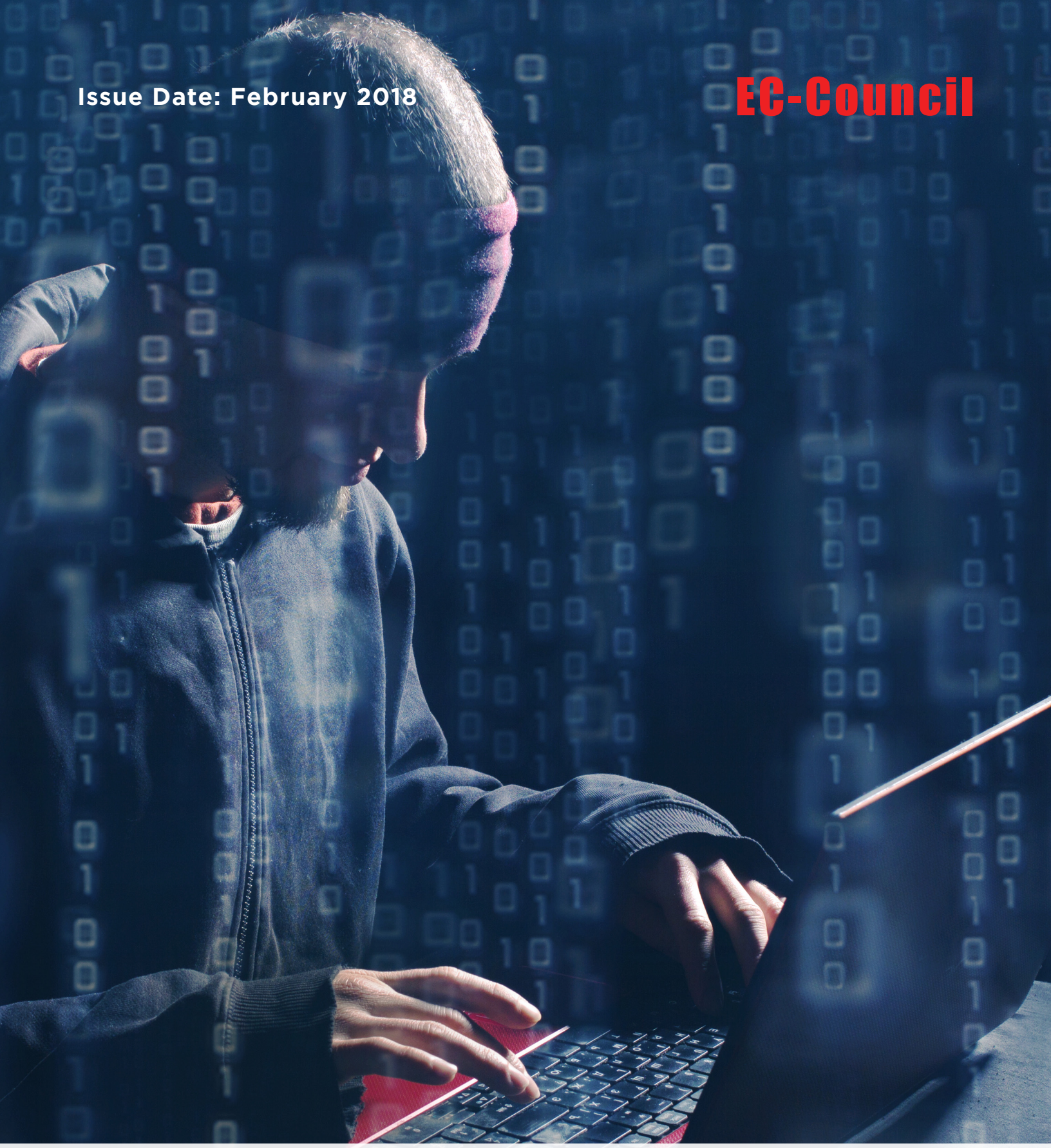
Issue Date: February 2018

EC-Council



# CHFI Candidate Handbook

# Table of Contents

# 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) and EC-Council Certified Security Analyst (ECSA)/License Penetration Tester (LPT) certification, and as well as many others certification schemes, that are offered in over 87 countries globally.

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-war, should the need ever arise". EC-Council is committed to withhold the highest level of impartiality and objectivity in its practices, decision making and authority in all matters related to certification.

