 covering the legal jurisdiction and geographical boundaries of the UAE;
- Individuals with the appropriate skills, certifications and competences will deliver the services;
- The approved service provider and individuals are bound by Codes of Conduct and Ethics, including an independent compliance process.

1.2 Scope and Applicability

1.2.1 Scope

The first phase of the program will focus on two disciplines: Penetration Testing and Incident Response. The scope will be updated as the program expands.

The Cyber Force Program may include, but not limited to, the following cyber security services:

- Cyber security governance;
- Cyber security risk management;
- Cyber security audit;
- Cyber security architecture;
- Digital forensics and malware analysis;
- Security Operations Centers (SOC) analysts;
- Threat hunting and intelligence;
- Vulnerability assessment.

It is mandatory for the following entities to procure the cyber security services from Cyber Force Certified Service Providers:

- Dubai government entities;

- Semi-government entities;[1]
- Critical organizations under Dubai CII.

Organizations other than the above entities, at their discretion, may choose from the approved service providers.

1.2.2 Applicability

The program applies to all cyber security service providers offering their services to the government entities, semi-government entities and CII organizations.

For this document, the stakeholders of the Cyber Force Program are described as follows:

- **Cyber security Service Providers:** The cyber security service providers deliver one or more activities listed under Section 1.2.1 (Scope). All cyber security service providers shall comply with the requirements stated in Section 2 of this document.
- **Certification Bodies:** The certification bodies referred to in this document are those that conduct the assessment, validation, and certification of the cyber security service providers. Section 3 provides information about existing certification bodies, information about any additional certification bodies will be added as the program evolves.
- **Cyber security service consumers:** Dubai governments and semi-governments, CII, and any other entities regulated by DESC are referred to as Cyber security service consumers. They should only procure and leverage the certified Cyber security service providers.

Section 5 provides guidelines to consider while acquiring cyber security services under the Cyber Force Program.

2. Cyber security Service Providers Requirements

This section highlights the program requirements set by DESC for each cyber security service provisioning discipline. This includes both the companies and individuals working for those companies.

DESC-approved cyber security service providers are required to consistently:

- Maintain data security following the Dubai-UAE Laws;
- Deploy recommended methodologies for a standardized cyber security service consumer experience;
- Leverage approved cyber security service providers to accelerate the procurement and selection process with confidence.

[1] Semi-government entities are defined as: Companies owned by government agencies or organizations in which the government contributes 25% or more of their capital. DESC, by management directives, may also extend its mandate to companies in which the government owns less than 25% capital.

2.1 Accountability of Service Providers

Given the likely complexity of any assignments delivered under this program, a qualified team from the chosen service provider will be required to deliver the engagements. It is recommended that a Team Leader is assigned with the ultimate accountability for the engagement. The Team Leader will provide guidance, direction, and leadership to the remaining Team Members engaged and must be identified and confirmed before an engagement commences.

The team should have members with the requisite skills aligned to their role. Without exception, they must be appropriately skilled to:

- Scope, oversee, and sign off an engagement: this is recommended to be performed by a certified Team Leader;
- Conduct the technical elements of an engagement: this is recommended to be performed by certified Team Members.

DESC sets out the skill and competence requirements of the Team Leader and Team Member for each discipline based on examination (evidenced by certifications) or other suitable experience. Each parties roles and responsibilities are outlined in Table 1.

Table 1: Roles and responsibilities.

Party	Roles and responsibilities
DESC	Provide technical requirements and approval criteria for certification bodies and service providers.
Cyber Security Service Providers	Obtain a local trade license and required Accreditations, ensure team members are skilled and competent and apply for certification.
Individuals	Obtain and maintain relevant certifications and requirements and complete the skilled person register.
Approved Certification Body	Certify individuals and companies to provide in-scope cyber security services to government, semi-government, and CII entities.
Cyber Security Service Consumers	Ensure certified providers conduct all in-scope engagements and are holding a valid security clearance.

2.2 Cyber Security Service Providers' Requirements (Companies)

The cyber security service providers are required to meet the qualifying criteria and present themselves with the requirements during the assessment.

2.2.1 Qualifying Criteria

All Companies must meet the following criteria:

- The individuals deployed by the Company to the Cyber Security Service Consumers must hold the requisite qualifications as stipulated in the DESC discipline-specific requirements (See Appendix C for the respective cyber security service provision);
- The Company must have a local presence in the country, achieved by holding a trade license in the UAE (either mainland or free zone);
- The Company must comply with the applicable UAE laws (See ISR V3: 11.1.1);
- The Company must have performed the relevant discipline services under their name for at least 6 months;
- Proposed team members are required to undergo Dubai Police security clearance requirements or other forms of identity confirmation.

It is recommended that at least one representative have Team Leader status, and the remainder may have Team Member status in the related discipline, depending on the scope and criticality of the activity.

2.2.2 Assessment Requirements

A service provider undergoes assessment for its service provision, which may cover an audit of its:

- Policies and operating procedures;
- Individual competences;
- Data assurance processes;
- Technical methodologies;
- Significant related engagements for at least one year;
- Two independent references from companies/organizations for which the Company has conducted related work;
- Evidence demonstrating that it has a quality and information security management policy and process for running each service offering, which is actively reviewed and updated to keep it fit for purpose.

2.3 Cyber Security Service Providers' Requirements (Individuals)

Individuals applying to this program must meet the following requirements:

- Individuals must work for a company with a local presence and a valid UAE trade license, and certified under the Cyber Force Program;

- Individuals must have the appropriate skills and competence set out by the DESC discipline requirements (See Appendix C for the respective cyber security service provision) and Dubai Digital Skills Framework;
- Individuals must be aware of, and comply with, the DESC Terms of Service. This will be shared by the Certification Bodies and signed by the Company;
- Individuals must have the right to work in Dubai (if operating physically within the country);
- Individuals must present a valid Dubai Police security clearance[2] when applying for certification;
- Individuals must adhere to any mandated DESC–approved methodologies according to the discipline.

3. Certification Bodies Overview

To achieve the objectives of the Cyber Force Program in effectively building the pool of skilled cyber security resources in Dubai, DESC is committed to aligning with the highest industry standards and best practices. Recognizing the importance of collaboration to achieve these goals, DESC is partnering with prominent organizations from the cyber security industry.

These partnerships are significant in providing both Dubai government and the private sector providing the services, with the assurance that our certification processes are thorough, credible, and aligned with international best practices.

As Cyber Force evolves, so will the network of partners, to include additional certification bodies that will cater to the different disciplines.

Once DESC approves the qualifications of the certification body, it follows the process described in Appendix B: Cyber Force Certification Program Process (High Level).

Certification Bodies will be re–evaluated against the criteria listed above every three years.

3.1 CREST International

For the purpose of implementing the first phase of the Cyber Force Program, DESC partnered with CREST International, a globally recognized authority in cyber security certification. CREST International is renowned for its rigorous standards and comprehensive certification programs, which are trusted by organizations worldwide. Their expertise spans various critical areas of cyber security, including penetration testing, threat intelligence, and incident response.

Established in 2006, CREST International is a not–for–profit accreditation and certification body that builds trust in the digital world by raising professional standards and delivering measurable quality assurance for the global cyber security industry.

