Issue Date: December 18th, 2023

EC-Council

CHFI Candidate Handbook v6

Policy Alignment: ISO 17024 Standard

Table of Contents

Policy Alignment: ISO 17024 Standard

Objective of C|HFI Candidate Handbook

The C|HFI Candidate Handbook outlines the following:

a. Impartiality and objectivity is maintained in all matters regarding certification.

b. Fair and equitable treatment of all persons in certification process.

c. Provide directions for making decisions regarding granting, maintaining, renewing, expanding and reducing EC-Council certification/s

d. Understand boundaries/limitations and restrictions of certifications.

About EC-Council

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and information security skills. It is the owner and creator of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), EC-Council Certified Security Analyst (ECSA), License Penetration Tester (LPT) certifications and as well as many other certifications that are offered in over 194 countries globally.

The EC-Council mission is "to validate information security professionals who are equipped with the necessary skills and knowledge required in a specialized information security domain that will help them avert a cyber conflict, should the need ever arise." EC-Council is committed to uphold the highest level of impartiality and objectivity in its practices, decision making, and authority in all matters related to certification.

Individuals who have achieved EC-Council certifications include those from some of the finest organizations around the world such as the US Army, the FBI, Microsoft, IBM and the United Nations.

Many of these certifications are recognized worldwide and have received endorsements from various government agencies including the US Federal Government via the Montgomery GI Bill, National Security Agency (NSA) and the Committee on National Security Systems (CNSS). Moreover, the United States Department of Defense has included the CEH program into its Directive 8570, making it as one of the mandatory standards to be achieved by Computer Network Defenders Service Providers (CND-SP).

EC-Council has also been featured in internationally acclaimed publications and media including Fox Business News, CNN, The Herald Tribune, The Wall Street Journal, The Gazette and The Economic Times as well as in online publications such as the ABC News, USA Today, The Christian Science Monitor, Boston and Gulf News.

For more information about EC-Council | Certification,
please visit **https://cert.eccouncil.org/**

WHAT IS THE C|HFI CREDENTIAL?

Digital forensic practices stem from forensic science, the science of collecting and examining evidence or materials. Digital or computer forensics focuses on the digital domain including computer forensics, network forensics, and mobile forensics. As the cyber security profession evolves, organizations are learning the importance of employing digital forensic practices into their everyday activities. Computer forensic practices can help investigate attacks, system anomalies, or even help System administrators detect a problem by defining what is normal functional specifications and validating system information for irregular behaviors.

In the event of a cyber-attack or incident, it is critical investigations be carried out in a manner that is forensically sound to preserve evidence in the event of a breach of the law. Far too many cyber-attacks are occurring across the globe where laws are clearly broken and due to improper or non-existent forensic investigations, the cyber criminals go either unidentified, undetected, or are simply not prosecuted.

Cyber Security professionals who acquire a firm grasp on the principles of digital forensics can become invaluable members of Incident Handling and Incident response teams. The Computer Hacking Forensic Investigator course provides a strong baseline knowledge of key concepts and practices in the digital forensic domains relevant to today's organizations. CHFI provides its attendees a firm grasp on the domains of digital forensics.

Why CHFI?

- It is designed and developed by experienced subject matter experts and digital forensics practitioners
- CHFI is a complete vendor neutral course covering all major forensics investigations technologies and solutions
- CHFI has detailed labs for hands-on learning experience. On an average, approximately 50% of training time is dedicated to labs
- It covers all the relevant knowledge-bases and skills to meet with regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- The student kit contains large number of white papers for additional reading
- The program presents a repeatable forensics investigation methodology required from a versatile digital forensic professional which increases employability
- The student kit contains several forensics investigation templates for evidence collection, chain-of custody, final investigation reports, etc.
- The program comes with cloud-based virtual labs enabling students to practice various investigation techniques in a real-time and simulated environment

CHFI Testimonials

"CHFI training was extremely helpful to understand the issues in Cyber Forensics field. Applying these to a specific issue that I am dealing with helped me get past a big hurdle. Thank you!

- Chaitanya Tottadi, CEH, CHFI

"Not only did this experience teach me the proper techniques of ethical hacking and the proper process of penetration testing as promised, but it also taught me how to learn independently, how to stick with a problem and find ways of solving it, and perhaps most significantly, the experience taught me the skills that will enable me to continue to develop my security knowledge beyond this certification.

- Solly Bopape

"For me, Certified Hacking Forensic Investigator (CHFI) is a useful tool to gain a better understanding of Digital Forensic and obtain such digital evidence to further verify all forms of fraud and corruption.

- Tumpal Wagner Sitorus

"There is a procedures and processes to follow when a hack occurs. Didn't know that? Well you will after this course. The course takes you through exactly that, step by step. Virtual Labs are absolutely amazing.

- Tevendren Padayachee (TEV)

"CHFI provides individuals with the technical, legal, and procedural knowledge needed to prepare for, and pursue, a rewarding career in a field where professionals of their kind are always in demand.

- Aaron P. Family

"I completed the CHFI program. The course and tools for the class are highly organized. The labs are amazingly sophisticated and give you ample time to finish. The courseware, media and documents are of a very high quality and extremely well prepared. We contacted a few departments of EC-Council in the due course of the programs for support and the staff is very helpful and quick to respond. I found the content in sync with the current trends in cyber security and close to real life situations. Maybe they can bring in the future some Wi-Fi, web cameras or even their own cyber city!

- Michelle

"The training content that EC-Council designed is the best and beyond my expectations. Honestly, the entire exercise gave me confidence to deal with cyber-crime and understand cyber security domain. Hope EC-Council will do a lot of cool new things in future.

- Muntashir Islam

"It is my pleasure to take the time to praise the EC-Council for having such a magnificent class, specifically THE Computer Hacking Forensic Investigator course. The course had an abundance of information, utilities, programs, and hands on experience. I am a consultant at Dell and we do have a lot of technical training, but I must comment that this one is one of the best trainings I have seen in several years. I will definitively recommend this course to all my colleagues.

- Hector Alvarez

“It’s a great honor to praise the EC-Council for having such fantastic certifications. The CHFI course has a lot of information and solid security engineering practices. I am an Operations Manager & Data Recovery Engineer at Disk Doctors, one of the world known Data recovery companies and do have a lot of on hand Data Recovery practices, but I must comment that this one is one of the best courses I have seen in several years. EC-Council training and methodologies have given me an upper hand to effectively and efficiently determine the forensic problems involved in the advancing Data Recovery business.

With data storage devices becoming the integral part of everyday life, forensic science has entered the dimension of bits & bytes. Forensic analysis of Data Storage devices involves the identification, preservation, discovery, retrieval, & reporting of digital evidence from any type of digital media storage devices containing valuable and sensitive information.

My CHFI certification is also an astonishing asset to my Microsoft, Cisco and CompTIA certifications plus qualities of this EC-Council course have certainly assisted my Data Recovery work because of the great in-depth detail they have. I'm certainly a much better forensic advisor and consultant in my Data Recovery field than what I was before which definitely puts a plus point for the company on the international market.

- Aziz Mirza

For latest C|HFI Testimonials, please visit **https://cert.eccouncil.org/chfi-testimonials.html**

Steps to Earn the ANAB-accredited C|HFI credential

Candidates will be granted the Computer Hacking Forensic Investigator credential by passing a proctored CHFI exam. The exam will be for 4 hours with 150 multiple choice questions.

The ANAB-accredited CHFI exam is available at VUE and EC-Council Test Centers. Please contact https://eccouncil.zendesk.com/anonymous_requests/new to provide you with the locations of the nearest test centers that proctor the ANAB-accredited CHFI exam.

You will be tested in the following domains of digital forensics:

Domains
Forensic Science
Regulations, Policies and Ethics
Digital Evidence
Procedures and Methodology
Digital Forensics
Tools/Systems/Programs

If you are interested in knowing the objectives of the ANAB-accredited CHFI exam, or the minimum competencies required to pass the ANAB-accredited CHFI exam, please refer to Appendix A: ANAB-accredited CHFI Exam Blueprint.

Upon successfully passing the exam you will receive your digital ANAB-accredited CHFI certificate within 7 working days.

The CHFI credential is valid for a 3-year period but can be renewed each period by successfully earning EC-Council Continued Education (ECE) credits. Certified members will have to achieve a total of 120 credits (per certification) within a period of three years.

All EC-Council-related correspondence will be sent to the email address provided during exam registration. If your email address changes notify EC-Council by contacting us at https://eccouncil.zendesk.com/anonymous_requests/new ; failing which you will not be able to receive critical updates from EC-Council.

To Attempt the CHFI Exam

In order to be eligible to attempt the CHFI certification examination, you may:-

A. Completed Official Training

Candidates who have completed the official CHFI instructor-led training (ILT), online live training, academic learning or has been certified in a previous version of the credential.

Prior to attempting the exam, you are required to AGREE to:

a. EC-Council Non-Disclosure Agreement terms
b. EC-Council Candidate Certification Agreement terms

You should NOT attempt the exam unless you have read, understood and accepted the terms and conditions in full. BY ATTEMPTING THE EXAM, YOU SIGNIFY THE ACCEPTANCE OF THE ABOVE-MENTIONED AGREEMENTS available on Appendix B. In the event that you do not accept the terms of the agreements, you are not authorized by EC-Council to attempt any of its certification exams.

B. Attempt Exam without Official Training

In order to be considered for the EC-Council certification exam without attending official training, candidate must:

a. Have at least two years of work experience in the Information Security domain.
b. Remit a non-refundable eligibility application fee of USD 100.00
c. Submit a completed Exam Eligibility Application Form.
d. The voucher purchase link will be sent upon application approval.

You need to fill the complete eligibility form and email it to eligibility@eccouncil.org for approval and remit USD100 eligibility fee through our webstore at https://store.eccouncil.org. Once approved, the applicant will be send instructions on purchasing a voucher from EC-Council directly. EC-Council will then send the candidate the voucher code which candidate can use to register and schedule the test.

1. ELIGIBILITY PROCESS

a. Applicant will need to go to *https://cert.eccouncil.org/Exam-Eligibility-Form.html* to fill in an online request for the Eligibility Application Form.
b. Applicant will receive an electronic Exam Eligibility Application Form and the applicant will need to complete the information required on the form.
c. Submit the completed Exam Eligibility Application form. The application is valid only for 90 days from the date when application is submitted. Should we not receive any update from the applicant post 90 days, the application will be automatically rejected. Applicant will need to submit a new application form.
d. On an average an application processing time would be between 5-10 working days once the verifiers on the application respond to EC-Council's requests for information. Should the applicant not hear from us after 5 working days, the applicant can contact *eligibility@eccouncil.org*
e. EC-Council will contact applicant's Boss/ Supervisor/ Department head, who have agreed to act as applicant's verifier in the application form, for authentication purposes.

For verification of educational background EC-Council requires a letter in written in either physical or electronic format confirming the certification(s) earned by the candidate.

a. If application is approved, applicant will be required to purchase a voucher from EC-Council DIRECTLY. EC-Council will then send the candidate the voucher code which candidate can use to register and schedule the test at EC-Council Test Centers.
b. The approved application stands valid for 3 months from the date of approval, the candidate needs to test within 1 year from date of voucher release.
c. An application extension request will require the approval of the Director of Certification.
d. If application is not approved, the application fee of USD 100 will not be refunded.

- ◯ CEH (Certified Ethical Hacker)
- ◯ CHFI (Computer Hacking Forensic Investigator)
- ◯ CND (Certified Network Defender)
- ◯ CCSE v2 (Certified Cloud Security Engineer v2)
- ◯ CTIA v1 (Certified Threat Intelligence Analyst v1)
- ◯ CASE-JAVA v1 (Certified Application Security Engineer - Java v1)
- ◯ CASE-.Net v1 (Certified Application Security Engineer - .Net v1)
- ◯ EDRP v3 (EC-Council Disaster Recovery Professional v3)
- ◯ ECDE v1 (EC-Council Certified DevSecOps Engineer v1)

Eligibility Requirements

In line with the ANAB ISO 17024 standard, either one of the following criteria is required by EC-Council to determine a candidate's eligibility.

a) A Candidate has completed "Official" training through an EC-Council Authorized Training Center (ATC). Accepted "Official" training solutions: ATC Instructor-Led (ILT) or Academic Learning.

Or

b) A Candidate may be granted permission to attempt the exam without "Official" training if:
   i) The Candidate has and can prove two years of Information Security related experience.* and;
   ii) The Candidate remits a non-refundable Eligibility Application Fee of $100 (USD) and;
   iii) The application must be approved by EC-Council.

Steps for Eligibility Application

Step 1: Complete the Application Form.
Step 2: Attach a copy of your updated resume.
Step 3: Send the application form and resume to eligibility@eccouncil.org
Step 4: Pay Eligibility Application Fee of USD100 (Non-refundable). For payment, click here.
Step 5: EC-Council will contact your nominated verifier for information validation.
Step 6: Eligibility Application Decision:

a. If your application is approved, you will be required to purchase the exam voucher directly from the EC- Council store. You will receive your exam voucher from EC-Council Certification Department within two working days of payment realization.
b. If your application is rejected, you will receive an email from the EC-Council Certification Department stating the reasons for rejection.

Confidentiality Of Information: We treat personal information securely and confidentially. EC-Council adheres to the data and privacy laws and will not disclose the submitted information to any third party except for disclosing the information with your verifier.

