Global ACE Certification Scheme Requirements Template

Title	Global ACE Certification Scheme Requirements Template	
Reference	CSPD-5-TEMP-2-GAC Scheme Requirements-v2	
Version	2	
Approved by & Date	Lt Col Mustaffa Bin Ahmad (Retired) Senior Vice President, OCB	23/11/23 Date
Effective Date	23/11/2023	

CyberSecurity Malaysia
Level 7 Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 (0)3 8800 7999
Fax: +60 (0)3 8008 3000
http://www.cybersecurity.my

REVISION HISTORY

DATE	VERSION NO.	PREPARED BY	DESCRIPTION OF CHANGES
1/4/2021	1	PEC	Initial version
22/11/2023	2	PEC	• Changed Copyright & Statement version and Co registration no. • Changed statement in Clauses 3 - 6 to reflect changes as mentioned in Internal Audit and Document review.

REVIEW RECORDS

VERSION NO.	REVIEWED BY	DATE
1	PEC	1/4/2021
2	PEC/QM	22/11/2023

CONTENTS

COPYRIGHT AND CONFIDENTIALITY STATEMENT

Registered office:

Level 7 Tower 1 Menara
Cyber Axis Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan MALAYSIA

Registered in Malaysia —
Company Limited by Guarantee Company No. 200601006881 (726630-U)

1 INTRODUCTION

1.1 GLOBAL ACE CERTIFICATION SCHEME(S)

1.1.1 CyberSecurity Malaysia is the certification body in Malaysia that develops and administers the Global ACE Certification scheme(s) to certify and recognise the cybersecurity workforce.

1.1.2 CyberSecurity Malaysia's Global ACE Certification Committee independently oversees all Global ACE certification scheme(s) and is responsible for essential decisions related to certification standards, policies, and procedures. The Committee is committed to the development, delivery and implementation of certification policies and programs that are applied consistently and are fair, impartial, and hold all individuals to the same standard.

1.2 TERMINOLOGY

1.2.1 For the purpose of this document, individuals who register for Global ACE certification scheme(s) are considered "Applicants". Applicants that submit complete documentation which contains details to take the examination and fulfil all registration requirements are granted "Candidate" status.

1.3 CDFFR CERTIFICATION (SCHEME)

1.3.1 The Certified Digital Forensics First Responder (CDFFR) certification scheme has been developed to include all the process and tasks needed to evaluate knowledge and skills for individuals who seek certification for digital forensics first responder.

1.3.2 CDFFR certification scheme is aligned with the KSA Descriptor that contains digital forensics first responders' tasks description and required knowledge and skills to perform the tasks. The KSA Descriptor for digital forensics first responders is available in Annex A.

1.3.3 CDFFR certificate holders are recognized as qualified and capable professionals to effectively perform the identification, collection, acquisition and preservation of potential digital evidence in accordance to the International Standard ISO/IEC 27037 - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence.

1.3.4 CDFFR certification program is available to all individuals who fulfils the following CDFFR certification requirements:

- Successfully complete and pass the CDFFR examination.
- Adhere to the Code of Ethics.
- Adhere to the Recertification Requirements

1.3.5. There are four main steps to obtain and maintain CDFFR certification as depicted in Figure 1. Detailed description of each step is available throughout this document.

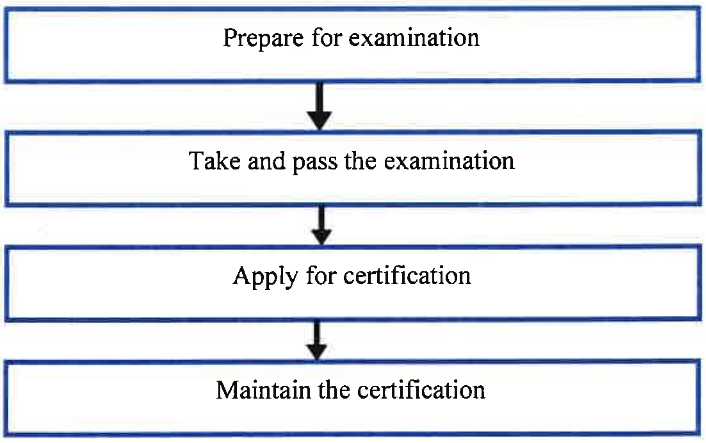

Figure 1. Steps to obtain and maintain CDFFR certification.