[2] To access Dubai Police security clearance portal, use the following link: https://www.dubaipolice.gov.ae/wps/portal/home/services/individualservices/goodconductcertificate?firstView=true

CREST regularly engages with governments and industries globally to develop frameworks and help implement programs to ensure excellence in the cyber security industry.

CREST also supports professional development and knowledge sharing, through pathways that encourage talent into the market and guidance material that enhance knowledge and increase awareness of best practice.

By collaborating with CREST International to certify Penetration Testing and Incident Response provisioning activities in Dubai, DESC will benefit from their extensive knowledge and well-established certification frameworks. This partnership ensures that DESC requirements, mapped with requirement from CREST are validated, reinforcing our commitment to upholding the highest standards of security and professional excellence.

Further information about CREST can be found on our website: https://www.crest-approved.org/

4. Certification Process

DESC will own the certification process and approval and may delegate operational responsibility to other certification bodies to conduct the process under DESC's oversight.

Applicants may receive feedback requiring additional information to complete an application. Any application that is formally refused may be resubmitted after one year from the date of the refusal. Applicants will be advised of the timeframe for re-applying if the application is unsuccessful.

This process is illustrated in Appendix B: Cyber Force Certification Program Process (High Level).

4.1 Certification Renewal

The process for renewing certification will be set out according to discipline-specific requirements, including frequency. This could include, but is not limited to, submission of evidence demonstrating conformity to the registration requirements (including any requirements added since the last submission), evidence of maintained or enhanced skills and competences, re-signing code/s of conduct, and re-applying for security clearance where required.

Registration renewal should be planned and initiated with sufficient notice to ensure minimal disruption to service provision. The service provider is responsible for this process.

4.2 Associated Cost

No costs are associated with applying to be certified under the DESC Cyber Force Program. However, the applicant and company will bear any costs to achieve the required individual certifications and company accreditations respectively as outlined in the Appendices.

4.3 Certificate Validity

The Cyber Force Certificate is renewable yearly. A certificate renewal process will also be conducted by the DESC-approved Certification Body.

Any certifications that expired, and new certifications acquired shall be provided during the recertification. Failure to submit these documents and to apply for a DESC certificate renewal will constitute an expiration of the certificate and the certification will be revoked.

5. Cyber Security Services Consumer Guidelines

Entities regulated under this program should use a risk–based approach when contracting to ensure that the service provider's team is suitably skilled and competent.

5.1 Selection and Management of Cyber Security Service Provider

Consumers of services under the Cyber Force Program are mandated to acquire the services certified by DESC. Therefore, it shall be ensured in the procurement process that the bidding vendors are DESC–certified. Table 2 provides recommendations for the selection and management of cybersecurity service providers in the various contracting stages.

Table 2: Recommendations during various contracting stages.

Contracting Stage	Area of Focus	Recommendation
Preliminary Activities (During tendering)	Selection of service provider	Ensure the selection of a service provider from the list of Certified Cyber Force Providers. The list can be found on this link: Cyber Force Certified Service Providers In the case of existing vendors not holding a Cyber Force Certificate, entities are encouraged to direct vendors to DESC to be enrolled in the program. In addition to compliance with DESC requirements, the vendor selection should be based a rigorous evaluation process of the vendor's technical capabilities and previous experiences.
	Risk Assessment	Conduct a thorough risk assessment prior to the engagement to identify potential risks. Use the results of the assessment to make an informed procurement decision.
	Trade License	Ensure that the service provider is holding a valid UAE trade license.
	Dubai Police Security Clearance	Ensure that all individuals engaged in the service present a valid Dubai Police Security Clearance.
	Scope	Ensure that the scope of the engagement matches the scope of the provider's certified service. The Cyber Force Program certificate is scope based and each discipline is clearly stated on the

Contracting Stage	Area of Focus	Recommendation
During Procurement	Contractual Agreements	Ensure the inclusion of a technical expert in the process of drafting the contractual agreements between the entity and the provider to properly define roles, responsibilities, and related SLAs. Any contract for cyber security services regulated under the Cyber Force Program is made between the procuring entity and the selected service provider. DESC is not a party to the individual contracts. The Cyber Security Service Consumer and Cyber Security Service Provider must sign a Non-Disclosure Agreement that is aligned to Appendix D: Cyber Force Certification Program Terms Section 6: Confidentiality and Publicity, and the Dubai Data Lawn No. 26 of 2015
	Service Delivery	Ensure the inclusion of a technical expert in the process of drafting the contractual agreements between the entity and the provider to properly define roles, responsibilities, and related SLAs. Any contract for cyber security services regulated under the Cyber Force Program is made between the procuring entity and the selected service provider. DESC is not a party to the individual contracts. The Cyber Security Service Consumer and Cyber Security Service Provider must sign a Non-Disclosure Agreement that is aligned to Appendix D: Cyber Force Certification Program Terms Section 6: Confidentiality and Publicity, and the Dubai Data Law No. 26 of 2015
	Data Protection and Privacy	Ensure that classified data always remain within the boundaries of the UAE (during and after engagement), in reference to ISR V3 2.7.1. Entities should emphasize in their contracts with the service providers on data protection and privacy to adhere with the local data regulations, as stated in ISR V3 2.7.1; 2.7.2
After procurement		The contract must include a clause ensuring that if a certified company changes its legal name, the Service Consumer is notified within 14 working days. The consumer must ensure that the company provides DESC with the required information to update it legal name on the Cyber Force Certificate.
	Reporting	Cooperate with the service providers to meet the reporting requirements stated in relation to each discipline, according to ISR V3 4.1.4

5.2 Reporting, Feedback and Complaint

5.2.1 Reporting

Depending on the discipline, DESC may require specific and regular reporting from government agencies, cyber security service providers, and certification bodies.
This will be detailed within the specific discipline requirements under Appendix C.

5.2.2 Feedback

DESC welcomes feedback to keep the program running smoothly and to continuously improve the requirements as needed. To share your feedback, email cyberforce@desc.gov.ae
Complaints about companies or individuals that have provided a service under the program should first be directed through the DESC–approved certification body which registered the company or individual on behalf of DESC.

6. Appendices

Appendix A: Definitions

Terms	Definition
Approved Cyber Security Service	The Companies approved under this program who meet the requirements of certification according to the scope of service.
Certification Body	Certification bodies are bodies which have been approved by DESC to conduct the assessment, validation, and certification of cyber security service providers and individuals under the Cyber Force Program.
Cyber Security Service Consumers	Entities regulated by DESC (government entities, semi–government, and CII organizations), utilizing services from the Cyber Force Program.[3]
Critical Information Infrastructure (CII) Organizations	Organizations with business processes/services whose compromise can severely impact Dubai's sustainability and continuity of the most critical functions and services. The incapacity of those services would drastically impact the UAE's society, economy, and safety.[4]
Cyber Digital Skills Framework	The framework which sets out cyber security's roles and career paths, covering role descriptions, tasks, technical skills, soft skills, training, and certifications.