Disclaimer: EC-Council reserves the right to deny certification to any candidate who attempted the exam without qualifying as per the mentioned eligibility criteria. Should the EC-Council audit team discover that a certificate was granted to a candidate who attempted the exam and did not qualify as per the eligibility criteria, EC-Council reserves the right to revoke the certification for such candidates and or pursue legal action.

Retention Of Documentation: EC-Council will not retain any supporting documents related to the application beyond a period of 90 days from the date of receipt.

Special Accommodation: Should you have a special accommodation request, you can write to us at certmanager@eccouncil.org, for more information on our special accommodation policy please refer to https://cert.eccouncil.org/special-accommodation-policy.html

Applicant Information (To be filled by the applicant)

First Name: Last Name:

Email Address:

Mailing Address:

City: Country: Zip/Postal Code:

Experience Qualifications

Company Name:

Company Website:

Job Title / Position:

Total number of years of experience in IT Security Domain:

Number of years of IT Security related work experience with the current employer:

Supervisor Name & Email Address: Position:

Statement of Compliance

The objective of EC-Council's certifications is to introduce, educate and demonstrate hacking techniques and tools for legal security testing purposes only. Those who are certified by EC-Council any of our various "Hacking" disciplines, acknowledge that such certification is a mark of distinction that must be both earned and respected.

In lieu of this, all certification candidates pledge to fully support the Code of Ethics. Certified professionals who deliberately or intentionally violate any provision of the Code will be subject to action by a review panel, which can result in the revocation of the certification.

To this end, you will not exploit the thus acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to illegally compromise any computer system. Additionally you agree to indemnify EC-Council and its partners with respect to the use or misuse of these tools, regardless of intent. You agree to comply with all applicable local, state, national and international laws and regulations in this regard.

I certify that I meet the experience and training requirements to apply to become certified in EC-Council's various "Hacking" certification discipline's. The information contained in this application is true and correct to the best of my knowledge. I understand that if I engage in any inappropriate, unethical, or illegal behavior or activity, my certification status can be terminated immediately.

By submitting this form to EC-Council, you agree to indemnify and hold EC-Council, its corporate affiliates, and their respective officers, directors and shareholders harmless from and against any and all liabilities arising from your submission of Personally Identifiable Information (such as passport, government ID, social security number etc) to EC-Council. Should EC-Council receive any Personally Identifiable Information attached to this application, this application will be rejected.

I do hereby state that all the details mentioned above are true and accurate to the best of my knowledge

Agree Disagree

Signature: _____ Date: _____

Print Form

If you submit this application form electronically, please do not forget to attach the requested documents. Also, by clicking agree and typing your name in the signature slot, you agree to comply with the statement of compliance. If you choose to print your application form, please sign with your original signature to secure your compliance.

*Cumulative experience is acceptable. (IT Security experience does not need to be in current job, or in one job)
**If self-employed, please submit letter from at least one client describing your IT Security contribution to their business.

Retakes & Extensions

EC-Council Exam Retake Policy

If a candidate does not successfully pass an EC-Council exam, he/she can purchase ECC Exam center voucher to retake the exam at a discounted price.

a. If a candidate is not able to pass the exam on the first attempt, no cooling or waiting period is required to attempt the exam for the second time (1st retake).

b. If a candidate is not able to pass the second attempt (1st retake), a waiting period of 14 days is required prior to attempting the exam for the third time (2nd retake).

c. If a candidate is not able to pass the third attempt (2nd retake), a waiting period of 14 days is required prior to attempting the exam for the fourth time (3rd retake).

d. If a candidate is not able to pass the fourth attempt (3rd retake), a waiting period of 14 days is required prior to attempting the exam for the fifth time (4thd retake).

e. A candidate is not allowed to take a given exam more than five times in a 12-month (1 year) period and a waiting period of 12 months will be imposed before being allowed to attempt the exam for the sixth time (5th retake).

f. Candidates who pass the exam are not allowed to attempt the same version of the exam for the second time.

EC-Council strongly advises candidate who fail the exam for the third time (2nd retake) to attend official hands-on training that covers the certification objectives.

EC-Council reserves the right to revoke the certification status of candidates who attempt the exam without abiding to EC-Council retake policy as stated above.

Extension Policy

EC-Council exam vouchers are valid for a maximum period of one year from the date of purchase. A candidate may opt to extend his/her EC-Council exam vouchers for an additional 3 months for $35 if the voucher is valid (not used and not expired). Vouchers can only be extended once.

Voucher Policy

Once purchased, EC-Council vouchers (new, retake, or extended) are non-refundable, nontransferable, and non-exchangeable. EC-Council reserves the right to revoke the certification status of candidates who attempt the exam without abiding to any of the above EC-Council voucher policies.

EC-Council Special Accommodation Policy

A candidate with disabilities is defined as a person who has a physical, sensory, physiological, cognitive and/or developmental impairment that makes it difficult or impossible to attempt EC-Council certification exams using the standard testing equipment or within the standard exam duration.

In line with EC-Council's commitment to comply with the Americans with Disabilities Act (ADA, 1991), EC-Council will accommodate reasonable requests by candidates with disabilities who would like to attempt any EC-Council certification exams. Such requests will fairly equate disabled candidates with other candidates and enable them to denote their skills and knowledge in EC-Council's exams.

The special accommodation request is evaluated based on the candidate's particular accommodation request, nature of disability, and reasonableness of the request. The request form requires a legally approved expert, practitioner, or professional in the fields of physical or mental healthcare to confirm the need for special accommodation. The request form has 2 sections:

Section 1 should be filled and signed by the candidate, and Section 2 is to be filled and signed by a legally approved professional, expert or practitioner to support the candidate's special accommodation request. The information requested by EC-Council will be held in strict confidence and will not be released without the candidate's permission.

Candidates are required to submit their special accommodation requests to EC-Council at least 30 days prior to registering for an exam. EC-Council will respond with its decision within 14 days and provide the contact details of testing center/s that have the infrastructure to accommodate the candidate's special needs.

For any details or clarification, please email to certmanager@eccouncil.org

EC-Council

Special Accommodation Request Form

Please submit the completed form to EC-Council as following:

E-mail Address	Send the form to certmanager@eccouncil.org. Please attach the form as a scanned document that includes the certifying authority's signature.

Section 1: APPLICANT INFORMATION

Name :.....

Email Address: .....

EC-Council Voucher Number (if available): .....

Please list all examinations and versions for which you are requesting accommodations:

.....

.....

.....

.....

.....

.....

.....

Signature: ..... Date: .....

EC-Council

Special Accommodation Request Form

Section 2: DOCUMENTATION OF ACCESSIBILITY NEEDS

I have known ..... since .....
(Examination applicant name) (Date)

in my capacity as a .....
(Professional title)

I have read the accompanying description of potential accessibility barriers and understand the nature of the examination(s) to be administered, and I certify that I have documentation on record supporting the need for accommodation. I believe that this applicant should be provided the following accommodations (identify relevant accommodations):

- ☐ Accessible testing site (for example, ramp for wheelchairs)
- ☐ Amanuensis (recorder of answers)
- ☐ Extended exam time—one and one-half times the usual allotment
- ☐ Extended exam time—twice the usual allotment
- ☐ Extra time for breaks (specify frequency and duration): .....
- ☐ Reader (person to read the exam items aloud)
- ☐ Separate testing room
- ☐ Special chair (specify type): .....
- ☐ Special input device, such as a trackball mouse (specify type): .....
- ☐ Special output device, such as a larger monitor (specify type): .....
- ☐ Written instruction of exam procedures
- ☐ Other (please describe in the space below):

.....

.....

.....

.....

EC-Council

Special Accommodation Request Form

Justification for accommodation (include description of condition):

.....

.....

.....

.....

.....

.....

Contact information for professional certifying accommodation needs:

Professional's Name: .....

Professional's Title : .....

Phone Number : .....

Email Address : .....

Signature: ..... Date: .....

EC-Council

Special Accommodation Request Form

POTENTIAL ACCESSIBILITY BARRIERS

Standard format for EC-Council certification exams present the following potential accessibility barriers.

Manual

Examinees must use a mouse to point-and-click, click-and-drag, navigate from one question to the next by clicking, and perform tasks in a simulated or emulated software environment. Exam question formats include multiple choice questions in which the candidate answers by clicking on the selected response(s).

Optical

Reading text: Exam questions are written at a reading level appropriate to the content. The electronic exams must be read on a 15-inch or larger monitor with at least 1024x768 resolution. The font can be as small as 9 pt. in graphics and 11 pt. in text. Graphics will be displayed on the monitor (possibly in color).

Physical Stamina

Exams last for 4 hours (standard)

If you need more information in order to decide what accommodations are necessary, please contact the EC-Council Certification Division at certmanager@eccouncil.org

ANAB-Accredited CHFI Exam Development & Exam Item Challenge

Exam development is a pivotal process that emphasizes on the technical, structural, semantic, and linguistic quality of exam items. Exam quality checks are done by a team of independent experts and professionals to ensure that the exam items are clear, error-free, unbiased and/or unambiguous.

Development Process

An invaluable input from industry experts was considered in the ANAB-accredited CHFI exam development, especially on how the CHFI qualifications and credentials are exercised worldwide. The CHFI exam is meant to meticulously and unsparingly transcend ordinary knowledge so as to reflectively gauge the necessary knowledge and skill required by experts in the domain of Computer Forensics.

Development phases

The CHFI exam development process is comprised of 9 phases that cogently focus on optimizing the exam to reflect qualities of relevance, validity and reliability.

- **Objective domain definition**

  Subject matter experts (SMEs) highlight the significant job functions of computer forensics.

- **Job analysis**

  The job analysis identifies the tasks and knowledge important to the work performed by professionals in the field of IT Security; and, creates test specifications that may be used to develop the ANAB-accredited CHFI exam. The result of a job analysis is a certification exam blueprint.

  The tasks and knowledge statements are transmuted into a survey that experts would use to rate, measure, and assess the skills and knowledge required. These ratings are used to rank the statements and determine the number of questions to stem from each exam statement.

- **Scheme Committee Approval**

  EC-Council Scheme Committee, a group of experts, inspects and validates the objective domain and the approach used in the job analysis prior to the authoring or writing of the exams.

- **Exam writing**

  SMEs write the exam items to measure the objectives stated in the exam blueprint. The exact number of exam items that they write is dependent on the feedback of the job analysis phase. The approved items are those that are technically, grammatically, and semantically clear, unbiased, and relevant.

- **Standard setting**

  A panel of experts other than those who write the items will answer and rate all items to deduce a minimum passing or cut score. Scores vary from one exam to another due to the score dependence on the items pool difficulty.

Final Scheme Committee Approval

The EC-Council Scheme Committee give their final approval of the whole process prior to the beta exam publication.

Beta exam

Once the Scheme Committee approves the scheme a beta exam is published. Candidates are to sit for the beta exam under identical conditions to the real exam. The distribution of the beta exam scores enables EC-Council to assess and calibrate the actual exam for better quality.

Final evaluation

The number and quality of items in the real live exam is determined by the scores and results of the beta exam. The analysis of the beta exam includes difficulty of items, capability of distinguishing level of candidates' competencies, reliability, and feedback from participants. EC-Council works closely with experts to continuously inspect the technical correctness of the questions and decide the pool of items that will be utilized for the live exam.

Final Exam Launch

ECC operate and oversee the administration of EC-Council certification exams in their centers around the world.

If the candidate believes that a specific part of the CHFI exam is incorrect, he/she can challenge or request evaluation of the part in question via the steps enumerated below. This should be done within three calendar days of the exam day. Such a process is necessary to identify areas of weakness or flaws in the questions but the exam itself cannot be re-scored. Nevertheless, all possible efforts are not spared to assure the candidate's satisfaction. The candidate's feedback is paramount to EC-Council certification exams.

Steps for challenging exam items

1. Fill and sign EC-Council Exam Feedback Form as detailed as possible. The detailed and clear description of the challenge will accelerate the review process. No candidate's exam item challenge of the exam's items will be considered without completing the form.

2. The form should be submitted within 3 calendar days from exam date to certmanager@eccouncil.org with the subject line typed **"Exam Item Evaluation".** Only requests received within 3 working days from taking the exams will be reviewed.

3. The candidate must fill a separate form for each exam item he/she is challenging.

4. EC-Council will acknowledge receipt of the request by email. This may include a conclusive result of the evaluation, or an estimated time for the evaluation process to be completed and results to be shared with the candidate.

EC-Council Exam Feedback Form

Use this form to describe in detail the specific reasons you are challenging an EC-Council Certification exam item. Include your contact information, registration ID, the number and name of the exam, the date you took the exam, and the location of the testing center. Please provide as much detail as possible about the item to expedite review. Your challenge will not be accepted for evaluation unless this form is complete.

Within three calendar days of taking the exam, submit this form by e-mail to **certmanager@eccouncil.org** with **"Exam Item Evaluation"** in the subject line. You must submit a separate form for each exam item you are challenging.

Your submittal will be acknowledged through e-mail. At that time, you will receive either the result of the evaluation or, if more time is needed for evaluation, an estimate of when you can expect a decision.

Full Name : .....

Email Address : .....

Exam Portal (VUE/ ECC Exam Center) : .....

Exam Voucher No : .....

Exam Name : .....

Exam Date (MM/DD/YYYY) (When did you take the exam?) .....