As of December 31st, 2017, EC-Council has certified over 200,000 security professionals. 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 **http://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***

# Steps to Earn the CHFI 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 CHFI exam is available at 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 CHFI exam.*

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

| Tasks | Knowledge |
|---|---|
| Forensic Science | Computer forensics in today's world |
| Regulations, Policies and Ethics | Computer Forensics Investigation Process |
| Digital Evidence | Understanding hard disks and file systems |
| Procedures and Methodology | Data acquisition and duplication |
| Digital Forensics | Defeating anti-forensics techniques |
| Tools/Systems/Programs | Operating system forensics |
| | Network forensics |
| | Investigating web attacks |
| | Database forensics |
| | Cloud forensic |
| | Malware forensics |
| | Investigating email crimes |
| | Mobile forensic |
| | Forensics report writing and presentation |

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

Upon successfully passing the exam you will be issued your CHFI credential and will receive your CHFI welcome kit within 4 – 8 weeks.

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. For more details about ECE please refer to the next section.

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

## A. Attend Official Training

Attend an official CHFI instructor-led training (ILT), computer-based training (CBT), 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 Application Agreement terms
c. 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 2 years of work experience in the Information Security domain.
b. Educational background that reflects specialization in Information Security.
c. Remit a non-refundable eligibility application fee of USD 100.00
d. Submit a completed Exam Eligibility Application Form.
e. Purchase an official exam voucher DIRECTLY from EC-Council through *https://store.eccouncil.org/*

## 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 after 90 days, the Application will be automatically rejected. Applicant will need to submit a new application form.

d. Waiting time for processing of Eligibility Application is approximately 5 working days after receiving the verification from verifier. Should the applicant not hear from us after 5 working days, the applicant can contact *cehapp@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 eligibility code and the voucher code which candidate can use to register and schedule the test at VUE and EC-Council Test Centers. Please note that VUE registration will not entertain any requests without the eligibility code.

b. The approved application stands valid for 3 months from the date of Approval, the candidate needs to test within 1 year from the date of voucher release.

c. An extension request will require the approval of the Director - Certification.

d. If application is not approved, the application fee of USD 100 will not be refunded.

# EC-Council Exam Eligibility Application Form v3

- CEH (Certified Ethical Hacker)
- CHFI (Computer Hacking Forensic Investigator)
- ECSA (EC-Council Certified Security Analyst)
- ECSP-Java (EC-Council Certified Secure Programmer – Java)
- ECSP-.NET (EC-Council Certified Secure Programmer – .NET)
- EDRP v3 (EC-Council Disaster Recovery Professional v3)
- ECDR-VT (EC-Council Certified Disaster Recovery and Virtualization Technology Professional)
- CND (Certified Network Defender)

## Eligibility Requirements

Either one of the following criteria is required by EC-Council so that a determination can be made regarding a candidate's eligibility.

a. A candidate has attended "Official" training through an EC-Council Authorized Training Center (ATC).

   Accepted Official Training Solutions: Instructor-Led (ILT), Computer-Based (CBT), Web-Based (WBT), or Academic Learning.

b. A candidate may be granted permission to attempt the exam without "Official" training if:

   1. The candidate has and can prove two years of work experience in the Information Security domain
   2. The candidate remits a non-refundable Eligibility Application Fee of $100 (USD).
   3. The candidate submits a completed Exam Eligibility Application.

## Application Submission Steps

**Step 1:** Complete the application form.

**Step 2:** Attach a copy of your resume, and a scanned copy of an identification document, such as Employee i-Card of your current or previous employment, which does not carry any Personally Identifiable Information. EC-Council strongly discourage you from submitting your passport, driver's license, government ID or any other identification document that carries Personally Identifiable Information.

**Step 3:** Scan the documents and e-mail them to cehapp@eccouncil.org

**Step 4:** Remit $100 payment for Non-refundable Eligibility Application Fee

**Step 5:** A representative from EC-Council's Certification Department will contact your Boss /Supervisor/ Department head to verify the information submitted on your application.

**Step 6:** If your application is approved, you will be required to purchase the exam voucher directly from EC-Council. You will then receive your exam eligibility code along with the exam voucher.