[3] Ref: https://www.desc.gov.ae/regulations/critical-information-infrastructure/

[4] Ref: https://www.desc.gov.ae/regulations/critical-information-infrastructure/

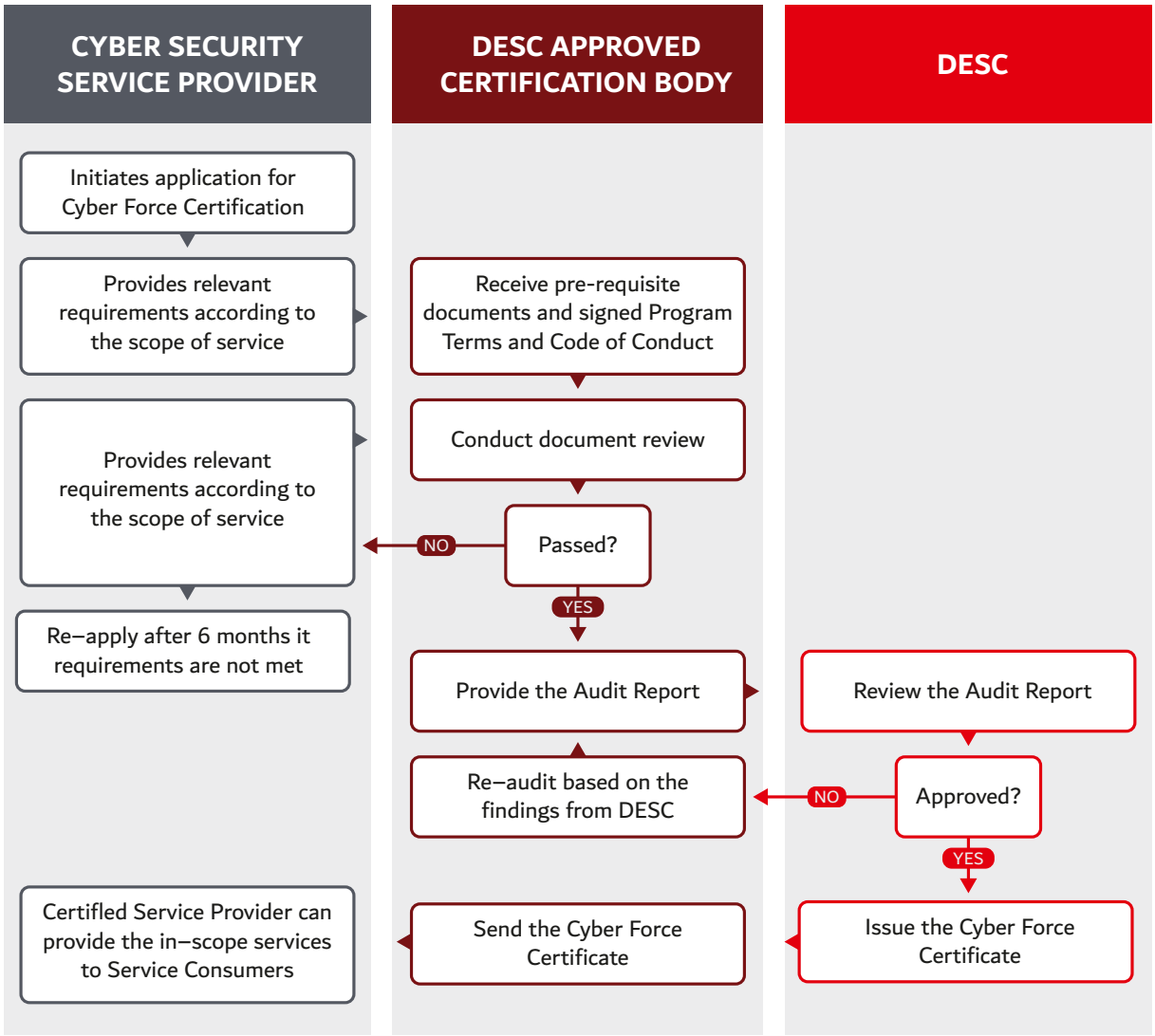
[5] (NIST 800–61 – Computer Security Incident Handling Guide).

[6] (NIST 800–115: Technical Guide to Information Security Testing and Assessment).

Terms	Definition
Dubai Cyber Force Program	The program which aims to certify companies that employ skilled and competent individuals who can provide in-scope services to defined entities within Dubai that DESC regulates.
Government entities	Refers to the Dubai government agencies regulated by DESC.
Incident Response	The process of detecting, analyzing, and responding to computer security incidents. It involves a set of actions taken by an organization when they become aware of a security incident.[5]
Individual	An employee of an approved cyber security service provider delivering services to the consumers.
Penetration testing	A test methodology in which assessors, typically working under a specific constraint, attempt to circumvent or defeat the security features of an
Semi-government entities	Companies owned by government agencies or organizations in which the government contributes 25% or more of their capital. DESC, following management directive, may also extend its mandate to companies in which the government owns less than 25% capital.[7]
Skilled Persons Register	The register collects details on individuals' education, training, certifications, industry tenure, specific sector alignments, and soft skills.
Team Leader	The individual within a service provider with the ultimate accountability for the engagement.
Team Members	The individual/s within a service provider team performing the work.
ISR	The Dubai Government Information Security Regulation provides key practices and controls in information security to be adopted by all Dubai Government Entities. Its purpose is to ensure continuity of critical business processes, and minimize information security related risks and damages and ensuring appropriate level of Confidentiality, Integrity and Availability for information handled within Dubai Government Entities.

[7] Law No. (4) of 2018: Create Financial Supervision Authority – Subject entities (Article 18).

Appendix B: Cyber Force Certification Program Process (High Level)



Appendix C: Specific Program Requirements

C.1: Penetration Testing Specific Program Requirements

Discipline: Penetration Testing	Date Implemented; November, 2023

Approved Certification Body: CREST

C.1.1 Overview

Penetration testing is a test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

Planning and commissioning a penetration test on your network should be done carefully. The CREST Defensible Penetration Test must be adhered to, which offers guidance on producing a commercially defensible assurance activity that is appropriately scoped, executed, and signed off.

The program will assess both companies and individuals. This approach assures that the services delivered under the program are delivered by companies rigorously assessed for their expertise and that those services will be appropriately scoped, executed, and signed off. In parallel, the program assures that individuals with the necessary skills and competences conduct the companies' services.

Furthermore, by interlinking these criteria with binding Codes of Conduct, the Consumers of services have confidence that the engagement will be conducted diligently.

C.1.2 Accountability

CREST International administers the Penetration Testing discipline of the DESC Cyber Force Program, but DESC remains responsible for overall accountability.

C.1.3 Scope of Services

This program facilitates the registration of companies and individuals working for those companies, providing penetration testing services regulated by DESC.

Such companies' individual registrants will have DESC–approved qualifications, experience and internationally accepted best practices, and CREST Defensible Penetration Test.

C.1.4 Discipline-Specific Requirements

C.1.4.1 Company

In addition to the requirements highlighted in section 2, the service providers performing in-scope services must supply the following:

- An outline of their Penetration Testing methodology that will be used;
- Completion of the Skilled Person Register;
- The company registers their technical staff on the CREST Skilled Persons Register. The register collects details on their education, training, and certifications and recognizes them as having the appropriate skills and competence. It also gathers information on their industry tenure, specific sector alignments, and soft skills;
- Sign Codes of Conduct and Ethics;
- Agreement to the enforceable Codes of Conduct and Ethics bind both Companies and individuals.

C.1.4.2 Individuals

Qualifying skills and competence

To provide certain cyber security services to the government in Dubai, service providers must demonstrate the competence of the individuals via certifications.