Test Center Name & Location : (Where did you take the exam?) : .....

Country : .....

EC-Council Exam Feedback Form

Item Description
(Describe the exam item in detail. Explain why you believe the item is not valid.)

.....

.....

.....

.....

....

Signature Date

EC-Council Certification Exam Policy

EC-Council has several exam policies to protect its certification program, including:

a. Non-Disclosure Agreement (NDA)
b. Candidate Certification Agreement (CCA)
c. Security and Integrity Policy

Non-Disclosure Agreement (NDA)

Prior to attempting an EC-Council exam, candidates are required to agree to EC-Council NDA terms. Candidates should not attempt the exam unless they have read, understood and accepted the terms and conditions in full. By attempting the exam, the candidates signify the acceptance of the NDA terms. In the event that the candidate does not accept the terms of the agreement, he/she is not authorized by EC-Council to attempt any of its certification exams.

The NDA mandates that candidates not to disclose exam content to any third party and do not use the content for any purpose that will negatively undermine the integrity and security of the certification exam. All content and wording of the exam questions is copyrighted by EC-Council under the protection of intellectual property laws.

Action will be taken against violators of their signed NDAs. EC-Council reserves the right to revoke the candidate's certification status, publish the infraction, and/or take the necessary legal action against the candidate.

Please refer to Appendix B for EC-Council NDA.

Candidate Certification Agreement (CCA)

Prior to attempting an EC-Council exam, candidates are required to agree to EC-Council CCA terms. Candidates should not attempt the exam unless they have read, understood and accepted the terms and conditions in full. By attempting the exam, the candidates signify the acceptance of the CCA terms. In the event that the candidate does not accept the terms of the agreement, he/she is not authorized by EC-Council to attempt any of its certification exams. Through passing the certification exam, successful candidates are governed through EC-Council CCA. They are authorized to provide corresponding services and to use EC-Council marks, titles and benefits pertaining to the certification program(s) that the candidate has completed. Action will be taken against violators of their signed CCAs. EC-Council reserves the right to ban candidates from attempting EC-Council exams, revoke the candidate's certification status, publish the infraction, and/or take the necessary legal action against the candidate.

Please refer to Appendix B for EC-Council CCA.

Security and Integrity

EC-Council is committed to communicating clearly what may or may not represent unethical, fraudulent, or cheating practices. We exert every effort to raise the necessary awareness among our candidates about this.

Security Policies

The policies developed and maintained by EC-Council are meant to guard the integrity, confidentiality, and value of EC-Council exams and intellectual property.

a. Candidate bans

In the case of any infringement to any rules or policies in the NDA or any misdemeanor or misuse that harms certification program in whatever way, EC-Council reserves the right to bar the candidate from any future EC-Council certification exams by EC-Council. This may also be accompanied by EC-Council decertification. Below are some examples:

- The transference, distribution, creation, trading, or selling of any derived content of the exam through means like but not limited to copying, reverse-engineering, downloading or uploading, or any other form of distribution whether electronically, verbally, or via any other conventional or unconventional means for any purpose.
- Infringing EC-Council intellectual property.
- Utilizing the exam or any of its content in any way that may be break the law.
- Not adhering to the exam retake policy
- Forgery of exam scores report or any manipulation with its content.
- Any sort of cheating during the exam including communicating with or peeking on other candidate's answers.
- The sending or receiving of any information that can be a source of any assistance not in accordance with accepted rules or standards, especially of morality or honesty.
- The use of disallowed or unauthorized materials such as cheat sheets, notes, books, or electronic devices such as tablets or mobile phones.
- The use of certain materials that have been memorized re-created to provide an almost or close exact replica of the exam, widely known as "brain dump".
- Identity impersonation when sitting for the exam.
- Not adhering to EC-Council NDA.
- Not adhering to EC-Council CPA.
- Not adhering to EC-Council exam guidelines.

b. Candidate Appeal Process

- Banned candidates have a right to appeal to EC-Council. The candidate should fill the EC-Council Appeal form in full, attach his/her exam transcript and submit it to certmanager@ eccouncil.org within 90 days from the EC-Council ban date.
- EC-Council will complete its thorough investigation in a maximum 15 working days and will contact the candidate with the final decision.
- If the candidate is not satisfied by EC-Council's decision, he/she has the right to refer his/her case to the Scheme Committee. The Scheme Committee decision is final. Please refer to the Appeal Process section for more details.

c. Exam Retake Policy

- If a candidate is not able to pass the exam on the first attempt, no cooling or waiting period is required to attempt the exam for the second time (1st retake).
- If a candidate is not able to pass the second attempt (1st retake), a waiting period of 14 days is required prior to attempting the exam for the third time (2nd retake).
- If a candidate is not able to pass the third attempt (2nd retake), a waiting period of 14 days is required prior to attempting the exam for the fourth time (3rd retake).
- If a candidate is not able to pass the fourth attempt (3rd retake), a waiting period of 14 days is required prior to attempting the exam for the fifth time (4thd retake).
- A candidate is not allowed to take a given exam more than five times in a 12-month (1 year) period and a waiting period of 12-month will be imposed before being allowed to attempt the exam for the sixth time (5th retake).
- Candidates who pass the exam are not allowed to attempt the same version of the exam for the second time.
- EC-Council strongly advises candidate who fail the exam for the third time (2nd retake) to attend official hands-on training that covers the certification objectives.
- EC-Council reserves the right to revoke the certification status of candidates who attempt the exam without abiding to EC-Council retake policy as stated above.

d. EC-Council Test Center (ETC) Closures Due to Security or Integrity Reasons

If there is a security or integrity issue with a certain testing center EC-Council may decide to suspend testing there until an investigation is complete or terminate the ETC status. EC-Council will provide affected candidates with a list of alternative test centers where they may attempt the EC-Council certification exam.

e. Candidate Retesting at Request of EC-Council

In the case of any suspicious patterns or trends on either the candidate's side or the testing center, EC- Council reserves the right to demand the candidate(s) to re-sit for the exam and/or Candidate Retest Audit (CRA) test. EC-Council will not release the certificate until the candidate passes the CRA exam comprising a different set of exam questions. If the candidate refuses to attempt the test within the 30-day time frame, EC-Council will not process the certification. The final status of the exam after the Candidate Retest Audit (CRA) test will be considered the final result. If a student fails the Candidate Retest Audit (CRA) test and wishes to retake the exam, they must purchase a retake voucher.

EC-Council has the right to ask for additional information pertaining to the experience and education background of the candidate on the grounds of verification.

f. Revoking Certifications

The infringement of any exam policies, rules, NDA, certification agreement or the involvement in misdemeanor that may harm the integrity and image of EC-Council certification program, may result in the candidate's temporary or permanent ban, at EC-Council's discretion, from taking any future EC-Council certification exams, revocation or decertification of current certifications. Such infringements include but are not limited to:

- The publication of any exam contents or parts with any person without a prior written approval from EC-Council.
- The recreation, imitation, or replication of any exam content through any means including memory recalling whether free or paid through any media including Web forums, instant messaging, study guides, etc.
- Harnessing any materials or devices not explicitly authorized by EC-Council during the exam.
- Taking out any materials that hold any exam contents outside the exam room, using for example, scratch paper, notebooks, etc.
- The impersonation of a candidate.
- Meddling with the exam equipment in an unauthorized way.
- Giving or being receptive of any assistance unauthorized by EC-Council.
- Acting in an uncivil, disturbing, mobbish, or unprofessional manner that may disregard or disrespect other candidates or exam officials during the exam.
- Communicating by whatever verbal or non-verbal means with other candidates in the exam room.
- Not adhering to EC-Council Exam Retake Policy and other candidate agreements.
- Not adhering to EC-Council Code of Ethics.
- Felony conviction in the court of law.

g. Beta Exam

- Sitting for a beta exam is only by invitation.
- Beta tests are focused on collecting data on the exam itself and are not focused on certifying you.

h. Right of Exclusion

EC-Council reserves the right of exclusion of any test centers, countries, or regions from EC-Council administering EC-Council certification exam/s.

CHFI Credential Renewal

Your CHFI credential is valid for 3 years.

To renew your credential for another 3-year period you need to update your EC-Council Continuing Education (ECE) credit account in the EC-Council Aspen portal and submit proof of your earned credits. To maintain your certification, you must earn a total of 120 credits within 3 years of ECE cycle period.

The credits can be earned in many ways including attending conferences, writing research papers, preparing for training classes in a related domain (for instructors), reading materials on related subject matters, taking an exam of a newer version of the certification, attending webinars, and many others.

If you fail to meet the certification maintenance requirements within the 3-year time frame EC-Council will suspend your certification. Your certification will be suspended for a period of 1 year unless you earn the required 120 ECE credits to maintain/renew your certification.

If you fail to meet certification maintenance requirements during the suspension period your certification will be revoked. You will need to take and pass the certification exam again to earn the certification.

If a member holds multiple certifications, credits earned will be applied across all the certifications. However, effective January 1st, 2013, each certification will have its own ECE recertification requirements within its respective 3-year ECE window.

For full details regarding the ECE Policy please refer to the next section.

EC-Council Continuing Education (ECE) Policy

1. REASONS FOR INTRODUCTION OF ECE SCHEME

All legitimate and credible certifications have a re-certification program. In fact, ANAB/ISO/IEC 17024, a quality accreditation body requires credible certification providers to have their own re-certification program. Requirement 6.5.1 states, "The certification body shall define recertification requirements according to the competence standard and other relevant documents, to ensure that the certified person continues to comply with the current certification requirements."

Continued competency can be demonstrated though many methodologies such as continuing professional education, examination (often not re-taking the original exam but an exam that would be at a higher level), or portfolios (when there is a product involved). The fact is there needs to be a time limit for the certification to ensure the consumers that the person has up-to-date knowledge.

This is why several governmental agencies are mandating accreditation of certifications in fields such as IT, Crane Operators, and Selling of Securities to the elderly.

Certification's main purpose is to "protect the public/consumers" NOT to protect the profession. When health, safety and security are at risk, certification is needed and it cannot be given for a "lifetime". It is generally noted that, if professionals are not required to maintain their knowledge and skills in their profession, they won't. Today, credible organizations within professional domains require their members to provide evidence of a continuous learning as a basis for maintaining their license.

Differentiation

The ECE will brand, differentiate and distinguish a certified member as dedicated IT Security professional if he/she is willing to continuously learn and share knowledge to keep abreast of the latest changes in technology that affects the way security is viewed, deployed and managed. This is a key requirement of employers internationally and EC-Council being a major certification organization supports it.

How does it work?

Once a candidate becomes certified by EC-Council, the relationship between EC-Council and candidate will always be governed by the EC-Council Candidate Certification Agreement which candidate must agree to, before receiving your certification. This agreement is also provided at https://cert.eccouncil.org/images/doc/EC-Council-Certification-Agreement-5.0.pdf

If a certified member earned certification/s that are included under the ECE scheme, he/she will have to achieve a total of 120 credits (per certification) within a period of three years. If a member holds multiple certifications, credits earned will be applied across all the certifications. However, effective January 1st, 2013, each certification will have its own ECE recertification requirements within its respective 3-year ECE window.

The credits can be earned in many ways including attending conferences, writing research papers, preparing for training classes in a related domain (for instructors), reading materials on related subject matters, taking an exam of a newer version of the certification, attending webinars, and many others. Qualified ECE activities must have been completed within ECE program's 3-year window and must be submitted in only one ECE 3-year window.

2. RECERTIFICATION

Effective January 1st, 2009, all EC-Council certifications will be valid for three years from the date of certification. During the three year period, the certification must be renewed by participating in EC-Council Continuing Education (ECE) Program.

For members who were certified prior to 2009, their ECE period will be from January 1st, 2009 until December 31st, 2011. For their first ECE Scheme Period (2009-2011), they are only required to meet a total of 120 ECE credits By March 31st, 2013.

Upon completion of the 3-year ECE program and meeting the requirements, the member's certification validity will be extended for another three years from the month of expiry.

EC-Council has introduced in 2018 its new ANAB-accredited version of its CHFI certification program.

3. SUSPENSION, REVOCATION & APPEAL

SUSPENSION

If the certified member fails to meet certification requirements within the 3-year time frame, EC-Council will suspend his/her certification.

Suspended members will not be allowed to use the certification logos and related EC-Council membership benefits.

Suspended members must remediate their suspension within a maximum period of 12 months from the date of the expiry of the 3 year time frame. Failing which, the member's certification and status will be revoked and the member will need to challenge and pass the certification exam again to achieve certification.

For members who were certified prior to 2009, they will be given an extended suspension deadline of March 31st, 2013.

Suspended members that subsequently meet the 120 ECE credit requirements within the specified 12 months deadline from the date of the expiry of the 3-year time frame will be reinstated as a member in good standing and can enjoy the use of their certification logo and related EC-Council benefits. However, the reinstated member will have only a reduced period to achieve another 120 ECE credits for their next recertification window. "Reduced period" refers to a time frame of 3 years less the suspension period.

REVOCATIONS

If member fails to meet certification requirements during the suspension period, he/she will have the certification revoked and will no longer be allowed to continue usage of the certification logo and related benefits. Members whose certification is revoked will be required to retake and pass the respective new exam to regain their certification.

APPEALS

Members whose certification has been suspended or revoked due to non-compliance of certification requirements may send in an appeal in writing to EC-Council. This appeal letter must be received by EC-Council within ninety (90) days of the suspension/ revocation notice, providing details of the appeal and reason(s) for non-compliance.