2 PREPARE FOR EXAMINATION

2.1 TRAINING AND EDUCATION

2.1.1 It is not compulsory for CDFFR candidates to attend specific trainings prior to sitting for the examination.

2.1.2 However, candidates can enrol in the Global ACE Certification training programs offered by CyberSecurity Malaysia and its registered training providers.

2.1.3 CyberSecurity Malaysia does not state or imply that the CDFFR examination would be much simpler, easier, or less expensive, if any specific education or training services are used.

3 TAKE AND PASS THE EXAMINATION

3.1 EXAMINATION REGISTRATION

3.1.1 Examination registration is performed online. The registration form is available at https://globalace.org/certification/examination. The registration form contains information about the applicant's education, the scheme which the applicant applies to be certified and an applicant's declaration.

3.1.2 Information about the examination fees can be viewed at https://globalace.org/certification/examination.

3.1.3 There are no prerequisites to sit for CDFFR examination. Applicants may take CDFFR examination prior to meeting the certification requirements, although CDFFR designation will only be awarded after all requirements are met.

3.1.4 The registration will include the applicant agreeing to:

- Having read and understood the Certification Scheme Requirements document.
- Understanding the scope of the Certification Scheme.
- Comply with all policies regarding the confidentiality of examination content that he or she agrees to keep the examination materials secure and obey the examination rules and regulations.

3.1.5 All registration will be processed by Professional Examination Committee (PEC), and applicants must make payments within the specified time.

3.1.6 Applicants who have successfully registered (referred as "Candidates") will be notified by email and will receive a notification slip to be eligible to sit for the examination.

3.2 ASSESSMENT METHOD

3.2.1 CDFFR assessment is set as the following:

Examination	Question type	Duration
Paper 1	70 Multiple-choice questions	1hour 30 minutes
Paper 2	Practical hands-on with one case scenario	1hour 50 minutes

3.2.2 Candidates must pass both Paper 1 and Paper 2 examinations. Candidates who passed Paper 1 but did not pass Paper 2 or vice versa, will then be required to re-sit for the failed Paper.

3.2.3 CDFFR examination covers the knowledge and skills described in the Knowledge, Skills, and Attitude (KSA) document in Annex A. The KSA document reflects the most current DFFR job practice from the job analysis and involvement of technical experts in digital forensics field. The latest KSA document is available at https://globalace.org/ksa/about-ksa.

3.2.4. CDFFR examination is offered in ENGLISH language, and it is a CLOSE BOOK examination.

3.2.5 In the event there is a change in the certification scheme which requires additional assessment, the specific methods and mechanisms required will be published in the Global ACE Certification Portal.

3.3 SPECIAL ACCOMMODATIONS

3.3.1 Special accommodations may be requested during registration process and approved by CyberSecurity Malaysia before the CDFFR scheduled examination. Accommodations must be requested at least four weeks in advance prior to preferred examination date.

3.3.2 The request must be submitted with supporting documentation from a physician or other qualified professional reflecting a diagnosis of the applicant's condition and explanation of exam aids or modifications needed no later than one week prior to the scheduled test date.

3.3.3 Reasonable examination accommodations will be made at no extra chargeto applicants with documented disabilities.

3.3.4 If an accommodation request is denied, the applicant may appeal the decision by submitting a written statement to the Global ACE Certification Director explaining the reasons for the request. The appeal will be reviewed by CyberSecurity Malaysia within 30 days of receipt and the decision is final.

EXAMINATION FEES

3.4.1 Information about the examination fees can be viewed at https://globalace.org/certification/examination.

3.4.2 Applicants must make payments within the specified time.

3.4 EXAMINATION SCHEDULE AND ADMINISTRATION

3.5.1 CyberSecurity Malaysia conducts periodic examinations as scheduled in the Global ACE Certification website. The closing date in general for the CDFFR examination is 2 weeks prior to the examination day.

3.5.2 Candidates should arrive at the examination centre at least 15 minutes prior to their scheduled examination time. Late arrivals will not be admitted.