CREST certifications have been mapped to requirements from the Dubai Digital Skills Framework, which outlines the expertise and skills that cyber security professionals must have. The program requirements have also been mapped to a number of internationally recognized certifications, to ensure international harmonization and alignment.

To qualify for Penetration Testing certification under the Cyber Force Program, individual employees must possess one of the following certifications in Figure 2. The role they are assigned within the Cyber Force, either as a Team Member or a Team Leader, is contingent on their specific certification.

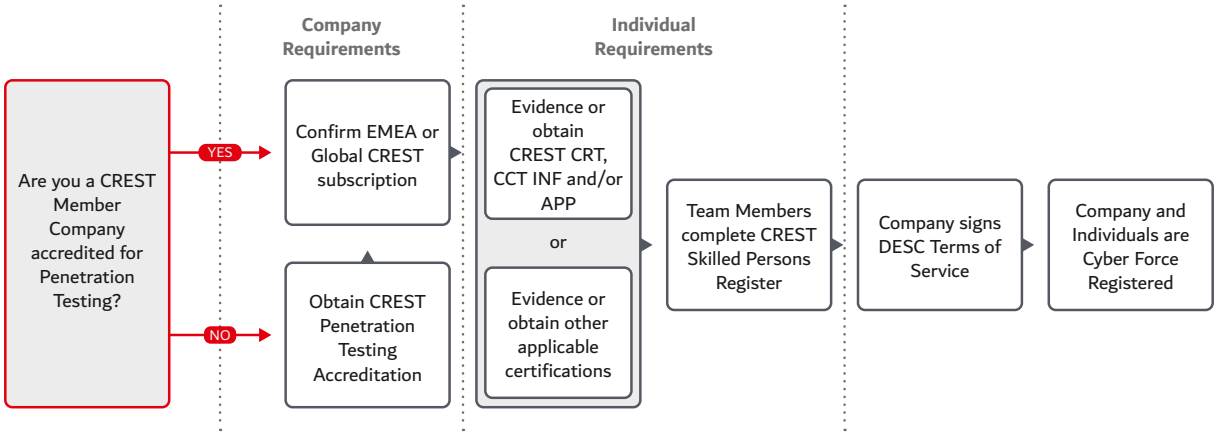
Figure 2: Mapping of Incident Response requirements to DESC Digital Skills Framework.

DESC Designation	Team Member	Team Leader			
Dubai Digital Skills Framework	Analyst / Tester	Senior Analyst / Tester & Leader / Specialist			Senior Specialist
	Pen Tester	Senior Pen Tester	Pen Tester Leader	Specialist Pen Tester	Senior Specialist Pen Tester
DESC accepted certifications	CREST CRT OffSec OSCP EC-Council ESCA, LPT GIAC GPEN, GWAPT	CREST CCT APP, CCT INF OffSec OSEP, OSWE GIAC GXPN			

C.1.5 Certification Process

The Figure 3 illustrates the certification process for the company and individuals, including route if the applicant is a CREST Member or not.

Figure 3: Certification Process for Penetration testing.



C.1.6 Reporting Requirements

The penetration test results should be reported according to the CREST Defensible Penetration Test standard.

DESC requires the Approved Service Providers providing services to cyber security service consumers to disclose any major gaps revealed in the security assessment. This information will be shared directly with DESC via the email cyberforce@desc.gov.ae, within five working days of issuing the report.

The following information will be required:

- Details about the Company providing the service (name, registration address);

- Names of the individuals providing the service;
- Detailed report about the scope and the results of the engagement;
- Summary of the next steps discussed with the in-scope entity.

C.1.7 Abbreviations

This tabele of abbreviations is specific to this discipline.

Terms	Definitions
CRT	CREST Registered Penetration Tester
CCT INF	CREST Certified Infrastructure Tester
CCT APP	CREST Certified Web Application Tester
OSCP	OffSec Certified Professional
ECSA	EC-Council Certified Security Analyst
ELPT	EC-Council Licensed Penetration Tester
GPEN	GIAC Penetration Tester
GWAPT	GIAC Web Application Penetration Tester
OSEP	OffSec Experienced Penetration Tester
OSWE	OffSec Web Expert
GXPN	SANS GIAC Exploit Researcher and Advanced Penetration Tester

C.2: Incident Response Specific Program Requirements

Discipline: Incident Response	**Date Implemented; November, 2023**
Approved Certification Body: CREST	CREST

C.2.1 Overview

Incident response is the process of detecting, analyzing, and responding to computer incidents. It involves a set of actions taken by an organization when they become aware of a security incident.

DESC-approved incident response services are required for multiple reasons, including:

- Maintaining data security;

- Deploying recommended methodologies for a standardized service experience;
- Leveraging approved testing providers to accelerate the selection process with confidence.

The program will assess both companies and individuals. This approach assures that the services delivered under the program are delivered by companies rigorously assessed for their expertise and that those services will be appropriately scoped, executed, and signed off. In parallel, the program assures that individuals with the necessary skills and competences conduct the companies' services.

Furthermore, by interlinking these criteria with binding Codes of Conduct, the service buyers have confidence that the engagement will be conducted diligently.

C.2.2 Accountability

CREST International administers the Incident Response discipline of the DESC Cyber Force Program, but DESC remains responsible for overall accountability.

C.2.3 Scope of Services

This program facilitates the registration of companies and individuals working for those companies, providing incident response services regulated by DESC.

It enables approved incident response providers to carry out authorized activities relating to cyber security service consumers' assets to respond to incidents, provide reports and remediation assistance.

The employees of such companies will have DESC–approved qualifications and experience.

C.2.4. Discipline–Specific Requirements

C.2.4.1 Company

In addition to the requirements highlighted in section 2, the service providers performing in–scope services must supply the following:

- An outline of their Incident Response methodology that will be used.
- Completion of the Skilled Person Register
  - The company registers their technical staff on the CREST Skilled Persons Register. The register collects details on their education, training, and certifications and recognizes them as having appropriate skills and competence. It also gathers information on their industry tenure, specific sector alignments, and soft skills.
- Sign Codes of Conduct and Ethics.
  - Agreement to the enforceable Codes of Conduct and Ethics bind both Companies and individuals.

C.2.4.2 Individuals

Qualifying skills and competence

To provide certain cyber security services to the government in Dubai, providers must demonstrate the competence of the individual via certifications.

CREST and other certifications have been mapped to requirements from the Dubai Digital Skills Framework, which outlines the expertise and skills that cyber security professionals must have.

To be certified for Incident Response under the Cyber Force Program, individual employees must possess one of the following certifications in Figure 4. The role they are assigned within the Cyber Force, either as a Team Member or a Team Leader, is contingent on their specific certification.