4. Audit Requirements

Certified members are required to maintain sufficient evidence to show your involvement in activities that earns you ECE credits.

5. Important Notice

Please note that the above is subject to change from time to time without prior notice. EC-Council reserves the right to make changes as required in order to maintain the reputation and recognition of its certifications and credentials. However, best effort will be used in informing members of changes via the website.

C|HFI CAREER PATH

If you would like to pursue your career beyond CHFI, you have many paths you can choose from:

a. If you would like to be a licensed security consultant, apply to become a Licensed Penetration Tester (LPT).

b. If you would like to become a trainer, apply to become a Certified EC-Council Instructor (CEI). (Terms & conditions apply)

c. If you would like to be a multi-domain expert, earn the Certified Ethical Hacking (CEH), Certified Threat Intelligence Analyst (CTIA), EC-Council Certified Incident Handler (ECIH) or choose from many other specialized certifications.

d. If you would like to earn a master's degree in IT Security, consider applying for the EC-Council University (ECU) Master of Security Sciences (MSS). By earning the CHFI credential you have automatically earned 3 credits towards the degree.

For more details regarding the above certifications, please visit https://cert.eccouncil.org/

Code of Ethics

1. Keep private and confidential information gained in own professional work, (in particular if it pertains to your client lists and client's personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without your client's prior consent.

2. Protect and respect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator. Disclose and report to appropriate persons or authorities' potential dangers to any e-commerce clients, the Internet community, or the public, as applicable.

3. Provide service in own areas of competence. You should be honest and forthright about any limitations of own experience and education. Ensure that the Certified Member is qualified for any project by an appropriate combination of education, training, and experience.

4. Never knowingly use software or process that is obtained or retained either illegally or unethically.

5. Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices. Use and protect the property of your clients or employers only in ways which are properly authorized, and with the owner's knowledge and consent.

6. Avoid any conflict of interest. Disclose to all concerned parties, including (without limitation) your clients, employers, EC-Council any actual or potential conflicts of interest that cannot reasonably be avoided or escaped. For the purpose of clarity, if you have participated in Item writing for any of the EC-Council certification examinations, you will not be allowed to sit for the same certification examination. Further, if you wish to be EC-Council's Consultant, you must disclose your association with EC-Council's other products and/or services and/or your association with competing products and/or services.

7. Ensure good management for any project as a Certified Member.

8. Add to the knowledge of the e-commerce profession by constant study, share the lessons of own experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.

9. Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in the Certified Member's knowledge and integrity.

10. Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.

11. Not to associate with malicious hackers or engage in any malicious activities.

12. Not to purposefully compromise or allow the client's or organization's systems to be compromised in the course of the Certified Member's professional dealings. Ensure all penetration testing activities are authorized and within legal limits.

13. Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.

14. Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.

15. Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.

16. Not to be in violation of any law of the land or have any previous conviction.

17. Make claims regarding certification only with respect to the scope for which the certification has been granted.

18. Not to use the certification in a manner as to bring EC-Council into disrepute.

19. Not to make misleading and/or unauthorized statement regarding the certification or EC-Council.

20 Discontinue the use of all trademarks as regard to the certification which contains any reference to EC-Council and/or EC-Council trademark or logo or insignia upon suspension/withdrawal of the said certification.

21. Return any certificates issued by EC-Council upon suspension/withdrawal of the certification.

22. Refrain from further promoting the certification in the event of the said certification is w ithdrawn or suspended.

23. Inform EC-Council without any undue delay of any physical or mental condition which renders the Certified Member incapable to fulfill the continuing certification requirements.

24. Maintain the certification by completing, within the time frame specified by EC-Council, all continuing certification requirements (if any) that correspond with Certified member's particular certification.

25. To not to participate in any cheating incident, breach of security, misconduct or any other behavior that could be considered a compromise of the integrity or confidentiality of any EC-Council certification examination.

ETHICS VIOLATIONS

EC-Council commitment towards ethics is the mainspring that holds all its programs, services, people and operations together. EC-Council regards ethics in earnest and from stem to stern. Corollary, EC-Council mandates and stipulates all its certified professionals, candidates, and prospective candidates to conduct themselves with the law, spirit of the law, and ethical practices that would reflect positively on clients, corporates, industries, and the society at large. The EC-Council Code of Ethics tops EC-Council mandatory standards and is a requisite and indeed a pillar of its strength.

EC-Council has an objective and fair process of evaluating cases of ethics violation. Any person/s may report an EC-Council certified professional by filling EC-Council Violation of Ethics Report form, describing clearly the facts and circumstance of the violation, and obtaining the confirmation of two verifiers who confirm that the report is true and correct. The Director of Certification has the authority to temporarily suspend a member that is suspected of violating EC-Council's Code of Ethics while the case is being brought before the EC-Council Scheme Committee.

The form will be submitted to EC-Council Scheme Committee for their review and resolution. The Committee will rule in light of substantial and sufficient evidence of ethics violation. Possible resolutions or penalties may include decertification, reprimand, warning, suspension of certification, publication of infraction and/or penalty, and lastly any possible litigation.

EC-Council will be formally notified of the Scheme Committee resolution in writing and with full details. EC-Council will notify the member/s, persons or parties concerned by email or registered mail of the Scheme Committee resolution. The Committee resolution is considered as final.

EC-Council Ethics Violation Report Form

Complaint lodged by:

Name : .....

Email Address : .....

Country : .....

EC-Council Cert ID : .....
(if applicable)

Complaint lodged against:

Name : .....

EC-Council Cert ID : .....
(if applicable)

Section of EC-Council Code of Ethics Violated:

.....

.....

A detailed description of the facts known and circumstances relevant to the complaint:

.....

.....

.....

Contact 1

Name : .....

Email Address : .....

Title/Company : .....

Country : .....

The information contained in this form is true and correct to the best of my knowledge.

.....
Signature/Date

Contact 2

Name : .....

Email Address : .....

Title/Company : .....

Country : .....

The information contained in this form is true and correct to the best of my knowledge.

.....
Signature/Date

Appeal Form v2

EC-Council

Policy Alignment: ISO 17024 Standard

EC-Council adapts the term appeal as a reference to the mechanism by which a candidate/member can request the reconsideration of an EC-Council decision or exam. The appeal applicants should fill EC-Council Appeal Form and attach all supporting evidence. For instance, if the applicant is seeking EC-Council's decision in relation to the exam, for example its equipment, materials, content, scheduling, registration, or proctoring, he/should submit EC-Council Appeal Form, EC-Council Exam Feedback form and exam transcript.

If the appeal is related to an EC-Council exam, the appeal request must be submitted to **certmanager@eccouncil.org** within seven (7) calendar days from exam date. All other appeals must be submitted to **certmanager@eccouncil.org** within sixty (60) calendar days from EC-Council's written decision. Appeals received beyond the above-mentioned timeframe would not be reviewed.

The appeal process is comprised of three primary stages:

Stage 1: EC-Council

EC-Council will inspect and scrutinize closely and thoroughly the candidate's appeal before providing a final decision. Technical issues like power outages, system crash, exam items will be forwarded to the testing companies (VUE or ECC) to advise whether there is valid grounds for appeal. EC-Council will provide the candidate with the appeal results within 30 days from receipt of candidate's appeal request.

Stage 2: Scheme Committee

While EC-Council would exert every effort to resolve all matters in a fair and objective manner, EC-Council gives the applicant the right to appeal to EC-Council Scheme Committee Board if he/she is not satisfied with EC-Council's decision. The Scheme Committee will verify the intactness of all events and processes and provide EC-Council with its final decision, and EC-Council would communicate the decision to the candidate.

The Scheme Committee meets once every quarter. Only appeal requests received at least 30 days before the meeting will be reviews at that session. Appeals received less than 30 days from the Scheme Committee meeting will be reviewed in the subsequent meeting.

Stage 3: Honorary Council

The appeal will only be put forward to the adjudication of a subcommittee of the EC-Council Honorary Council, which will comprise of no less than 3 members; if the applicant is not satisfied with the Scheme Committee final decision. The request should be submitted to https://eccouncil.zendesk.com/hc/en-us/requests/new within thirty days from the date of the Scheme Committee written decision. Appeals received beyond the 30-days timeframe would not be reviewed.

The Honorary Council meets once every year. Only requests received at least 30 days prior to the Honorary Council meeting will be review at that session. Appeals received less than 30 days from the Honorary Council meeting will be reviewed in the subsequent meeting. The decision concluded by the Honorary Council is irrefutable and is obligatory to all parties involved in the appeal.

EC-Council Appeal Form

If the appeal is related to an EC-Council exam, the appeal request must be submitted within seven (7) calendar days from exam date. All other appeals must be submitted within sixty (60) calendar days from EC-Council's written decision. Appeals received beyond the above-mentioned timeframe would not be reviewed.

Kindly submit your appeal form to **certmanager@eccouncil.org**

SECTION A

Name Details (Name given when enrolled) : .....

Email Address : .....

Are you a certified EC-Council member? If yes, please complete section B with one of your certification details.

SECTION B

EC-Council Cert ID : .....

Title of Certification : .....

Are you appealing against an EC-Council Exam? If yes, please complete Section C. If no, kindly proceed to Section D.

SECTION C

Test Centre Name : .....

Test Centre Location : .....

Exam Voucher No. .....

Date Tested : .....

EC-Council Appeal Form

SECTION D

Please provide the details of your appeal

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Candidate's Signature

*Please attach a copy of score transcript/certificate, exam item or any other documents that may support your appeal.

Change in Certification Scope

EC-Council shall, where applicable, give due notice to interested parties and certified members on changes in scope of certifications, rationale behind change, and effective dates of change. Such changes will be published on the EC-Council Certification website (https://cert.eccouncil.org).

EC-Council shall verify that each certified member complies with the changed requirements within such a period of time as is seen as reasonable for EC-Council. For instance, old versions of certification exams are retired six months from the date of official announcement of the launch of the new version of the exam. These changes will only be done after taking into consideration EC-Council Scheme Committee views.

EC-Council's Scheme Committee is a member based network of volunteers that are recognized by EC-Council as experts in the field of information security. They are carefully selected from the industry and are committed to the information security community.

More importantly, they remain an independent voice for the industry and are responsible to advise EC-Council in the development and the maintenance of key certification-related matters.

Changes may be suggested by any stakeholder of EC-Council, but changes will be verified with documented psychometric analysis conducted by experts. Psychometric analysis would be conducted to determine the certification scope every three years or sooner; whereas evaluation would be conducted every year to ensure if amendment in scope of certification is required.

EC-Council
Logo Usage

Policy Alignment: ISO 17024 Standard

EC-Council Logo Usage Guidelines

To use any of EC-Council's logos, candidate must be an EC-Council Certified Professional, EC-Council Test Center, EC-Council Accredited Training Center, or a Licensed Penetration Tester. A list of certifications can be found at https://cert.eccouncil.org/certifications.html

In this context, logo shall mean and include all logos provided by EC-Council. The logo is a trademark of EC-Council.

1. GENERAL

- Certified Member can only use the logo in its original form as provided by EC-Council.
- Certified Member must state the certification version number next to the logo such as v4, v6, v7. Certified Member may not alter, change or remove elements of the logo in any other way.
- Only ANAB-accredited certifications carry the ANAB logo", the Computer Hacking Forensics Investigator ANAB-accredited version does not carry a version number.
- Certified Member may not alter, change or remove elements of the logo in any other way.
- Certified Member may not translate any part of the logo.
- Certified Member may not use elements of the logo to be part of the design of other materials or incorporate other designs into the logo.
- Certified Member may not incorporate the logo or parts of the logo into Certified Member company name, company logo, website domain, trademark, product name and design, or slogan.
- Certified Member may not use the logo to show any form of endorsement by EC-Council.

2. INDIVIDUALS

- Certified Member may use the logo on his/her business cards, business letters, resume, Websites, emails, and marketing materials for individual service.
- Certified Member may only use the logo of the credential he/she is awarded.
- Certified Member may not use the logo if certification has been revoked or suspended
- Certified Member may not use the logo if certification term has expired/lapsed and not renewed.
- Certified Member may not display the logo to be larger or more prominent than candidate's name or company name and logo.
- Candidates who hold EC-Council 'Retired Status' may not use the logo unless the logo is used with the word 'retired'.
- Candidate may not use the logo if he/she is not certified.
- Candidate may not use the logo if he/she is still in the midst of a program and have not passed the certification exam.
- Candidate may not use the logo to show affiliation with EC-Council in any way.

3. EC-Council Test Centers (ETCs) and EC-Council Accredited Training Partners (ATPs)

- ETCs and ATP's may use the logo on their marketing materials related to EC-Council programs and certifications. ETCs and ATP's may not use the logo on any material not related to EC-Council certifications or programs.
- ETCs may not use the logo to signify any relationship or affiliation with EC-Council other than as an ETC.
- ATPs may not use the logo to signify any relationship or affiliation with EC-Council other than as an ATP.

EC-Council Logo Usage Guidelines

4. COMPLIANCE

- EC-Council may occasionally conduct surveillance audits for materials bearing the logos. Candidates are to abide by the guidelines stated above. Certified Member may be subject to sanction if he/she does not adhere to these guidelines and may have his/her certification credential suspended or revoked.
- Certified Member must immediately cease to display, advertise or use the logo upon the suspension or revocation of certification credential.