Confidentiality of Information: We treat personal information securely and confidentially. EC-Council adheres to strict US privacy laws and will not disclose the submitted information to any third party except for your Boss / Supervisor / Department head. (As stated above, verification is required)

Disclaimer: EC-Council reserves the right to deny certification to any candidate who attempts to sit for this exam without qualifying as per the mentioned eligibility criteria. Should the audit team discover that a certification was granted to a candidate who sat for the exam and did not qualify as per the eligibility criteria, EC-Council also reserves the right to revoke the candidate's certification.

Retention of Documentation: EC-Council will not retain any supporting documents related to the application beyond a period of 2 years from 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*

# EC-Council Exam Eligibility Application Form v3

## **Applicant Information** (Please write legibly)

First Name: _____ Last Name: _____

Proof of Identity: _____

Address: _____

City/State/Province: _____ Country: _____ Zip/Postal Code: _____

Daytime phone number/Cellular/other: _____

e-mail: _____

## Experience Qualifications

Company Name: _____

Company URL: http:// _____

Job Title / Position: _____

Number of Years with This Employer: _____

Number of Months of Security related work experience with this employer: _____

Type of security related work: _____

Experience qualifications certified by supervisor / agency representative

Supervisor Name & e-mail: _____ Position: _____

# EC-Council Exam Eligibility Application Form v3

## 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 disciplines. 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.

☐ Agree ☐ Disagree

Signature _____ Date _____

*If you submit electronically please don't 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 and fax in your application, please sign with your original signature to secure your compliance.*

**Cumulative experience is acceptable. (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 a retake exam voucher for the ECC Exam Center.

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 *https://eccouncil.zendesk.com/anonymous_requests/new*

# EC-Council

## Special Accommodation Request Form

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

| | |
|---|---|
| E-mail | Send the form to https://eccouncil.zendesk.com/anonymous_requests/new Please attach the form as a scanned document that includes the certifying authority's signature. |

**Section 1: APPLICANT INFORMATION**

Name :.....

Address (including city, state, and postal code) : .....

.....

.....

Phone Number: .....

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 : .....

License Number
and Type (if applicable}: .....

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 to decide what accommodations are necessary, please contact the EC-Council Certification Division at *https://eccouncil.zendesk.com/anonymous_requests/new.*

# C|HFI 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 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 to reflectively gauge the necessary knowledge and skill required by experts in 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 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 https://eccouncil.zendesk.com/anonymous_requests/new 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 https://eccouncil.zendesk.com/anonymous_re quests/new 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 : .....

Phone Number : .....

Mailing Address: : .....
(including city, state, and postal code)

.....

.....

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

Exam Voucher No : .....

Exam No & Name : .....

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

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

Test Center Name .....

Street Address
City, State/ Province
Zip/Postal Code
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 Application Agreement (CAA)
c. Candidate Certification Agreement (CCA)
d. 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 Application Agreement (CAA)**

Prior to attempting an EC-Council exam, candidates are required to agree to EC-Council CAA 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 CAA 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.

Action will be taken against violators of their signed CAAs. 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 CAA.

**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 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 https://eccouncil.zendesk.com/anonymous_requests/new 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 case of any suspicious patterns or trends on either the side of the candidate or the testing center EC-Council reserves the right to demand the candidate(s) to re-sit for the exam and/or assessment test. Candidate is to agree to the retest, failing which EC-Council will not award

the certification to the candidate. Candidate will be given one chance to take the Candidate Retesting Audit (CRA) exam. Should candidate fail to pass the CRA exam, candidate will be given one chance to take the full exam again. Should candidate fail to pass the full exam, candidate will be temporarily barred from taking the exam.

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 Delta 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 you hold multiple EC-Council certifications, credits earned will be applied to all active certifications.

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, ANSI/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.

Therefore, 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-4.0.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.

Upon completion of the 3-year ECE program and meeting the requirements (please refer to the How does it work? paragraph below), the member's certification validity will be extended for another three years from the month of expiry.