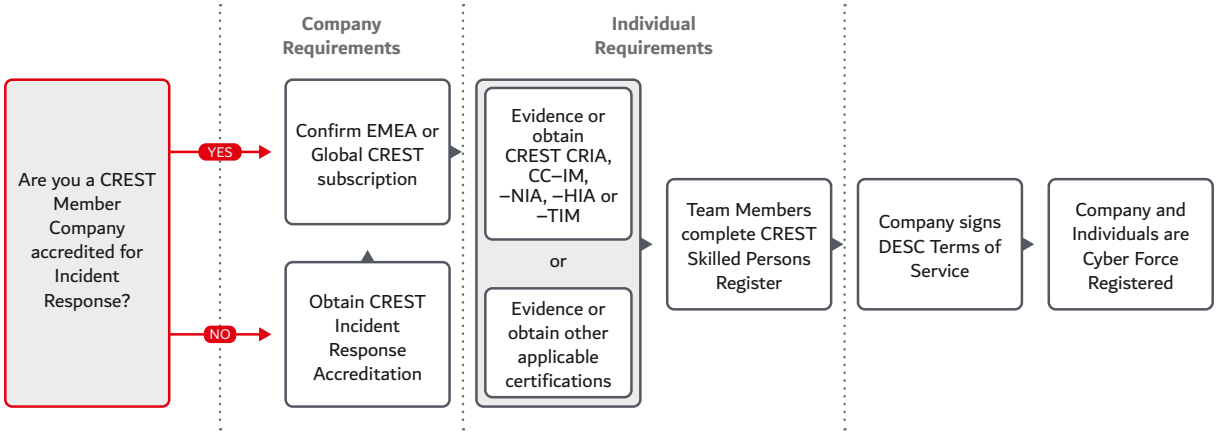
Figure 4: Mapping of Incident Response requirements to DESC Digital Skills Framework.

DESC Designation	Team Member	Team Leader			
Dubai Digital Skills Framework	Analyst / Tester	Senior Analyst / Tester & Leader / Specialist			Senior Specialist
	Incident Response Analyst	Senior Incident Response Analyst	Senior Threat Hunting (TH) & Intelligence Analyst (IA)	TH & IA Manager TH & IA Specialist	Senior Specialist TH & IA
DESC accepted certifications	CREST CRIA GIAC GCFR, GCFA	CREST CCIM, CCNIA, CCHIA (IR) CREST CCTIM (TI) GIAC GREM			

C.2.5 Certification Process

The Figure 5 illustrates the certification process for the company and individuals, including route if the applicant is a CREST Member or not.

Figure 5: Incident Response Cyber Force Certification Process.



C.2.6 Reporting Requirements

DESC requires Approved Service Providers to provide services to cyber security service consumers to disclose any critical incidents to which they respond. This information will be shared directly with DESC via the email cyberforce@desc.gov.ae, within the same day it is discovered.

The following information will be required:

Details about the Company providing the service (name, registration address);

Names of the individuals providing the service;

Detailed report about the results of the engagement;

Summary of the next steps discussed with the in-scope entity.

C.2.7 Abbreviations

This table of abbreviations is specific to this discipline.

Terms	Definitions
CRIA	CREST Registered Penetration Tester
CCNIA	CREST Certified Infrastructure Tester
CCHIA	CREST Certified Web Application Tester
CCIM	OffSec Certified Professional
CCTIM	EC-Council Certified Security Analyst
GCFR	EC-Council Licensed Penetration Tester
GCFA	GIAC Penetration Tester
GREM	GIAC Web Application Penetration Tester

Appendix D: Cyber Force Certification Program terms

The Program Terms govern the delivery of Regulated Services under the CyberForce Certification Program as between DESC, a Certifying Body and any Certified Service Provider. The Certified Service Provider will be expected to enter into separate contractual arrangements with each Requesting Entity to govern the terms of any Regulated Service that the Certified Service Provider provides.

1. Definitions

In these Program Terms the following definitions shall apply:

Applicant means any individual, entity or organisation that applies for the CyberForce Certification Program;

Application means a form (in a format to be determined by DESC) sent by Applicants to DESC or the Certifying Body requesting enrolment and certification pursuant to the CyberForce Certification Program in respect of a Regulated Service;

Application Period means the period commencing from the date that an Applicant send an Application to DESC or the Certifying Body until the date of the notice sent to the Applicant by DESC or the Certifying Body notifying them of the outcome of their application;

Certification Mark means any logo, identifier, symbol or picture provided by DESC to the Certified Service Provider indicating their qualification as a Certified Service Provider which they may use in accordance with Clause 6 of these Program Terms;

Certification Period means the period commencing from the date of the notice sent to the Applicant notifying them that they have successfully obtained the CyberForce Certificate and until the expiration date of the CyberForce Certificate in accordance with the CyberForce Program Guidelines, unless the CyberForce Certificate is earlier revoked, suspended or terminated;

Certified Service Provider means an Applicant that has successfully completed the CyberForce Certification Program and holds a valid CyberForce Certificate;

Certifying Body means any entity appointed by DESC to assess an Application and may include DESC and any other third party certification body;

Certifying Body Code of Conduct means any rules or terms and conditions pertaining to the CyberForce Certification Program that are mandated by the Certifying Body and for which Applicants and Certified Service Providers are required to comply with;

Cyberforce Certificate means a certificate issued to an Applicant confirming that they have successfully completed the CyberForce Certification Program and are now deemed as a Certified Service Provider for a specific Regulated Service;

Cyberforce Certification Program means a certification program administered by any Certifying Body, and DESC to regulate a Requesting Entity's engagement with cybersecurity service providers in relation to Regulated Services and to ensure that Regulated Services are only offered

by Certified Service Providers, the details of which are set out in the CyberForce Program Guidelines;

Cyberforce Program Guidelines means the rules and requirements for Applicants to obtain the CyberForce Certificate and become a Certified Service Provider in respect of the Regulated Services and are attached hereby as Appendix A;

DESC means the Dubai Electronic Security Center, a Dubai Government entity responsible for regulating cybersecurity in Dubai and overseeing and monitoring the implementation and adoption of security standards and controls in addition to securing systems and information for Dubai Government and semi-government entities, amongst other objectives in its mandate;

Good Industry Practice means the practices, methods and procedures and that best degree of skill, diligence, prudence and foresight which would reasonably be expected from a skilled and experienced professional of international repute engaged in carrying out activities the same as, or similar to, the Regulated Services under the same or similar circumstances;

Regulated Service means a cybersecurity service which DESC in its sole discretion may determine that only Certified Service Providers can provide to Requesting Entities and includes any cybersecurity services that DESC may designate as a Regulated Service from time to time;

Requesting Entity means Dubai Government Entities, Dubai Semi-Government Entities and Dubai's critical information infrastructure entities (as determined by DESC) who require Regulated Services and **Requesting Entities** shall be construed accordingly; and

Program Terms means these program terms pertaining to the CyberForce Certification Program.

2. Acceptance of Program Terms

2.1. Each Applicant and Certified Service Provider acknowledges that they have read and understood these Program Terms and agree to be bound by them throughout the Application Period and the Certification Period (as applicable).

2.2. These Program Terms apply to Regulated Services and shall include any ancillary services that may be provided by any Certified Service Provider alongside the Regulated Services.

2.3. These Program Terms shall prevail over any other terms and conditions pertaining to the Regulated Services, including any Certifying Body's Code of Conduct. Notwithstanding the foregoing, the Certifying Body's Code of Conduct may be referred to and cited by DESC in the event of a complaint from an Applicant or Certified Service Provider.

2.4. Each Applicant agrees that any Application shall only be deemed valid if the Applicant has made payment of all relevant fees. An Application will not be considered by DESC or the Certifying Body unless and until all payment of the relevant fees has been made. For the avoidance of doubt, DESC shall have no liability or responsibility for any fees paid or payable to third parties.