5. LOGO DETAILS

a) Color

Full Color

The colors used for the logos are red, yellow, black and white. The color codes are:

Color- Red
RGB R: 255, G: 0, B: 0

Color- Yellow
RGB R: 255, G: 255, B: 0

Black and White

The logo can also be printed in black and white due to budget restrictions. For this, the color for the wordings and background of the logo must always be reversed. That is, the wordings are in black and the background is white or the wordings are in white and the background is black.

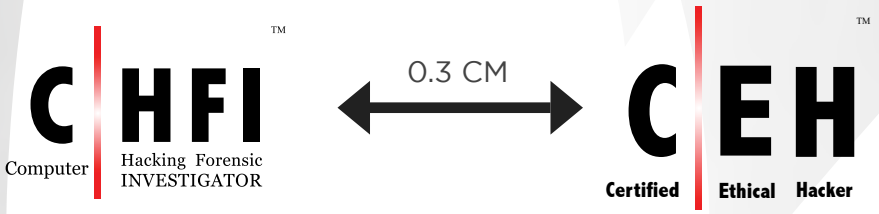
b) Size

The logo can be of any size but it must maintain all the elements of the logo without any distortions. All elements of the logo must remain legible.

EC-Council Logo Usage Guidelines

c) Spacing

The logo must not be overlapped and be fully prominent. There must be sufficient space between the logo and any other text or object. We recommend a minimum spacing of 0.3 centimeters.



d) Elements

All elements must remain in its original form. All elements of the logo must not be distorted or altered. Certified Member must ensure that the aspect ratio is maintained at all times.

e) Orientation

The logo must be presented in its upright form and not be displayed at other angles other than its horizontal layout.

f) Multiple Credentials

Individuals who attain multiple EC-Council certification credentials may display any of the logos for which certification has been achieved. Certified Member may not however, create a logo which displays a combination of all the credentials achieved. All logos must stand alone in its own right.

EC-Council Logo Usage Guidelines

6. USAGE EXAMPLES

These are examples on the usage of the logo. The usage guidelines must be strictly adhered to

a. **Business Cards:** We recommend displaying the logo on the lower left or lower right-hand side of Certified Member business card.

b. **Business Letters:** We recommend displaying the logo on the lower left or lower right-hand side of the letterhead page of Certified Member business letter.

c. **Resume:** We recommend displaying the logo on the lower left or lower right-hand side of Certified Member resume.

d. **Website:** We recommend displaying the logo at an appropriate location on Certified Member website.

e. **Email:** We recommend displaying the logo at the bottom of Certified Member email signature.

f. **Marketing Materials:** We recommend displaying the logo at an appropriate but prominent place in Certified Member marketing materials.

FREQUENTLY ASKED QUESTIONS

Should I attend training to attempt the CHFI exam?

EC-Council recommends, but not mandatory, that CHFI aspirants attend formal classroom training to reap maximum benefit of the course and have a greater chance at clearing the examinations.

What are the pre-requisites for taking a CHFI exam?

If you have completed CHFI training (online, instructor-led, or academia learning), you are eligible to attempt the CHFI examination. If you opt for self study, you must have minimum two years of work experience in the Information Security domain, submit a complete eligibility form and email it to eligibility@eccouncil.org for approval and remit USD100 eligibility fee through our webstore at https://store.eccouncil.org. Once approved, the applicant will be sent instructions on purchasing a voucher from EC-Council store directly. EC-Council will then send the candidate the voucher code which candidate can use to register and schedule the test.

What are the eligibility criteria for self-study students?

It is mandatory for you to record two years of information security related work experience and get the same endorsed by your employer.

Where do I purchase the prepaid examination vouchers?

You can purchase the vouchers directly from EC-Council through its webstore at https://store.eccouncil.org

Is the $100 application fee refundable?

No, the $100 application fee is not refundable.

I have just completed the training. Can I defer taking a test to a later date?

Yes, you can - subject to the expiry date of your exam voucher. Ensure that you obtain a certificate of attendance upon completion of the training. You may contact your testing center at a later date and schedule the exam.

For how long is the exam voucher code valid for?

The exam voucher code is valid for 1 year from the date of receipt.

Do I have to recertify?

You will need to earn EC-Council Continuing Education Credits (ECE) to maintain the certification. Go to https://cert.eccouncil.org/ece-policy.html for more information. If you require any assistance on this, please contact https://eccouncil.zendesk.com/anonymous_requests/new

Why are there different versions for the exam?

EC-Council certifications are under continuous development. We incorporate new techniques and technology as they are made available and are deemed necessary to meet the exam objectives, as students are tested on concepts, techniques, and technology. The ANAB-accredited certifications do not have an exam version number, but there will be an ANAB logo on the certificate.

How many times can I attempt the examination in case I do not?

Kindly refer to the Exam Retake Policy on our web- site at https://cert.eccouncil.org/exam-retake-policy.html

When will I get my certificate once I pass the certification examination?

Upon successfully passing the exam you will receive your digital ANAB-accredited CHFI certificate within 7 working days.

How many questions are there in the exam and what is the time duration?

The examination consists of 150 questions. The exam is of 4-hour duration.

What kind of questions can I expect in the exam?

The examination tests you on security related concepts, hacking techniques and technology. Please refer to the ANAB-accredited CHFI Test Blueprint to find out the competencies that you would be tested on.

Can I review my answers?

You can mark your questions and review your answers before you end the test.

Are there any annual continuous education fees payable?

Effective January 1st, 2016. Any member certified or recertified requires to pay continuous education fee of USD80 if he/she holds a minimum of one certificate under the ECE policy and USD20 if he/she holds certificates that are not under the ECE policy.

More details about the continuous education fee, cycle and due date can be found at https://cert.eccouncil.org/continuing-education-fees.html

How do I register my ECE credit?

Please log on to the Aspen Portal (https://aspen.eccouncil.org) to register your ECE credits.

ECE Qualifying Activities

Only IT security related events are qualified for ECE scheme such as IT seminars, reading IT security books, publishing a paper on IT Security related topics and anything that updates your knowledge on IT Security not only from EC-Council.

ECE Qualifying Events

- Association/Organization Chapter Meeting (per Meeting) – 1 credits
- Association/Organization Chapter Membership (per Association/Organization) – 3 credits
- Association/Organization Membership (per Association/Organization) – 2 credits
- Author Article/Book Chapter/White Paper – 20 credits
- Author Security Tool – 40 credits
- Authoring Book – 100 credits
- Authoring Course/Module – 40 credits
- Certification Examination Related to IT Security – 40 credits
- EC-Council Beta Exam Testing – 80 credits
- EC-Council ECE Examinations – 120 credits
- EC-Council Exam Survey – 20 credits
- EC-Council Item Writing – 3 credits
- EC-Council Job Task Analysis Survey – 40 credits
- EC-Council Review Board – 80 credits
- EC-Council Standard Setting – 60 credits
- Education Course – 1 credits
- Education Seminar/Conference/Event – 1 credits
- Higher Education Per Quarter – 10 credits
- Higher Education Per Semester – 15 credits
- Identify New Vulnerability – 10 credits
- Presentation – 3 credits
- Reading an Information Security Book/Article Review/Book Review/Case Study – 5 credits
- Teach New – 21 credits
- Teach Upgrade – 11 credits
- Volunteering in public sector – 1 credits

What certifications from EC-Council are included in the ECE system?

EC-Council Examinations (CEH, CEH (Practical), ECSA, ECSA (Practical), LPT, LPT (Master), CHFI, EISM, CCISO, CND, ECIH, EDRP, CASE, CSA, CBP, CPM, CTIA, ECES, ICS/SCADA Cyber Security, CEI, CAST, CIMP and CDM) : 120 credits.

How many credits are awarded for passing non ECE certifications?

40 ECE credits are awarded for non-ECE certifications which are listed below:
CSCU, DFE, EHE, NDE, CRM, ECSS, ENSA, Ethical Hacking Fundamentals, Secure Computer User Specialist, Network Security Fundamentals and Computer Forensics Fundamentals

Can a member holding any of the above-mentioned certification be exempted from the ECE scheme?

No.

Who can I speak to if I need more help?

If the particular event or activity is not listed on the Aspen portal, you can contact the Administrator at delta@eccouncil.org for assistance.

Can I use the certification name and logo after I pass my exams?

Yes, you can use the respective logos and labels of the certifications that you hold.

Where do I go to download the logos and guidelines?

You can download logos and usage guidelines from
https://cert.eccouncil.org/images/doc/ec-council-logo-usage-v3.0.pdf

EC-Council

CHFI Exam Blueprint v4

(New Exam Blueprint effective April 10th, 2024)

Policy Alignment: ISO 17024 Standard

Domains	Sub Domain	Description	Number of Questions	Weightage (%)
1. Forensic Science	Understand Different Types of Cybercrimes and List Various Forensic Investigation Challenges	▪ Types of Computer Crimes ▪ Impact of Cybercrimes at the Organizational Level ▪ Cyber Attribution ▪ Cyber Crime Investigation ▪ Challenges Cyber Crimes Present for Investigators ▪ Indicators of Compromise (IoC) ▪ Network and Web Application Threats and Attacks ▪ Challenges in Web Application Forensics ▪ Indications of a Web Attack ▪ What is Anti-Forensics? ▪ Anti-Forensics Techniques ▪ Challenges to Forensics from Anti-Forensics	**5**	**15%**
	Understand the Fundamentals of Computer Forensics and Determine the Roles and Responsibilities of Forensic Investigators	▪ Understanding Computer Forensics ▪ Need and Scope of Computer Forensics ▪ Why and When Do You Use Computer Forensics? ▪ Forensic Readiness and Business Continuity ▪ Forensics Readiness Planning and Procedures ▪ Computer Forensics as part of the Incident Response Plan ▪ Overview of Incident Response Process Flow ▪ Role of SOC in Computer Forensics ▪ Role of Threat Intelligence in Computer Forensics ▪ Integration of Artificial Intelligence with Digital Forensics ▪ GitOps and its Impact on Digital Forensics ▪ Forensics Automation and Orchestration ▪ Need for Forensic Investigator ▪ Roles and Responsibilities of Forensics Investigator	**6**	

Policy Alignment: ISO 17024 Standard

		▪ What makes a Good Computer Forensics Investigator? ▪ Code of Ethics ▪ Managing Clients or Employers during Investigations ▪ Accessing Computer Forensics Resources ▪ Other Factors that Influence Forensic Investigations ▪ Web Applications and Network Forensics ▪ Postmortem and Real-Time Analysis ▪ Forensics-as-a-Service (FaaS)		
	Understand Data Acquisition Concepts and Rules	▪ Data Acquisition ▪ Live Acquisition ▪ Order of Volatility ▪ Dead Acquisition ▪ Rules of Thumb for Data Acquisition ▪ Types of Data Acquisition ▪ Determine the Data Acquisition Format	**5**	
	Understand the Fundamental Concepts and Working of Databases, Cloud Computing, Emails, IOT, Malware (file, fileless, and .NET), and Dark Web	▪ Dark Web ▪ TOR Relays and TOR Bridge Node ▪ How the TOR Browser works ▪ Risks of Investigating the Dark Web ▪ Internal Architecture of MySQL ▪ Structure of Data Directory ▪ Types of Cloud Computing Services ▪ Cloud Deployment Models ▪ Cloud Computing Threats and Attacks ▪ Fundamentals of Amazon Web Services (AWS) and Google Cloud ▪ Components Involved in Email Communication ▪ How Email Communication Works ▪ Understanding Parts of an Email Message ▪ Malware and its Components	**6**	

Policy Alignment: ISO 17024 Standard

		▪ Common Techniques Attackers Use to Distribute Malware Across Web ▪ Types of Malware and their Characteristics ▪ Coordination and Management in Addressing Malware ▪ Fileless Malware ▪ Infection Chain of Fileless Malware ▪ How Fileless Attack Works via Memory Exploits, Websites, Documents, and Containers ▪ Detecting Linux memfd_create() Fileless Malware with Command Line Forensics ▪ Infection Chain of .NET Malware ▪ Analyzing .NET Malware ▪ IoT Architecture ▪ IoT Security Problems ▪ OWASP Top 10 IoT Vulnerabilities ▪ IoT Threats and Attack Surface Areas ▪ Understand OT and OT Security Problems ▪ OT Threats ▪ Understand Multimedia Basics		
2. Regulations, Policies and Ethics	Understand Rules and Regulations Pertaining to Search and Seizure of the Evidence and Evidence Examination	▪ Rules of Evidence ▪ Best Evidence Rule ▪ Federal Rules of Evidence ▪ ACPO Principles of Digital Evidence ▪ Computer Forensics vs. eDiscovery ▪ ChatGPT-4's Role in Evidence Processing, Analysis, and Production ▪ Best Practices for Handling Digital Evidence ▪ Seeking Consent ▪ Obtaining Witness Signatures ▪ Obtaining a Warrant for Search and Seizure ▪ Searches Without a Warrant ▪ Initial Search of the Scene ▪ Preserving Evidence	**5**	**10%**