## 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.

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

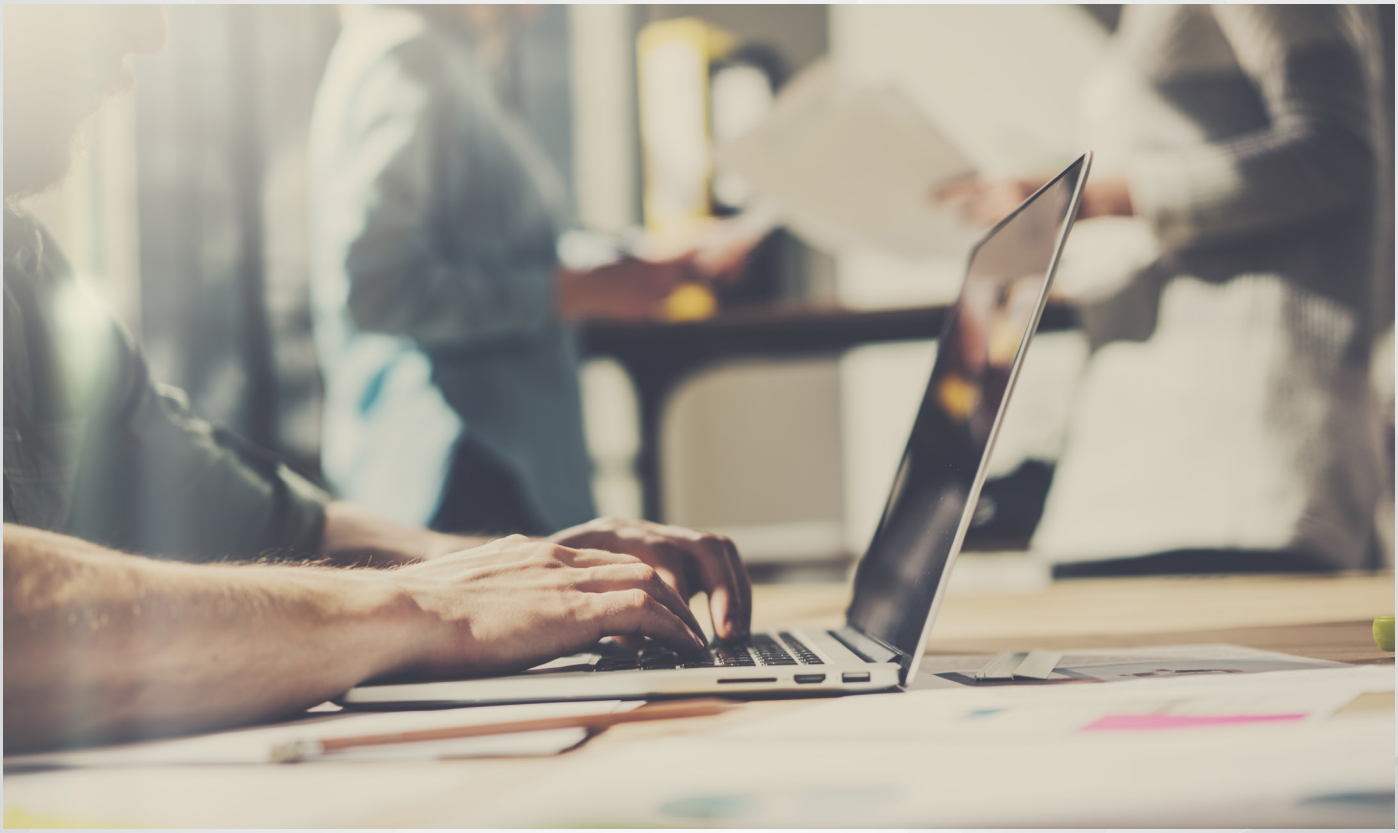
Members whose certification has been suspended or revoked due to non-compliance of certification requirements may send in an appeal in writing to EC-Council. This appeal letter must be received by EC-Council within ninety (90) days of the suspension/ revocation notice, providing details of the appeal 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. There is no requirement to submit evidence until it is requested for specifically by EC-Council.