2.5. DESC may charge a fee for each Application and any fees payable shall be set out in the fees schedule in Appendix B of these Program Terms.

2.6. At the date of submission of an Application, the Applicant undertakes, warrants and represents that: (I) where required by law, it has been duly incorporated or established and is validly existing under the laws of the jurisdiction of its incorporation or establishment; and (II) where applicable, it shall ensure that each of its personnel has read, understood and shall fully comply with these Program Terms during the Certification Period.

3. Scope of Program Terms

3.1. The Certifying Body will evaluate and assess the qualifications and credentials of Applicants applying for the CyberForce Certification Program, based on the criteria set out in the CyberForce Program Guidelines.

3.2. An Application will not be considered for assessment unless and until the Applicant has provided such complete documentation as may be required by DESC or the Certifying Body and has complied with all requests from DESC or the Certifying Body.

3.3. If an assessment of an Applicant for a CyberForce Certification Program is completed with a positive result, the Applicant shall be issued with a CyberForce Certificate in accordance with the CyberForce Program Guidelines and shall be deemed for the duration of the CyberForce Certificate tenure as a Certified Service Provider unless the CyberForce Certificate is otherwise revoked, suspended or terminated in accordance with these Program Terms.

3.4. If an assessment of an Applicant for a CyberForce Certification Program is completed with a negative result, the Applicant shall be notified by the Certifying Body in writing of the unsuccessful outcome of their application for the CyberForce Certification Program and whether they have a right to appeal the decision made by the Certifying Body.

3.5. No refunds of any fees will be issued to Applicants who do not successfully complete the CyberForce Certification Program or who complete the CyberForce Certification Program with a negative result.

4. Certified Service Provider's Standard of Service

4.1. During the Certification Period, each Certified Service Provider:

4.1.1. Shall provide the Regulated Services in line with Good Industry Practice and in compliance with the regulations applicable to these Regulated Services at the time of contract conclusion with any Requesting Entity; and

4.1.2. Acknowledges and agrees that the Certifying Body may at any time during the Certification Period conduct audits, inspections, or re-evaluations of Certified Service Providers (whether on-site or remotely) to ensure ongoing compliance with the CyberForce Certification Program requirements, and Certified Service

Providers shall comply with all such audits, inspections and re-evaluations, including providing any documents or information requested by the Certifying Body.

5. Participation and Conduct

5.1. Each Applicant and Certified Service Provider undertakes, warrants and represents to DESC, Certifying Body and any Requesting Entity that:

5.1.1. During the Application Period, it shall provide accurate and truthful information during the CyberForce Certification Program application process, and promptly update DESC and the Certifying Body about any changes that may affect their eligibility or compliance;

5.1.2. During the Application Period and Certification Period, all information concerning the Applicant or Certified Service Provider which has been disclosed to DESC or the Certifying Body is true and accurate and does not omit to state any fact the omission of which makes any such information to be misleading, or which might, if disclosed, adversely affect the decision of DESC or the Certifying Body to grant the CyberForce Certificate.

5.1.3. During the Application Period and Certification Period, it shall comply with all relevant laws together with any applicable codes of practice and other recommendations, instructions and any code of conduct issued by DESC from time to time;

5.1.4. During the Application Period and Certification Period, it shall comply with all applicable laws, regulation, and industry standards concerning the collection, use, and protection of personal data in the United Arab Emirates;

5.1.5. During the Application Period and Certification Period, it shall not, nor shall its personnel, representatives or subcontractors, offer, provide, demand or accept any illegal or improper commission, gift, financial or moral benefit or inducement from or to any person or party in connection with the Certification or with intent to influence DESC, the Certifying Body or their personnel;

5.1.6. During the Application Period and Certification Period, it shall not, nor shall its personnel, representatives or subcontractors, transfer, transmit, process or store any Confidential Information in any manner at any location outside the UAE;

5.1.7. During the Application Period and Certification Period, it shall not, nor shall its personnel, representatives or subcontractors, misuse, abuse or otherwise do any unauthorised act with respect to any materials, equipment or Confidential Information of DESC, the Certifying Body or any Requesting Entity;

5.1.8. During the Application Period and Certification Period, it shall not, nor shall its personnel, representatives or subcontractors, cause or attempt to cause any harm,

damage or loss to DESC, the Certifying Body, any Requesting Entity, their personnel, the Government of Dubai or the public interest in any manner;

5.1.9. It recognises the goodwill attached to the names of DESC, the Certifying Body, the Requesting Entity and the Government of Dubai and shall, during the Application Period and Certification Period, not knowingly or negligently take or do any action or permit or suffer any omission that would be detrimental to or adversely affect the goodwill associated with names of DESC, the Certifying Body, the Requesting Entity or the Government of Dubai or create unfavourable publicity or bring disrepute to DESC, the Certifying Body, the Requesting Entity or to the Government of Dubai at any time. It undertakes to uphold the goodwill, reputation and image of DESC, the Certifying Body, the Requesting Entity and the Government of Dubai at all times;

5.1.10. During the Application Period and Certification Period, it shall not, and it shall ensure that its personnel, representatives and subcontractors shall not, misuse, abuse or otherwise do any unauthorised act with respect to any materials, systems, software, equipment, infrastructure, networks or Confidential Information belonging to DESC, the Certifying Body or any Requesting Entity;

5.1.11. During the Application Period and Certification Period, it is not subject to any contractual or other restriction imposed on him/her which may prevent or materially impede the Applicant or the Certified Service Provider from meeting his/her obligations in respect of the CyberForce Certification Program;

5.1.12. During the Application Period and Certification Period, it shall conduct itself in an open and collaborative manner consistent with the aims of the CyberForce Certification Program and shall share information, ideas and learnings with DESC and the Certifying Body in an open and transparent manner;

5.1.13. During the Application Period and Certification Period, it shall behave in a professional and respectful manner towards DESC, the Certifying Body, the Requesting Entity, all employees and personnel of DESC and the Certifying Body, the Requesting Entity and the Government of Dubai and shall comply with the laws and respectfully observe the culture and ethics of the United Arab Emirates;

5.1.14. During the Application Period and Certification Period, it will not engage in any conduct that may harm the reputation, credibility, or integrity of the CyberForce Certification Program, DESC, the Certifying Body or any Requesting Entity;

5.1.15. During the Certification Period, it shall only use the certificate issued by DESC or the Certifying Body, logo, or other approved identifiers in accordance with DESC and the Certifying Body's guidelines and policies;

5.1.16. During the Certification Period, it shall comply with the CyberForce Certification Program requirements, codes of conduct, or any additional requirements established by DESC or the Certifying Body;

5.1.17. During the Certification Period, it shall participate in audits, inspections, or re-evaluations as required by DESC or the Certifying Body to verify ongoing compliance with the CyberForce Certification Program requirements;

5.1.18. During the Certification Period, it shall promptly (and in any event no later than 24 hours) report any changes, incidents, or circumstances that may impact their continued compliance with the CyberForce Certification Program requirements to DESC and the Certifying Body in writing; and

5.1.19. During the Certification Period, it commits to report the results of each Regulated Service with the Requesting Entity to DESC in writing in accordance with the CyberForce Program Guidelines.