Policy Alignment: ISO 17024 Standard

		▪ Chain of Custody ▪ Sanitize the Target Media ▪ Records of Regularly Conducted Activity as Evidence ▪ Division of Responsibilities		
	Understand Different Laws and Legal Issues that Impact Forensic Investigations	▪ Legal and IT Team Considerations for eDiscovery ▪ Role of Local/International Agencies during Cybercrime Investigation ▪ Legal Issues, Privacy Issues and Legal Compliance ▪ Other Laws that May Influence Computer Forensics ▪ Legal Challenges in Dealing with Malware ▪ U.S. Laws Against Email Crime: CAN-SPAM Act	**5**	
	Understand Various Standards and Best Practices Related to Computer Forensics	▪ ISO Standards ▪ ENFSI Best Practices for Forensic Examination of Digital Technology	**5**	
3. Digital Evidence	Understand the Fundamental Characteristics and Types of Digital Evidence	▪ Types of Digital Evidence ▪ Characteristics and Role of Digital Evidence ▪ Sources of Potential Evidence ▪ Understanding Hard Disk and Solid State Drive (SSD) ▪ Logical Structure of Disks ▪ RAID Storage System ▪ RAID and Virtualization ▪ NAS/SAN Storage ▪ Disk Interfaces ▪ Logical Structure of Disks	**5**	**18%**
	Understand the Fundamental Concepts and Working of Desktop and Mobile Operating Systems	▪ Booting Process ▪ Essential Windows System Files ▪ Windows Boot Process: BIOS-MBR Method and UEFI-GPT ▪ Macintosh and Linux Boot Processes ▪ Windows, Linux, and macOS File Systems ▪ MAC Forensics Data, Log Files, and Directories	**6**	

Policy Alignment: ISO 17024 Standard

		▪ Architectural Layers of Mobile Device Environment ▪ Android Architecture Stack and Boot Process ▪ iOS Architecture and Boot Process ▪ Mobile Storage and Evidence Locations ▪ Mobile Phone Evidence Analysis ▪ Data Acquisition Methods ▪ Components of Cellular Network ▪ Different Cellular Networks ▪ Cell Site Analysis: Analyzing Service Provider Data ▪ CDR Contents ▪ Subscriber Identity Module (SIM) ▪ Android and iOS File Systems ▪ Rooting of Android and Jailbreaking of iOS Devices ▪ Different Types of Network-based Evidence		
	Understand Different Types of Logs and their Importance in Forensic Investigations	▪ Types of Logon Events ▪ Event Log File Format ▪ Organization of Event Records ▪ ELF_LOGFILE_HEADER structure ▪ EventLogRecord Structure ▪ Windows 11 Event Logs and Other Audit Events ▪ Evaluating Account Management Events ▪ Log Files as Evidence ▪ Legal Criteria for Admissibility of Logs as Evidence ▪ Guidelines to Ensure Log File Credibility and Usability ▪ Ensure Log File Authenticity and Maintain Log File Integrity ▪ Implement Centralized Log Management ▪ IIS Web Server Architecture and Logs ▪ Analyzing IIS Logs ▪ Apache Web Server Architecture and Logs ▪ Apache Access and Error Logs	**6**	

Policy Alignment: ISO 17024 Standard

	Understand Various Encoding Standards and Analyze Various File Types	▪ Character Encoding Standard: ASCII and UNICODE ▪ OFFSET ▪ Understanding Hex Editors and Hexadecimal Notation ▪ Image File Analysis: JPEG and BMP ▪ Understanding EXIF data ▪ Hex View of Popular Image File Formats ▪ PDF, Word, PowerPoint, and Excel File Analysis ▪ Hex View of Other Popular File Formats	**5**	
	Understand the Fundamental Workings of WAF and MySQL Database	▪ Web Application Firewall (WAF) ▪ Benefits and Limitations of WAF ▪ Data Storage in SQL Server ▪ Database Evidence Repositories ▪ MySQL Forensics ▪ Viewing the Information Schema ▪ MySQL Utility Programs for Forensic Analysis	**5**	
4. Procedures and Methodology	Understand the Forensic Investigation Process	▪ Forensic Investigation Process ▪ Importance of the Forensic Investigation Process ▪ Setting Up a Computer Forensics Lab ▪ Building the Investigation Team ▪ Understanding the Hardware and Software Requirements of a Forensic Lab ▪ Validating Laboratory Software and Hardware ▪ Ensuring Quality Assurance ▪ Building Security Content, Scripts, Tools, or Methods to Enhance Forensic Processes ▪ First Response and First Responder ▪ First Response Basics ▪ First Response by Non-forensics Staff, System/Network Administrators, and Laboratory Forensics Staff ▪ First Responder Common Mistakes ▪ Health and Safety Issues	**5**	**17%**

Policy Alignment: ISO 17024 Standard

		▪ Documenting the Electronic Crime Scene ▪ Search and Seizure ▪ Evidence Preservation ▪ Data Acquisition and Data Analysis ▪ Case Analysis ▪ Reporting ▪ Testify as an Expert Witness ▪ Generating Investigation Report ▪ Electron Applications and Chat Application Forensics ▪ Mobile Forensics Process ▪ Mobile Forensics Report Template ▪ Sample Mobile Forensic Analysis Worksheet ▪ Social Media Forensics ▪ Social Engineering Forensics ▪ Insider Threat and Identity Theft Forensics ▪ Cryptocurrency and Blockchain Forensics ▪ Virtualization Forensics ▪ Cloud Forensics ▪ Forensic Methodologies for Containers and Microservices ▪ Bluetooth Forensics ▪ IoT Forensics ▪ OT Forensics ▪ Multimedia Forensics		
	Understand the Methodology to Acquire Data from Different Types of Evidence	▪ Data Acquisition Methodology ▪ Step 1: Determine the Best Data Acquisition Method ▪ Step 2: Select the Data Acquisition Tool ▪ Step 4: Acquire Volatile Data ▪ Step 5: Enable Write Protection on the Evidence Media ▪ Step 6: Acquire Non-Volatile Data ▪ Step 7: Plan for Contingency ▪ Step 8: Validate Data Acquisition ▪ Data Acquisition Guidelines and Best Practices ▪ Collecting Volatile Information and Non-Volatile Information	**5**	

Policy Alignment: ISO 17024 Standard

		▪ Live Mac Data Collection - Imaging, RAM and Volatile Data ▪ Collecting Volatile Database Data ▪ Collecting Primary Data Files and Active Transaction Logs Using SQLCMD ▪ Collecting Primary Data Files and Transaction Logs ▪ Collecting Active Transaction Logs Using SQL Server Management Studio ▪ Collecting Database Plan Cache ▪ Collecting Windows Logs ▪ Collecting SQL Server Trace Files and Error Logs ▪ Data Acquisition in the Cloud ▪ Data Acquisition on OT Systems		
	Understand the eDiscovery Process	▪ eDiscovery Process Flow ▪ Electronic Discovery Reference Model (EDRM) Cycle ▪ Monitor and Maintain Accurate Metrics and Detailed Tracking Information Related to eDiscovery ▪ eDiscovery Collections/Methodologies ▪ eDiscovery Best Practices to Mitigate Costs and Risk	**5**	
	Illustrate Image/Evidence Examination and Event Correlation	▪ Getting an Image Ready for Examination ▪ Viewing an Image on Windows, Linux, and Mac Forensic Workstations ▪ Windows Memory Analysis and Registry Analysis ▪ Extracting Additional Windows OS Artifacts ▪ File System Analysis Using Autopsy and The Sleuth Kit (TSK) ▪ File System Timeline Creation and Analysis ▪ Types of Event Correlation ▪ Event Deconfliction ▪ Timeline and Kill Chain Analysis ▪ Prerequisites of Event Correlation ▪ Event Correlation Approaches	**6**	

Policy Alignment: ISO 17024 Standard

		▪ Collecting and Analyzing macOS Artifacts ▪ Analyzing macOS User Activities ▪ Cloud Digital Evidence Analysis		
	Explain Dark Web and Malware Forensics	▪ Dark web forensics ▪ Information Found on the Dark Web ▪ Safety Precautions while Exploring the Dark Web ▪ Identifying TOR Browser Artifacts: Command Prompt, Windows Registry, and Prefetch Files ▪ Malware Forensics ▪ Why Analyze Malware? ▪ Malware Analysis Challenges ▪ Identifying and Extracting Malware ▪ Malware Forensic Artifacts and Indicators ▪ Prominence of Setting up a Controlled Malware Analysis Lab ▪ Preparing Testbed for Malware Analysis ▪ Supporting Tools for Malware Analysis ▪ General Rules for Malware Analysis ▪ Documentation Before Analysis ▪ Types of Malware Analysis	**5**	
5. Digital Forensics	Review Various Anti-Forensic Techniques and Ways to Defeat Them	▪ Anti-Forensics Technique: Data/File Deletion ▪ What Happens When a File is Deleted in Windows? ▪ Recycle Bin in Windows ▪ File Carving ▪ Anti-Forensics Techniques: Password Protection, Steganography, Alternate Data Streams, Trail Obfuscation, Artifact Wiping, Overwriting Data/Metadata, Encryption, Program Packers, Exploiting Forensics Tools Bugs and Detecting Forensic Tool Activities ▪ Anti-Forensics Countermeasures and Tools	**5**	**29%**

Policy Alignment: ISO 17024 Standard

	Analyze Various Files Associated with Windows, Linux, and Android Devices	▪ Windows File Analysis ▪ Metadata Investigation ▪ Windows ShellBags ▪ Analyze LNK Files and Jump Lists ▪ Event logs ▪ File System Analysis using The Sleuth Kit (TSK) ▪ Linux Memory Forensics ▪ Viewing Log Messages in Mac ▪ APFS File System Analysis: Biskus APFS Capture ▪ Parsing metadata on Spotlight ▪ Logical Acquisition of Android and iOS Devices ▪ Physical Acquisition of Android and iOS Devices ▪ Android and iOS Forensic Analysis ▪ SQLite Database Extraction ▪ Challenges in Mobile Forensics	**6**	
	Analyze Various Logs and Perform Network Forensics to Investigate Network Attacks	▪ Analyzing Firewall, IDS, Honeypot, Router, and DHCP Logs ▪ Analyzing Cisco Switch, VPN, and DNS Server Logs ▪ Investigating SSH Logs ▪ Network Protocols and Packet Analysis ▪ Why Investigate Network Traffic? ▪ Gathering Evidence via Sniffers ▪ Sniffing Tools ▪ Analyze Traffic for TCP SYN and SYN-FIN Flood DOS Attack ▪ Analyze Traffic for UDP and HTTP Flood Attacks ▪ Analyze Traffic for FTP and SMB Password Cracking Attempts ▪ Analyze Traffic for Sniffing Attempts ▪ Analyze Traffic to Detect Malware Activity ▪ Analyze SMTP and SNMP Traffic ▪ Centralized Logging Using SIEM Solutions ▪ SIEM Solutions	**6**	

Policy Alignment: ISO 17024 Standard

		▪ Examine Brute-Force Attacks, DoS Attacks, and Malware Activity ▪ Examine Data Exfiltration Attempts made through FTP ▪ Examine Network Scanning Attempts and Ransomware Attacks ▪ Detect Rogue DNS server (DNS Hijacking/DNS Spoofing) ▪ Wireless Network Security Vulnerabilities ▪ Performing Attack and Vulnerability Monitoring ▪ Detect a Rogue Access Point and Access Point MAC Spoofing Attempts ▪ Detect Misconfigured Access Points, Honeypot Access Points, and Signal Jamming Attack ▪ Investigate Wireless Network Traffic		
	Analyze Various Logs and Perform Web Application Forensics to Examine Various Web-Based Attacks	▪ Investigating Cross-Site Scripting, SQL Injection, and Directory Traversal Attacks ▪ Investigating Command Injection, Parameter Tampering, and XML External Entity Attacks ▪ Investigating Brute Force Attack and Cookie Poisoning Attack	**6**	
	Perform Forensics on Databases, Dark Web, Emails, Cloud and IoT devices	▪ Database Forensics Using SQL Server Management Studio and ApexSQL DBA ▪ Common Scenario for Reference ▪ MySQL Forensics for WordPress Website Database ▪ Tor Browser Forensics: Memory Acquisition ▪ Collecting Memory Dumps ▪ Memory Dump Analysis: Bulk Extractor ▪ Forensic Analysis of Memory Dumps to Examine Email Artifacts (Tor Browser Open and Tor Browser Closed) ▪ Forensic Analysis of Storage to Acquire the Email Attachments (Tor Browser Open and Browser Closed)	**6**	

Policy Alignment: ISO 17024 Standard

		▪ Forensic Analysis: Tor Browser Uninstalled ▪ Dark Web Forensics Challenges ▪ Steps to Investigate Email Crimes ▪ Division of Responsibilities ▪ Where Is the Data Stored in Azure? ▪ Logs in Azure ▪ Acquiring a VM in Microsoft Azure ▪ Acquiring a VM Snapshot Using Azure Portal and PowerShell ▪ AWS Forensics ▪ Cloud Storage Forensics ▪ Google Workspace Forensics ▪ Google Cloud Forensics ▪ Wearable IoT Device: Smartwatch ▪ IoT Device Forensics: Smart Speaker-Amazon Echo		
	Perform Static and Dynamic Malware Analysis in a Sandboxed Environment	▪ Malware Analysis: Static and Dynamic ▪ Analyzing Suspicious Word, Excel, and PDF Documents	**5**	
	Analyze Malware Behavior on System and Network Level, Analyze Malware Persistence, and Analyze Fileless Malware	▪ Registry-Based Malware Persistence Mechanisms ▪ Identifying Malware Persistence ▪ System Behavior Analysis: Monitoring Registry Artifacts, Processes, Services, Startup Programs, Windows Event Logs, API Calls, and Device Drivers ▪ System Behavior Analysis: Installation and System Calls Monitoring ▪ System Behavior Analysis: Monitoring Files and Folders, Monitoring Network Activities, Port, and DNS ▪ Artifact Analysis for Suspicious or Malicious Content ▪ Fileless Malware Analysis: GOOTLOADER ▪ Perform Timeline Analysis	**5**	