## 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:

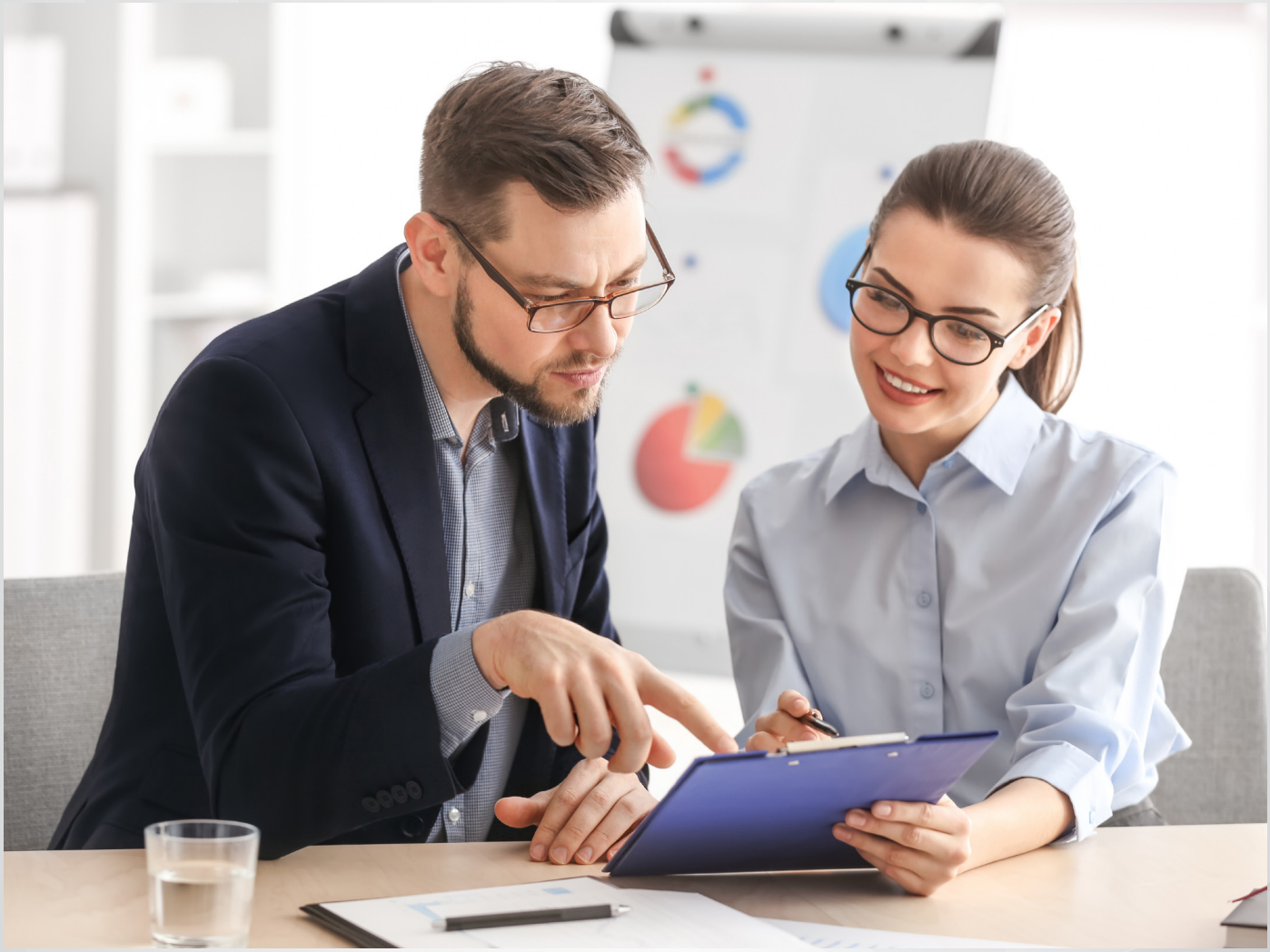
a. If you would like to be a licensed security consultant, earn the EC-Council Certified Security Analyst (ECSA) credential and apply to become a Licensed Penetration Tester (LPT)

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), EC-Council VoIP Professional (ECVP), EC-Council Certified Secure Programmer (ECSP) 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 http://cert.eccouncil.org.



# Code of Ethics

1. Keep private and confidential information gained in your professional work, (in particular as it pertains to client lists and client 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 client prior consent.

2. Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.

3. Disclose to appropriate persons or authorities potential dangers to any e-commerce clients, the Internet community, or the public, that you reasonably believe to be associated with a particular set or type of electronic transactions or related software or hardware.

4. Provide service in your areas of competence, being honest and forthright about any limitations of your experience and education. Ensure that you are qualified for any project on which you work or propose to work by an appropriate combination of education, training, and experience.

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

6. Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

7. Use the property of a client or employer only in ways properly authorized, and with the owner's knowledge and consent.

8. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

9. Ensure good management for any project you lead, including effective procedures for promotion of quality and full disclosure of risk.