5.2. In relation to physical attendance at the premises of DESC, the Certifying Body or the Requesting Entity, during the Application Period and Certification Period, each Applicant or Certified Service Provider: (I) must comply with all health and safety rules and regulations and any other reasonable security requirements that apply at the relevant premises; (II) shall not misuse, abuse or otherwise do any unauthorised act with respect to any materials, furnishings, equipment or hardware at the relevant premises; and (III) accepts that the safety of the Applicants or Certified Service Provider's personal possessions are their sole responsibility and DESC, the Certifying Body or the Requesting Entity shall not be responsible nor liable for anything that is lost or stolen at the premises.

5.3. During the Application Period and the Certification Period, each Applicant or Certified Service Provider shall be responsible and liable for any loss, damages or costs including any damage to DESC, the Certifying Body or the Requesting Entity's facilities, furnishings, premises and equipment, arising out of or in connection with any breach by the Applicant or Certified Service Provider of these Program Terms or any act or omission, including negligence or wilful misconduct of the Applicant or the Certified Service Provider. If any such breach, violation or non-compliance constitutes a violation of criminal and civil laws, DESC and the Certifying Body reserve the right to take legal action against the Applicant or Certified Service Provider including, without limitation, reporting to the relevant authority or law enforcement agency any illegal or unlawful activities.

6. Confidentiality and Publicity

6.1. Applicants and Certified Service Providers shall keep all information and materials relating to the CyberForce Certification Program, DESC, the Certifying Body and any Requesting Entity **(the Confidential Information)** in strictest confidence and shall: (I) not use the Confidential Information for any purpose other than the fulfilment of its obligations in relation to the CyberForce Certification Program; (II) not disclose the

Confidential Information to any third party or otherwise publish or make available to the public (including on social media platforms, blogs, vlogs and other means of self-publication) without the prior written consent of DESC, the Certifying Body or the Requesting Entity (as applicable); and (III) protect and treat all Confidential Information with the same degree of care as it uses to protect its own confidential information and with not less than reasonable care.

6.2. All materials and information (in whatever form) provided by DESC, the Certifying Body or the Requesting Entity to an Applicant in connection with the CyberForce Certification Program may not be copied, distributed or made available to any third parties.

6.3. Applicants and Certified Service Providers shall not issue in any media worldwide or otherwise publish or make available to the public by any means any material, images, marketing, publicity, press release, public announcement or statement referring to or associating themselves with the CyberForce Certification Program, the Certifying Body, DESC, any Requesting Entity or the Government of Dubai without the prior written agreement of DESC, the Certifying Body or the Requesting Entity (as applicable). Notwithstanding the foregoing, each Certified Service Provider shall be entitled to use the Certification Mark during the Certification Period;

6.4. Each Certified Service Provider agrees to participate in and co-operate with promotional activities relating to the CyberForce Certification Program that may be initiated and/or organised by DESC or the Certifying Body from time to time during their Certification Period;

6.5. DESC and the Certifying Body may acknowledge a Certified Service Provider's involvement with the CyberForce Certification Program at any time without prior notice. By holding a CyberForce Certificate, the Certified Service Provider provides its express consent and approval to DESC, the Certifying Body or its appointed representatives publishing details of the CyberForce Certification Program and photographs and video footage of the Certified Service Provider and the right to make further press or other public announcements, or release in any form any marketing or other publicity or releases, whether in written or oral form, relating to the CyberForce Certification Program, the Certified Service Provider and results or data of the Certified Service Provider;

6.6. By applying for the CyberForce Certification Program, each Applicant or Certified Service Provider provides its express consent for DESC and the Certifying Body to collect, use, and retain any and all information, including any personal data, submitted in connection with their application. Applicants or Certified Service Providers may withdraw their consent at any time, by providing prior written notice to DESC and the Certifying Body. If an Applicant or Certified Service Provider withdraws their consent in accordance with this Clause 6.4, they will face the following consequences: (I) if they are an Applicant, their application will be deemed ineligible and will not be considered further for the CyberForce

Certification Program; or (II) if they are a Certified Service Provider, their CyberForce Certificate will be terminated in accordance with Clause 9.1 of these Program Terms;

6.7. The Confidentiality Obligations in this Clause 6 of the Program Terms shall remain in force and effect in perpetuity, notwithstanding the termination or revocation of the Program Terms, the CyberForce Certification Program or the CyberForce Certificate, under any circumstances.

7. Data Retention and Data Security

7.1. The Applicant or Certified Service Provider will process and retain the Confidential Information for only as long as necessary to implement, administer and manage the CyberForce Certification Program, to provide services in accordance with the CyberForce Certification Program, or to comply with legal or regulatory obligations. As soon as the Applicant or Certified Service Provider no longer requires the Confidential Information for any of the above purposes, the Applicant or Certified Service Provider undertakes to remove the Confidential Information from its systems in a secure manner that protects against the unauthorised disclosure of the Confidential Information;

7.2. The Applicant or Certified Service Provider shall ensure that it has at all times sufficient technical, security and all other measures in place to protect the Confidential Information of DESC, the Certifying Body and any Requesting Entity against any potential security incident or data security breach. This shall include access controls and data management controls such as data encryption, data transfer, transport and transmission control, software patching, backup, retention and recovery procedures;

7.3. In the event of a security incident, data security breach or unauthorized access to Confidential Information, the Applicant or Certified Service Provider shall notify DESC, the Certifying Body, the Requesting Entity and any other individuals or entities impacted by the breach immediately in writing (in any event, no later than 24 hours of becoming aware) and take all appropriate remedial actions as required by applicable laws and regulations;

8. Intellectual Property

Any Intellectual Property Rights in any material provided or made available to an Applicant or Certified Service Provider for use in connection with the CyberForce Certification Program (including without limitation the names and logos of the Certifying Body, DESC and their affiliates, partners and providers and the names and logos of the Cyber Force Program Certification) shall remain vested and owned by the Certifying Body or DESC or its rightful owners/licensors and shall only be used strictly in accordance with the Certifying Body and DESC's express written instructions.

9. Termination

9.1. DESC may revoke, or terminate the CyberForce Certificate of a Certified Service Provider at any time during the Certification Period by giving written notice to the Certified Service Provider, if the Certified Service Provider: (I) fails to comply with the standards set by DESC or the Certifying Body; (II) is in breach of these Program Terms; (III) conducts itself in any way that provides DESC or the Certifying Body with the right to terminate its CyberForce Certificate in accordance with these Program Terms or the CyberForce Program Guidelines; or (IV) engages in any conduct that undermines or has the potential to undermine the integrity of the Cyber Force Program or the reputation of DESC or the Certifying Body.

9.2. Where it deems appropriate, DESC may provide the Certified Service Provider with a remedy period of 30 days to rectify or remedy any breach of the Program Terms or any failure that has resulted in the termination of its CyberForce Certificate. For the avoidance of doubt, DESC shall not be required to specify the reasons for termination, in accordance with its mandate to protect Dubai Government entities from any malicious activity.

9.3. Termination shall result in the revocation of the CyberForce Certificate from the Certified Service Provider, removal of the Certified Service Provider from the list of certified individuals/entities, and any other actions as deemed appropriate by DESC.

9.4. Upon termination of the Certified Service Provider's CyberForce Certificate, the Certified Service Provider must immediately cease using the Certification Mark or any other approved identifiers associated with the Certification.