	Perform Digital Forensics using Python	▪ Python Digital Forensics Basics ▪ Data Acquisition using Python ▪ Windows and Linux Forensics using Python ▪ Malware Forensics using Python ▪ Web Application and Cloud Forensics using Python ▪ Email Forensics using Python ▪ Mobile Device and IoT Forensics using Python ▪ Multimedia Forensics using Python	**5**	
6. Tools/ Systems/Programs	Identify Various Tools to Investigate Operating Systems, Including Windows, Linux, Mac, Android, and iOS	▪ File System Analysis Tools ▪ File Format Analyzing Tools ▪ Volatile and Non-Volatile Data Acquisition Tools ▪ Data Acquisition Validation Tools ▪ eDiscovery Tools ▪ Digital Forensic Imaging Solutions ▪ Tools for Examining Images on Windows, Linux, and macOS ▪ Tools for Carving Files on Windows, Linux, and macOS ▪ Partition Recovery Tools ▪ Using Rainbow Tables to Crack Hashed Passwords ▪ Password Cracking Tools ▪ Tool to Reset Admin Password ▪ Steganography Detection Tools ▪ Detecting Data Hiding in File System Structures Using OSForensics ▪ ADS Detection Tools ▪ Detecting File Extension Mismatch using Autopsy ▪ Tools to Detect Overwritten Data/Metadata ▪ Program Packers Unpacking Tools ▪ USB Device Enumeration using Windows PowerShell ▪ Tools to Collect Volatile and Non-Volatile Information on Windows and Linux	**6**	**11%**

Policy Alignment: ISO 17024 Standard

		▪ Tools to Perform Windows Memory and Registry Analysis ▪ Tools to Examine the Cache, Cookie, and History Recorded in Web Browsers ▪ Private Browsing and Browser Artifact Recovery ▪ Tools to Examine Windows Files, Metadata, ShellBags, LNK files, and Jump Lists ▪ Linux File system Analysis Tools ▪ Tools to Perform Linux Memory Forensics ▪ APFS File System Analysis ▪ Parsing Metadata on Spotlight ▪ MAC Forensic Tools ▪ Network Traffic Investigation Tools ▪ Incident Detection and Examination with SIEM Tools ▪ Detect and Investigate Various Attacks on Web Applications by Examining Various Logs ▪ Tools to Identify TOR Artifacts ▪ Tools to Acquire Memory Dumps ▪ Tools to Examine the Memory Dumps ▪ Tools to Perform Static and Dynamic Malware Analysis ▪ Tools to Analyze Suspicious Word and PDF Documents ▪ Tools to Analyze Malware Behavior on a System and Network ▪ Tools to Perform Logical and Physical Acquisition on Android and iOS Devices ▪ Mobile Forensic Tools		
	Determine the Various Tools to Investigate MSSQL, MySQL, Azure, AWS, Emails, and IoT Devices	▪ Tools to Collect and Examine the Evidence Files on MSSQL Server and MySQL Server ▪ Tools for Investigating Microsoft Azure and AWS ▪ Tools to Acquire Email Data and Deleted Emails ▪ Tools to Perform Forensics on IoT devices	**5**	

Policy Alignment: ISO 17024 Standard

	Identify Various Tools to Perform Network, Web Application, Cloud, Social Media, and Insider Threat Forensics	▪ Network Log Analysis Tools ▪ Tools for Investigating Network Traffic ▪ Social Media Forensic Tools ▪ Insider Threat Tools ▪ Tools for Analyzing IIS Logs and Apache Logs ▪ Blockchain Forensic Tools ▪ AWS Forensic Tools	**5**	

Policy Alignment: ISO 17024 Standard

AGREEMENTS

Appendix B

Policy Alignment: ISO 17024 Standard

NON-DISCLOSUREAGREEMENT

EC-Council

Policy Alignment: ISO 17024 Standard

EC-Council NON-DISCLOSURE AGREEMENT

EC-Council and/or its Affiliate ("Disclosing Party") intends to make available or have made available to you ("Receiving Party" or "You") certain proprietary and confidential information including but not limited to exam items, materials, any notes or calculations, questions, exam methodologies, exam content and/or exam standards (together referred to as "Exam Materials") in connection with EC-Council certification ("Purpose"), in accordance with the terms of this Confidentiality and Non-Disclosure Agreement ("Agreement"). Disclosing Party either on its own or via its appointed representative spends substantial sums of time and money in developing and administering its Exam Materials which are the Intellectual Property of EC-Council. Such information related to Exam Materials so provided to You whether provided before or after the date hereof and whether written or oral, together with all manuals, documents, memoranda, notes, analyses, forecasts and other materials are strictly confidential and prohibited to be produced in any form whether written or oral, in any medium whether now known or to be developed later, in English or in any language, whatsoever, which contain or reflect, or are generated from, such Exam Material shall be collectively referred to herein as the "Confidential Information." For the purpose of clarity, "Affiliate" shall mean with respect to EC-Council at a given time, any entity whether incorporated or not, which is either controlled by or under common control with, or controls, the other entity, either directly or indirectly.

The Receiving Party now agrees as set forth below.

You shall hold Disclosing Party's Confidential Information in strict confidence and shall not disclose such Confidential Information to any third party or use it for any purpose other than to further the Purpose. You further agree not to create or engage in activities, either alone or jointly with others for the purpose of publishing any brain dump and/or any other unauthorized material that contains Exam Materials and any portion of the Confidential Information without the prior written consent of Disclosing Party. Further, You shall not copy or attempt to make copies (written, photocopied, or otherwise) of any Exam Material, including, without limitation, any exam questions or answers.

The Exam Materials including any questions and answers of the Exam are the exclusive and confidential property of the Disclosing Party and are protected by Disclosing Party's intellectual property rights, including but not limited to all patent, copyright, trademark, design and other proprietary rights and interests therein. You acknowledge and agree that nothing contained in this Agreement shall be construed as (i) granting any rights or license (either expressly or impliedly) in or to any Confidential Information or (ii) obligating either party to enter into an agreement regarding the Confidential Information, unless otherwise agreed to in writing. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable by You.

CONFIDENTIAL INFORMATION IS PROVIDED "AS IS" AND DISCLOSING PARTY MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR OTHERWISE, REGARDING CONFIDENTIAL INFORMATION, INCLUDING AS TO ITS ACCURACY. DISCLOSING PARTY ACCEPTS NO RESPONSIBILITY FOR ANY EXPENSES, LOSSES OR ACTION INCURRED OR UNDERTAKEN YOU AS A RESULT OF YOUR RECEIPT OR USE OF ANY INFOR- MATION PROVIDED HEREUNDER.

Any Confidential Information disclosed hereunder and any copies thereof (including, without limitation, all documents, memoranda, notes, analyses, forecasts and other materials prepared by the Disclosing Party, and all electronically stored copies or physically stored) will be returned or destroyed.

Your obligations under this Agreement shall survive the termination of the Agreement. This Agreement shall be governed by and construed in accordance with the laws of the State of New Mexico, without regard to its conflict of law principles.

You hereby acknowledge and agree that violation of any of these provisions will cause irreparable harm to the Disclosing Party for which monetary remedies may be inadequate, and that the Disclosing Party shall be entitled, without waiving any other rights or remedies, to take all appropriate actions to remedy or prevent such disclosure or misuse, including obtaining an immediate injunction.

This Agreement may not be modified except by writing by Disclosing Party. If any provision of this Agreement or any portion thereof shall be held invalid, illegal or unenforceable by a court of competent jurisdiction, the remaining provisions of this Agreement shall remain in full force and effect, and the affected provisions or portion thereof shall be replaced by a mutually acceptable provision, which comes closest to the economic effect and intention of the parties hereto. This Agreement may be executed in counterparts, all of which shall constitute one agreement.

DO NOT attempt an EC-Council certification exam unless you have read, understood and accepted the terms and conditions in full. By attempting an exam, you signify the acceptance of those terms. Please note that in the event that you do not accept the terms and conditions of the Agreement, you are not authorized by EC-Council to attempt any of its certification exams. EC-Council reserves the right to revoke your certification status, publish the infraction, and/or take the necessary legal action against you, if you fail to comply with the above terms and conditions.

EC-Council Certification Agreement v5.0

w.e.f. June 1st, 2020

EC-Council

Policy Alignment: ISO 17024 Standard

EC-Council CERTIFICATION AGREEMENT v5.0

Candidate Application Agreement and Candidate Certification Agreement (Hereinafter referred to as“ Certification Agreement” v5.0)

READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY. EXAMINATION SHALL NOT BE ATTEMPTED UNLESS ALL THE TERMS AND CONDITIONS OF THE AGREEMENT HAS BEEN DULY READ, UNDERSTOOD AND ACCEPTED IN FULL.

This EC-Council Certification Agreement (the “Agreement”) is entered into between you and International Council of E-Commerce Consultant(“EC-Council”) as of the date of the acceptance of the agreement.

1. DEFINITIONS

For purposes this Agreement, the terms defined in this Section shall have the meanings set forth below:

1.1 **“Candidate”** means an individual who attempts the certification examination but is not conferred the said certification unless he fulfils all the requirements such as the Passing Criteria. When it is evidenced that the candidate is conferred a certification status, the Candidate shall referred to as a

1.2 **"Program"** shall mean one of the certification programs offered by EC-Council.

1.3 **"Examination Materials"** shall mean EC-Council certification examination(s) and any questions. instructions, responses, answers, worksheets, drawings and/or diagrams related to such examination(s) and any accompanying materials. The list is inclusive of all related EC-Council Training Materials.

1.4 **“Marks”** means, as the case may be, any and all EC-Council titles, trademarks, service marks and/or logos which EC-Council may from time to time expressly designate for use corresponding to the EC-Council certification that a candidate attempts or a Certified Member have achieved.

1.5 Passing Criteria shall mean passing criteria for an EC-Council certification exam which may vary from exam to exam. The passing criteria for an EC-Council exam can be found at https://cert.eccouncil.org/faq.html.

2. OBLIGATIONS

2.1 At all times, you shall agree to adhere to the certification/candidate policies of EC-Council including but not limited to:

2.1.1 Certification Exam Policy (https://cert.eccouncil.org/certification-exam-policy.html);

2.1.2 Exam Retake Policy (https://cert.eccouncil.org/exam-retake-policy.html);

2.1.3 Eligibility Policy (https://cert.eccouncil.org/application-process-eligibility.html);

2.1.4 EC-Council Non-Disclosure Agreement (https://cert.eccouncil.org/images/doc/NDA-Non-Disclosure-Agreement-v2.0.pdf);

2.1.5 Special Accommodation Policy (https://cert.eccouncil.org/special-accommodation-policy.html);

2.1.6 Appeal Procedure (https://cert.eccouncil.org/appeal-procedure.html);

2.1.7 Voucher Extension Policy (https://cert.eccouncil.org/exam-voucher-extension-policy.html)

EC-Council reserves the right to add, edit, amend or delete the abovementioned policies at any time with or without notice.

2.2 At all times, you shall, either in the capacity of being a Candidate and/or a Certified Member, as applicable, agree to adhere to the Code of Ethics of EC-Council including but not limited to:-

- Keep private and confidential information gained in own professional work, (in particular if it pertains to your client lists and client's personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without your client's prior consent.
- Protect and respect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator. Disclose and report to appropriate persons or authorities' potential dangers to any e-commerce clients, the Internet community, or the public, as applicable.
- Provide service in own areas of competence. You should be honest and forthright about any limitations of own experience and education. Ensure that the Certified Member is qualified for any project by an appropriate combination of education, training, and experience.
- Never knowingly use software or process that is obtained or retained either illegally or unethically.
- Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
- Use and protect the property of your clients or employers only in ways which are properly authorized, and with the owner's knowledge and consent.
- Avoid any conflict of interest. Disclose to all concerned parties, including (without limitation) your clients, employers, EC-Council any actual or potential conflicts of interest that cannot reasonably be avoided or escaped. For the purpose of clarity, if you have participated in Item writing for any of the EC-Council certification examinations, you will not be allowed to sit for the same certification examination. Further, if you wish to be EC-Council's Consultant, you must disclose your association with EC-Council's other products and/or services and/or your association with competing products and/or services.
- Ensure good management for any project as a Certified Member.
- Add to the knowledge of the e-commerce profession by constant study, share the lessons of own experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.
- Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in the Certified Member's knowledge and integrity.
- Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.
- Not to associate with malicious hackers or engage in any malicious activities.
- Not to purposefully compromise or allow the client's or organization's systems to be compromised in the course of the Certified Member's professional dealings. EC-Council Certification Agreement v5.0 04
- Ensure all penetration testing activities are authorized and within legal limits.

- Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.
- Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.
- Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.
- Not to be in violation of any law of the land or have any previous conviction.
- Make claims regarding certification only with respect to the scope for which the certification has been granted.
- Not to use the certification in a manner as to bring EC-Council into disrepute.
- Not to make misleading and/or unauthorized statement regarding the certification or EC-Council.
- Discontinue the use of all trademarks as regard to the certification which contains any reference to EC-Council and/or EC-Council trademark or logo or insignia upon suspension/withdrawal of the said certification.
- Return any certificates issued by EC-Council upon suspension/withdrawal of the certification.
- Refrain from further promoting the certification in the event of the said certification is withdrawn or suspended.
- Inform EC-Council without any undue delay of any physical or mental condition which renders the Certified Member incapable to fulfill the continuing certification requirements.
- Maintain the certification by completing, within the time frame specified by EC-Council, all continuing certification requirements (if any) that correspond with Certified member's particular certification.
- To not to participate in any cheating incident, breach of security, misconduct or any other behavior that could be considered a compromise of the integrity or confidentiality of any EC-Council certification examination.

2.2.1 Code of Ethics of EC-Council is subject to change from time to time in order to remain compliant with any applicable laws, rules and regulations and the same shall be updated and located at https://cert.eccouncil.org/code-of-ethics.html. It is your responsibility to always refer to such link for any updates.

2..2.2 Upon being a Certified member, you shall adhere to the EC-Council Education (ECE) policy (https://cert.eccouncil.org/ece-policy.html).

3. CERTIFICATION

3.1 You shall be conferred a certification only upon a successful completion of the required certification examination and your compliance with the requirements described in the current corresponding program brochure. You agree that EC-Council has the right to modify any examination, certification scheme, test objectives or the requirements for obtaining or maintaining any EC-Council certification at any time.

3.2 Notwithstanding anything in this agreement to the contrary, EC-Council has the sole discretion to withdraw, suspend, or refuse to renew and/or grant you the certification if EC-Council in good faith determines that your certification or use of the corresponding Marks will adversely affect EC-Council or the community at large or consumers.

3.3 Upon being conferred the certification, you are expected to notify EC-Council of any changes to your contact information to retain your certification. You may withdraw your contact information at any time in which case, EC-Council shall not have any obligation to keep your certification updated.

3.4 Once you are certified, you are solely responsible for keeping yourself informed after EC-Council's continuing certification requirements for maintaining your own certification. If you fail / do not complete the continuing certification requirements timeframe specified by EC-Council, your certification for that particular program will be revoked without further notice, and all rights pertaining to that certification (including the right to use the applicable marks) will be terminated.

3.5 Notwithstanding anything in this agreement to the contrary, EC-Council has the sole discretion to withdraw, suspend, or refuse to renew and/ or grant you the certification if EC-Council learns at any point of time that the Candidate and/or the Certificate Member, as applicable, has cheated and/ or used unethical measures and/or suppressed any material information leading to conflict of interest to obtain the relevant certification.

3.6 Notices: All notices herein shall be in writing and in English language. EC-Council may publish any notice online and/or send email at your registered email ID. You may wish to write to EC-Council at certmanager@eccouncil.org and/or send notices by mail at the below addresses:

For Europe, Middle East and Asia regions:-

Attention: Director of Certification

6-3-883/4/2,
Panjagutta (Exide battery Lane),
Hyderabad, Telangana, 500082
INDIA

USA and South America

Attention: Director of Certification

101 C Sun Avenue NE,
Albuquerque, NM 87109
USA

4. TERM AND TERMINATION

4.1 **Term:** Upon being conferred the certification, you are required to maintain the certification and update the validity of the EC-Council certification via EC-Council's ECE program located at https:// cert.eccouncil.org/ece-policy.html. The initial certification validity is three years and you are required to fulfill the terms and conditions of the ECE Program to retain the validity of the relevant certification. The term of this Agreement is coterminous with the validity of the certification if you are a Certified Member and if you are not a Certified Member, then the agreement shall be deemed to terminated at the end of your relevant certification exam as a Candidate.

4.2 **Effect of Termination:** Upon the termination of this Agreement, you as a Certified Member shall immediately cease all use of the Marks, all representations or claims that you hold any EC-Council Certifications, or any other statements that imply in any way that you are EC-Council certified. This obligation includes, but is not limited to, immediately removing the Marks from all web sites and electronic materials under your control, including resumes, profession profiles, and email signatures, as well as from all hard copy materials, including business cards. All unused business cards or other hard copy materials bearing the Marks shall be destroyed within ten (10) days of termination, and you agree to provide EC-Council a written statement under oath attesting to such destruction, if requested by EC-Council. Upon termination, you shall also lose all access to the related portals made available to you by EC-Council during the term by which you are a Certified Member.

5. LICENSE

5.1 If you are a Candidate and has not been conferred with certification, you shall not be granted the rights to use and/or display the EC-Council trademarks, logo, insignia (hereinafter "Marks") for whatsoever purpose, be it for promotional, advertising, marketing and/or publicity purposes. Failure to abide with this section shall attract legal recourse in the forms of injunctions, civil liability, and forfeiture of profits, and punitive damages and/or other legal sanctions deemed reasonable to address such breach.

5.2 Subject to the terms and conditions of this Agreement and the attainment of one or more of EC-Council certifications, EC-Council shall grant you in your capacity as Certified Member a nonexclusive and non-transferable license to only use and display the relevant Marks solely in connection with providing the professional services that correspond to the certification program t hat the Certified Member had earned.

5.3 Once certified, you may use the Marks such on such promotional display and advertising materials as it may, in your judgement, promote the professional services in correspondence to your certification.

5.4 You shall not use the Marks for any purposes that are not directly related to the provision of the professional services corresponding to your particular certification You shall not use the Marks if any certification program unless you have completed the certification program requirements and have been notified by EC-Council in writing that you have achieved the certification status for that particular Program.

5.5 As a Certified Member, you shall not misrepresent your own certification status or qualifications so as to imply or suggest that EC-Council in any way endorses, sponsors or recommends you, or any of your products or services.

5.6 You also agree that your status as a Certified Member and your rights pertaining to the Marks as vested to you under this Agreement shall not permit you to hold yourself out as having any ownership rights over the official Training/Examination Materials. Any attempts/action which implies to the public that you have some degree of ownership to the official Training/Examination Materials shall be construed as a material breach of this Agreement and your certification shall be revoked with immediate effect.

6. OWNERSHIP OF MARKS BY CERTIFIED MEMBERS

Once certified, no title or ownership of the Marks shall be transferred, either explicitly or impliedly, to you pursuant to this Agreement. EC-Council owns and retains all title and ownership of all intellectual property rights in the products, documentation, certificate and all other related materials and Marks. EC-Council does not transfer any portion of such title and ownership, or any of the associated goodwill to you, and this Agreement should not be construed to grant you any right or license, whether by implication, estoppel, or otherwise, except as expressly provided. You agree to be bound by and observe the proprietary nature of the materials acquired by reason of your certification under this Agreement.

7. CONDUCT OF BUSINESS OF CERTIFIED MEMBERS

You as a Certified Member shall agree to (i) conduct business in a manner which reflects favorably at all times on the products, goodwill and reputation of EC-Council; (ii) avoid deceptive, misleading or unethical practices which are or might be detrimental to EC-Council or its products; and (iii) refrain from making any representations, warranties, or guarantees to customers that are inconsistent with the policies established by EC-Council. Without limiting the above, you are also obliged to not to misrepresent your certification status or level of skill and knowledge related thereto.

8. QUALITY OF PROFESSIONAL SERVICES BY CERTIFIED MEMBERS

You shall also agree that it is of fundamental importance to EC-Council that the professional services are of the highest quality and integrity. Accordingly, you agree that EC-Council will have the right to determine in its absolute discretion whether the professional services meet EC-Council's standards of merchantability. In the event that EC-Council determines that you are no longer meeting accepted levels of quality and/or integrity, EC-Council agrees to advise you and to provide you with a commercially reasonable time of no less than one (1) month to rectify and meet the same.

9. RESERVATION OF RIGHTS AND GOOD WILL IN EC-COUNCIL

EC-Council retains all rights not expressly conveyed to you by this Agreement. You must recognize the value of the publicity and goodwill associated with the Marks and acknowledge that the goodwill will exclusively inure to the benefit of, and belong to, EC-Council. You as a Certified Member shall have no rights of any kind whatsoever with respect to the Marks licensed under this Agreement except to the extent of the license granted in this Agreement.

10. NO REGISTRATION BY CERTIFIED MEMBER

You agree not to file any new trademark, collective mark, service mark, certification mark, and/or trade name application(s), in any class and in any country, for any trademark, collective mark, service mark, certification mark, and/or trade name that, in EC-Council's opinion, is the same as, similar to, or that contains, in whole or in part, any or all of EC-Council's trade names, trademarks, collective marks, service marks, and/or certification marks, including, without limitation, the Marks licensed under this Agreement. You further agree to not to register or use as your own any internet domain name which contains ECCouncil's Marks or other trademarks in whole or in part or any other name which is confusingly similar thereto. To the extent that Certified Member obtains or develops any rights in or to the EC-Council Marks or any confusingly similar trademarks, Certified Member agrees to assign, and does hereby irrevocably assign such rights to EC-Council. This section shall survive the expiration or termination of this Agreement.

11. PROTECTION OF RIGHTS BY CERTIFIED MEMBER

11.1 You agree to assist EC-COUNCIL, to the extent reasonably necessary and at EC-Council's expense, to protect or to obtain protection for any of EC-Council's rights to the Marks.

11.2 If at any time EC-Council requests that you discontinue using the Marks and/or substitute using a new or different Mark, you shall immediately cease use of the Marks and cooperate fully with EC- Council to ensure all legal obligations have been met with regards to use of the Marks.

12. INDEMNIFICATION BY CERTIFIED MEMBER

12.1 You shall agree to indemnify and hold EC-Council harmless against any loss, liability, damage, cost or expense (including reasonable legal fees) arising out of any claims or suits made against EC-Council (i) by reason of your threatened or actual breach of the terms and conditions under this Agreement; (ii) arising out of your use of the Marks in any manner whatsoever except in the form expressly licensed under this Agreement; and/or (iii) for any personal injury, product liability, or other claim arising from the promotion and/or provision of the professional services.

13. CONFIDENTIALITY

13.1 Training/Examination Materials are the proprietary, confidential and copyrighted materials of EC-Council. Any disclosure of the contents of any EC-Council certification examination is strictly prohibited.

13.2 You, at all times, hereby agree to maintain the confidentiality of all Examination Materials and not to disclose, publish, reproduce, distribute, post or remove from the examination room, any portion of the Examination Materials. Failure to observe and comply with this provision shall be deemed as a breach and shall attract legal recourse in the forms of injunctions, civil liability, forfeiture of profits, punitive damages and/or other legal sanctions deemed reasonable to address such breach.

13.3 Your obligation of confidentiality hereunder shall terminate when you can establish that the Examination Materials (a) is already in the public domain or becomes generally known or published without breach of this Agreement; (b) is lawfully disclosed by a third party free to disclose such information; or (c) is legally required to be disclosed provided that you promptly notify EC-Council so as to permit such EC-Council to appear and object to the disclosure and further provided that such disclosure shall not change or diminish the confidential and/or proprietary status of the Confidential Information.

13.4 You further agree that, except as otherwise stated in this Agreement, you shall not use the name of EC-Council and/or its other corresponding entities, either expressed or implied in any of its advertising or sales promotional material.

14. LIMITATION OF LIABILITY

IN NO EVENT WILL EC-COUNCIL BE LIABLE TO YOU FOR ANY SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL PUNITIVE, EXEMPLARY OR ANY SIMILAR TYPE OF DAMAGES ARISING OUT OF OR IN ANY WAY RELATED TO THIS AGREEMENT.

15. GENERAL PROVISIONS

15.1 **Governing Law and Venue:** This Agreement will in all respects be governed by the law of the State of New Mexico, excluding its conflicts of laws and provisions, and venue of any actions will be proper in the courts of the State of New Mexico of the United States of America.

15.2 **Attorney's Fees:** In the event of any action arising out of or relating to this Agreement, the prevailing party shall be entitled to recover the costs and expenses of the action, including reasonable attorney's fees, incurred in connection with such action from the losing party.

15.3 **Non-Waiver:** No waiver of any right or remedy on one occasion by either party will be deemed a waiver of such right or remedy on any other occasion.

15.4 **Assignment:** Neither this Agreement nor any of your rights or obligations arising under this Agreement may be assigned without EC-Council's prior written consent. This Agreement is freely assignable by EC-Council, and will be for the benefit of EC-Council's successors and assigns.

15.5 **Independent Contractors:** You acknowledge that you and EC-Council are independent contractors and you agree to not to represent yourself as, an employee, agent, or legal representative of EC-Council.

15.6 **Compliance with Laws:** You agree to comply, at your own expense, with all statutes, regulations, rules, ordinances, and orders of any governmental body, department, or agency that apply to or result from your rights and obligations under this agreement.

15.7 **Modifications:** Any modifications to the typewritten face of this Agreement will render it null and void. This Agreement will not be supplemented or modified by any course of dealing or usage of trade. Any modifications to this Agreement must be in writing and signed by both parties.

15.8 **Revision of terms:** EC-Council reserves the right to revise the terms of this Agreement from time to time. In the event of a revision, your signing or otherwise manifesting assent to a new agreement may be a condition of continued certification..

EC-Council

Policy Alignment: ISO 17024 Standard