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

11. Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in your knowledge and integrity.

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

13. Not to associate with malicious hackers nor engage in any malicious activities.

14. Not to purposefully compromise or allow the client organization's systems to be compromised in the course of your professional dealings.

15. Ensure all penetration testing activities are authorized and within legal limits.

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

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

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

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

# 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 : .....

Title/Company : .....

Country : .....

Phone : .....

EC-Council Membership No. (if applicable) : .....

**Complaint lodged against:**

Name : .....

EC-Council Membership No. (if applicable) : .....

Section of EC-Council Code of Ethics Violated:

.....

.....

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

.....

.....

.....

**Verified by**

**Contact 1**

Name : .....

Email : .....

Title/Company : .....

Country : .....

Phone : .....

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

.....

Signature/Date

**Contact 2**

Name : .....

Email : .....

Title/Company : .....

Country : .....

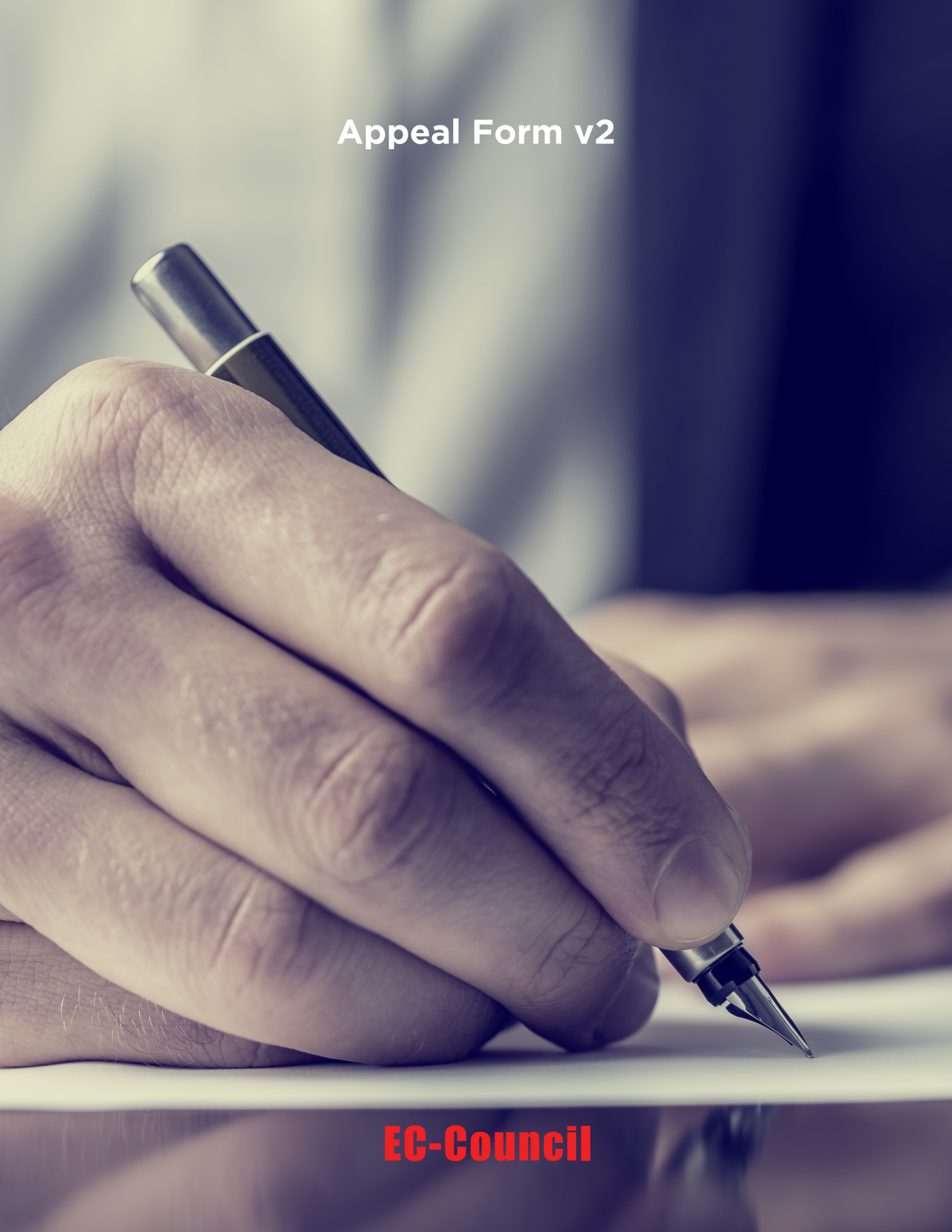
Phone : .....