9.5. DESC may publicly disclose the termination of the CyberForce Certificate of a Certified Service Provider.

9.6. No refunds of any fees will be issued to Certified Service Providers whose CyberForce Certificate has been revoked or terminated.

9.7. DESC may revoke any Application at any time during the Application Period by giving written notice to the Applicant, if the Applicant: (I) fails to comply with the standards set by DESC or the Certifying Body; (II) is in breach of these Program Terms; (III) conducts itself in any way that provides DESC or the Certifying Body with the right refuse its Applicant in accordance with these Program Terms or the CyberForce Program Guidelines; or (IV) engages in any conduct that undermines or has the potential to undermine the integrity of the Cyber Force Program or the reputation of DESC or the Certifying Body.

9.8. Following termination, a previously Certified Service Provider may be eligible to reapply for the CyberForce Certification Program after a period specified by DESC provided they meet the requirements and criteria set forth by DESC.

9.9. A Certified Service Provider may terminate their Cyber Force Certificate by providing a written notice to DESC requesting such termination. DESC will give effect to such termination unless the Certified Service Provider is currently providing a Regulated Service to any Requesting Entity, in which case the termination shall only take effect once the Certified Service Provider has completed the provision of any Regulated Services to any Requesting Entity. Termination by the Certified Service Provider shall result in the revocation of the Cyber Force Certificate from the Certified Service Provider, removal of the Certified Service Provider from the list of certified individuals/entities, and any other actions as deemed appropriate by DESC. No refunds of any fees will be issued to Certified Service Providers who have terminated their Cyber Force Certificate and DESC may publicly disclose the termination of the Certified Service Provider's Cyber Force Certificate.

10. Suspension

10.1. DESC may at any time with fourteen (14) days prior written notice suspend the CyberForce Certificate of a Certified Service Provider if DESC believes that the Certified Service Provider may be in breach of these Program Terms or that may have undermined or whose actions are likely to undermine the integrity of the CyberForce Certification Program.

10.2. Upon suspension of the Certified Service Provider's CyberForce Certificate, DESC will conduct an investigation and determine the appropriate course of action for the Certified Service Provider including whether it will reinstate or terminate the Certified Service Provider's CyberForce Certificate.

10.3. Reinstatement following the suspension of a Certified Service Provider's Certification will be at the sole discretion of DESC, based on the outcome of the investigation and the corrective measures taken by the suspended Certified Service Provider.

10.4. During any period of the suspension of Certified Service Provider's CyberForce Certificate, the Certified Service Provider is prohibited from using the Certification Mark or other approved identifiers and may be subject to other restrictions as deemed appropriate by DESC at its sole discretion.

10.5. Applicants acknowledge and agree that DESC may publicly disclose the suspension of the Certified Service Provider at any time.

11. Liability

11.1. The Applicant or Certified Service Provider shall indemnify and hold harmless DESC, the Certifying Body and DESC's affiliates, partners and providers and their respective personnel **(the Indemnified Persons)** from all claims, damages, liabilities, losses (including any loss of, or damage to, any property of, or injury to or death of, any person) and expenses of any kind whatsoever incurred or suffered by the Indemnified Persons arising

out of or in connection with any error or wilful or negligent act or omission by the Applicant or Certified Service Provider, and/or any breach by the Applicant or Certified Service Provider of these Program Terms, any agreement or applicable laws.

11.2. The Applicant or Certified Service Provider shall be liable for the consequence of any error, omission, lack of care or negligence on its part or on the part of its personnel, representatives and subcontractors in the performance of its obligations under these Program Terms. No enquiry, inspection, approval, decision or instruction made or given by or on behalf of DESC, the Certifying Body or any Requesting Entity on any matter related to the Program Terms shall in any way operate to exclude, absolve or release the Applicant or Certified Service Provider from any such obligation, responsibility or liability.

11.3. To the fullest extent permitted by law, DESC, the Certifying Body its affiliates, partners and providers shall not be liable to any Applicant or Certified Service Provider for any losses, claims, damages, fees, liabilities, costs or expenses suffered or incurred by any Applicant or Certified Service Provider arising under or in connection with the quality of the CyberForce Certification Program or use or rely on the CyberForce Certification Program for any other reason.

11.4. The right of DESC and the Certifying Body to be indemnified under this Clause 11 is in addition to, and not exclusive of, any other right, power or remedy provided by law or under this Agreement.

12. General

12.1. During the Application Period and Certification Period, the Applicant or Certified Service Provider may not assign, subcontract, transfer, create a charge over or otherwise dispose of any of its rights or obligations under this Agreement without the prior written approval of both the Certifying Body and DESC. Notwithstanding any such approval from the Certifying Body and DESC, the Applicant or Certified Service Provider shall continue to be liable for the performance of all obligations stipulated in this Agreement. During the Certification Period, the Certified Service Provider irrevocably and unconditionally accepts all liability for the acts and omissions of any of their subcontractors (including their respective personnel, representatives and agents) as if they were the acts and omissions of the Certified Service Provider. Nothing in these Program Terms shall prevent or restrict DESC or the Certifying Body from assigning, subcontracting, transferring, creating a charge over or otherwise disposing of any of its rights or obligations under this Agreement.

12.2. Nothing in these Program Terms shall constitute or be deemed to constitute a relationship of an agency, partnership or joint venture between DESC, the Certifying Body and any Applicant or Certified Service Provider (as applicable).

12.3. DESC and the Certifying Body makes no representation, warranty or guarantee, whether express or implied, as to the quality of the CyberForce Certification Program or

concerning any future revenue or engagement prospects of any Certified Service Provider.

12.4. If any term of these Program Terms is or becomes illegal, invalid or unenforceable, that shall not affect the legality, validity or enforceability of any other term of these Program Terms.

12.5. Any expiry or termination of the Certification Period shall not affect any accrued rights or liabilities of either party. Paragraphs 5, 6, 7, 11 and 12 shall remain in full force and effect notwithstanding any termination or expiry of these Program Terms.

12.6. These Program Terms and the relationship between DESC, the Certifying Body, any Requesting Entity, the Applicant and the Certified Service Provider (as applicable) shall be governed by the laws of the Emirate of Dubai and the applicable federal laws of the United Arab Emirates. In the event of a dispute and prior to initiating any legal proceedings, the parties agree to engage in negotiation to resolve the dispute. If the parties are unable to reach a resolution through negotiation within 30 days of the date of the dispute arising, the dispute shall be referred to and finally resolved by the Dubai Courts (as established by Law No. 3 of 1992 and referred to in Law No. 13 of 2016) who shall have exclusive jurisdiction to settle the dispute. The Applicant (as applicable) hereby unconditionally and irrevocably renounces any right it may have to challenge in any other jurisdiction or arbitral system the decision of the Dubai Courts.

[The remainder of this page is intentionally left blank].

By signing below, the Parties confirm that they have read and agree to the all the terms and conditions (including the Appendices) forming the Program Terms. The Program Terms are entered into by the Parties on the date of the last signature below:

For and on behalf of the **Dubai Electronic Security Center:**

_____

[insert name] [insert designation] [insert date]

For and on behalf of the **Certifying Body:**

_____

[insert name] [insert designation] [insert date]

For and on behalf of **[insert Applicant/Certified Service Provider details]:**

_____

[insert name] [insert designation] [insert date]