3.5.3 Candidates are required to present acceptable forms of identification (with photograph) such as:

- Malaysia National Identification Card
- Government-Issued Driver's License
- Passport or Passport Card
- Permanent Resident Visa
- Military Issued Identification Card

3.5.4 Candidates are also required to agree and accept the confidentiality requirements.

3.5.5 By default, the examination centre is CyberSecurity Malaysia. However, specific examination centre location for a candidate's examination will be included in the confirmation email from CyberSecurity Malaysia with the subject line "Global ACE Certification: Certified Digital Forensic for First Responder Examination."

3.5.6 Candidates have the opportunity to give feedback during the examination on any issues with regards to the examination. Comments can be related to a specific item or equation, the administration of the exam, or the test site conditions. Comments can be made on the feedback form provided during the examination. Candidates will not receive specific responses to their comments; however, all comments are reviewed by Quality Manager.

3.5 EXAMINATION DAY RULES

3.6.1 Candidates are not allowed to bring any type of electronic devices, any kind of food or drinks or any type of papers in the examination room.

3.6.2 Candidates suspected of cheating or other unacceptable behaviours will be subject to the disciplinary policies and procedures. Such behaviours may include, but are not limited to:

- Removing materials from the examination room
- Aiding or receiving aids from other Candidates
- Creating a disturbance
- Recording examination materials
- Posting content on any discussion forum

3.6 EXAMINATION SCORING

3.7.1 CDFFR examination is criterion-referenced examination, i.e., the passing score is set beforehand, and a candidate's performance on the examination is not compared to the performance of others taking the examination. In a criterion-referenced examination, a candidate must obtain a score equal to or higher that a predetermined passing score to pass the examination.

3.7.2 CyberSecurity Malaysia takes full responsibility to fairly review and score Candidates' examination papers.

3.7.3 A candidate must receive a minimum score of 70% to pass the examination.

3.7 RE-SIT POLICY

3.8.1 There is no limit on the number of times a candidate may re-sit an examination.

3.8.2 However, there are some limitations in terms of allowed time frame in between examination re-sit, such as:

- If a Candidate does not pass the exam on the first attempt, he/she must wait 15 days for the next attempt (1st re-sit). Fee applies.

- If a Candidate does not pass the exam on the second attempt, he/she must wait 3 months (from the initial date of the exam) for the next attempt (2nd re-sit). Fee applies.

- If a Candidate does not pass the exam on the third attempt, he/she must wait 6 months (from the initial date of the exam) for the next attempt (3rd re-sit). Fee applies.

- After the fourth attempt, a waiting period of 12 months from the last session date is required for candidate to sit again for the same examination. Fee applies.

4 APPLY FOR CERTIFICATION

4.1 GET CERTIFIED

4.1.1 Candidates who passed CDFFR examination must apply for CDFFR Certification within three-year period, starting from the date specified in the Printed Date column on the examination result slip. The application form is available at https://globalace.org/certification/form. (Portal registration/sign-in is required).

4.1.2 Candidates must meet the following certification requirements to be CDFFR certified:

- Pass the CDFFR examination within the last 3 years.
- Submit the Global ACE Certification Application Form.

4.1.3 Approval of applications may take up to 7 working days upon receipt of completed applications. Official CDFFR certificates will be issued to successful CDFFR candidates.

5 MAINTAIN THE CERTIFICATION

5.1 RECERTIFICATION REQUIREMENTS

5.1.1 The CDFFR Certification is valid for three years, beginning with the certification or recertification decision. The purpose of certification renewal is to demonstrate ongoing competency of CDFFR certificate holders.

5.1.2 The period of validity is aligned with industry standards and benchmarking against similar recognized certifications such as EC Council CHFI, SANS GCFA, and ISACA CISA. The recertification period has considered the following:

a. changes to normative documents, which is the ISO 27037.

b. the nature and maturity of the industry or field in which the certified person is working.

c. the risks resulting from an incompetent person.

d. ongoing changes in technology, and requirements for certified persons.

e. requirements of interested parties.

5.1.3 The certification is valid for three years, is aligned with industry standards and benchmarked against recognized certifications such as EC Council CHFI, SANS GCFA, and ISACA CISA.

5.1.4 CDFFR Certification is maintained by accumulating a minimum of 20 Continuing Professional Development (CPD) hours yearly with a total of 60 CPD hours within the three-year certification cycle.

5.1.5 If less than 60 CPD hours is recorded upon expiry of the CDFFR certificate, new application for examination is required and a new certificate will be issued upon fulfilment of all CDFFR certification requirements.

6 SUSPENSION

6.1.1 When a complaint of wrongdoing is received by CyberSecurity Malaysia which upon investigation appears to be intentional or due to negligence by the certificate holder, CyberSecurity Malaysia may suspend the certificate holder's certification for a specific period. CyberSecurity Malaysia will notify the certificate holder by registered mail or email at his or her last known address.

6.1.2 CyberSecurity Malaysia may establish monitoring procedures during the suspension which the certificate holder must conform to. During the time of suspension, the certificate holder must refrain from further promotion of his or her certification. If the certificate holder does not remedy the conditions of the suspension, the CDFFR certification may be withdrawn.

6.1.3 When CyberSecurity Malaysia has evidence that charges against a certified person are valid, it shall notify the certified person by registered mail or email at his or her last known address.

6.1.4 The CDFFR certificate holders will have the opportunity to present his or her defence to CyberSecurity Malaysia in writing within 21 days.

6.1.5 The suspension or revocation shall remain in effect until CyberSecurity Malaysia reviews the case. CyberSecurity Malaysia shall then uphold or lift the suspension or revocation.

6.1.6 CyberSecurity Malaysia will restore the suspended certification after the issues that have led to suspension are satisfactorily resolved or CyberSecurity Malaysia will withdraw or reduce of the scope of certification. In most cases the suspension would not exceed 6 months.

7 WITHDRAWAL

7.1.1 When a complaint is received by CyberSecurity Malaysia which upon investigation appears to be due to negligence or intentional malpractice or violation of the code of ethics, CyberSecurity Malaysia may withdraw the certificate holder's certification. In the event of withdrawal, the certificate holder must refrain from further use of all references to certified status. CyberSecurity Malaysia will notify the certificate holder by registered mail or email at his or her last known address.

7.1.2 For withdrawal cases, the certified person must re-sit the examination and re-apply the certification.

8 FEEDBACK, COMPLAINT AND APPEAL

8.1.1 CyberSecurity Malaysia gives candidates the opportunity to submit their complaints or concerns on the examination content and procedures about:

- Technical accuracy of the examination
- Fairness in the administration of the examination

8.1.2 A candidate who has a concern about administrative procedures at an examination site or who has observed a breach of security or other improper conduct may submit a complaint or concern in writing to the CyberSecurity Malaysia within five working days after taking the examination. The candidate must include email and other contact information.

8.1.3 A candidate who has a question or concern about the reliability, validity, or fairness of the examination may submit a complaint or concern in writing to the CyberSecurity Malaysia within 10 working days after the examination' date.

8.1.4 Complaints must be submitted in written to the Quality Manager at info@globalace.org. The details and steps to submit a complaint is available at https://globalace.org/faq.

8.1.5 Candidates or certified persons may file an appeal against the decisions taken by CyberSecurity Malaysia (e.g.: withdrawal of certification due to violation of code of ethics). Appeals must be submitted in writing within 30 days of the notice of decisions.

8.1.6 Candidates are not allowed to appeal against the results of multiple-choice examinations.

8.1.7 Candidates who passed the examination are not allowed to challenge their examination results, or request for a retest to try to improve their scores.

8.1.8 Appeals must be submitted in written to the Quality Manager at info@globalace.org. The details and steps to submit appeals is available at https://globalace.org/faq.

9 USE OF CERTIFICATE CREDENTIAL

9.1.1 CDFFR certificate holders must adhere to the Global ACE Code of Ethics in Annex B.

9.1.2 CDFFR certificate holders may identify themselves as:

[Name], Certified Digital Forensics First Responder

or

[Name], CDFFR

The name and acronym above may only be used in connection with a certified individual only.

9.1.3 CDFFR certificate holders must comply with all recertification requirements to maintain use of the credential.

9.1.4 Individuals who fail to maintain the certification or whose certification is suspended or revoked must immediately discontinue use of the credential and are prohibited from stating or implying that they hold the certification.

10 CONTACT INFORMATION

For further information, contact us at https://globalace.org/contact-us.