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

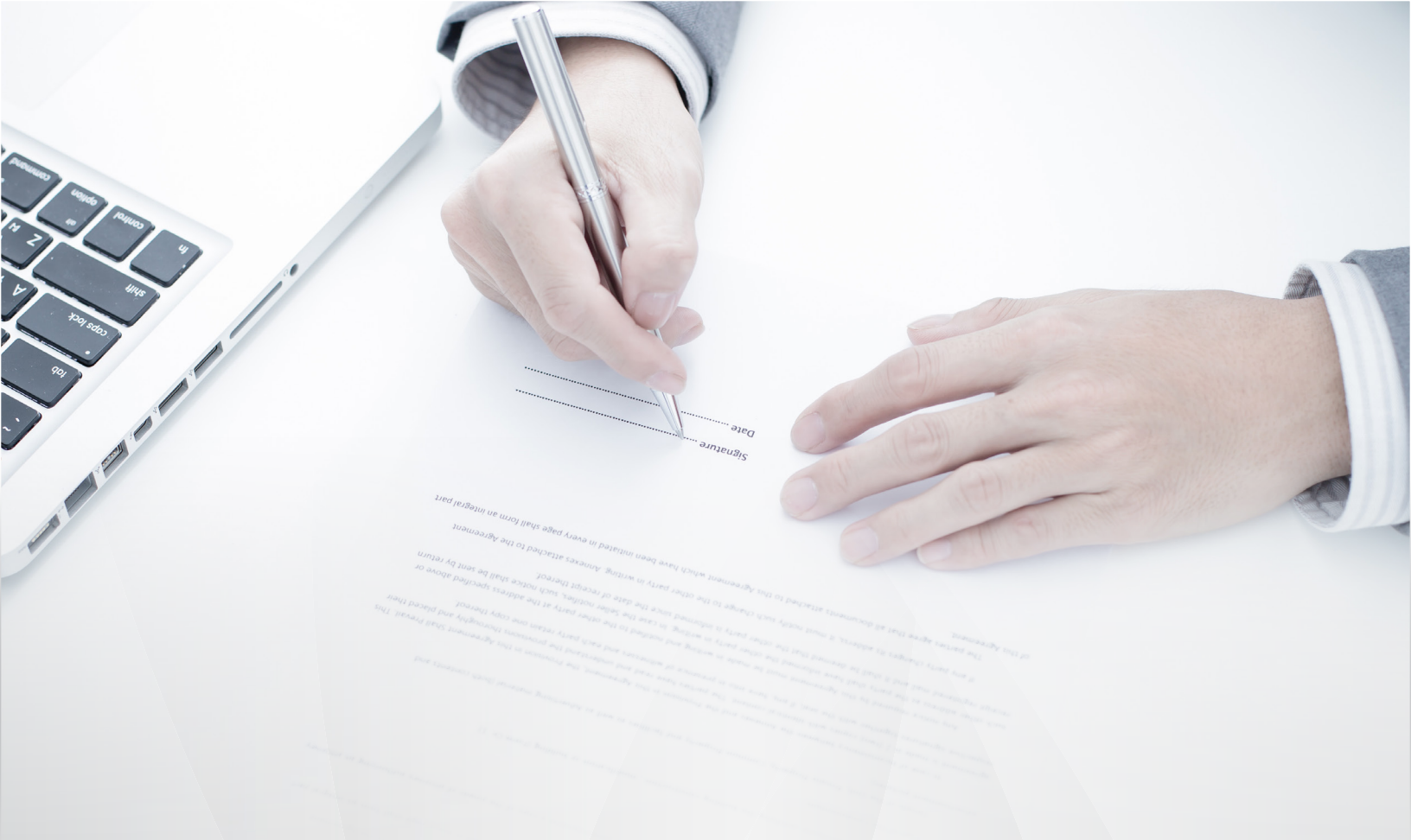
.....

Signature/Date

# Appeal Form v2



EC-Council



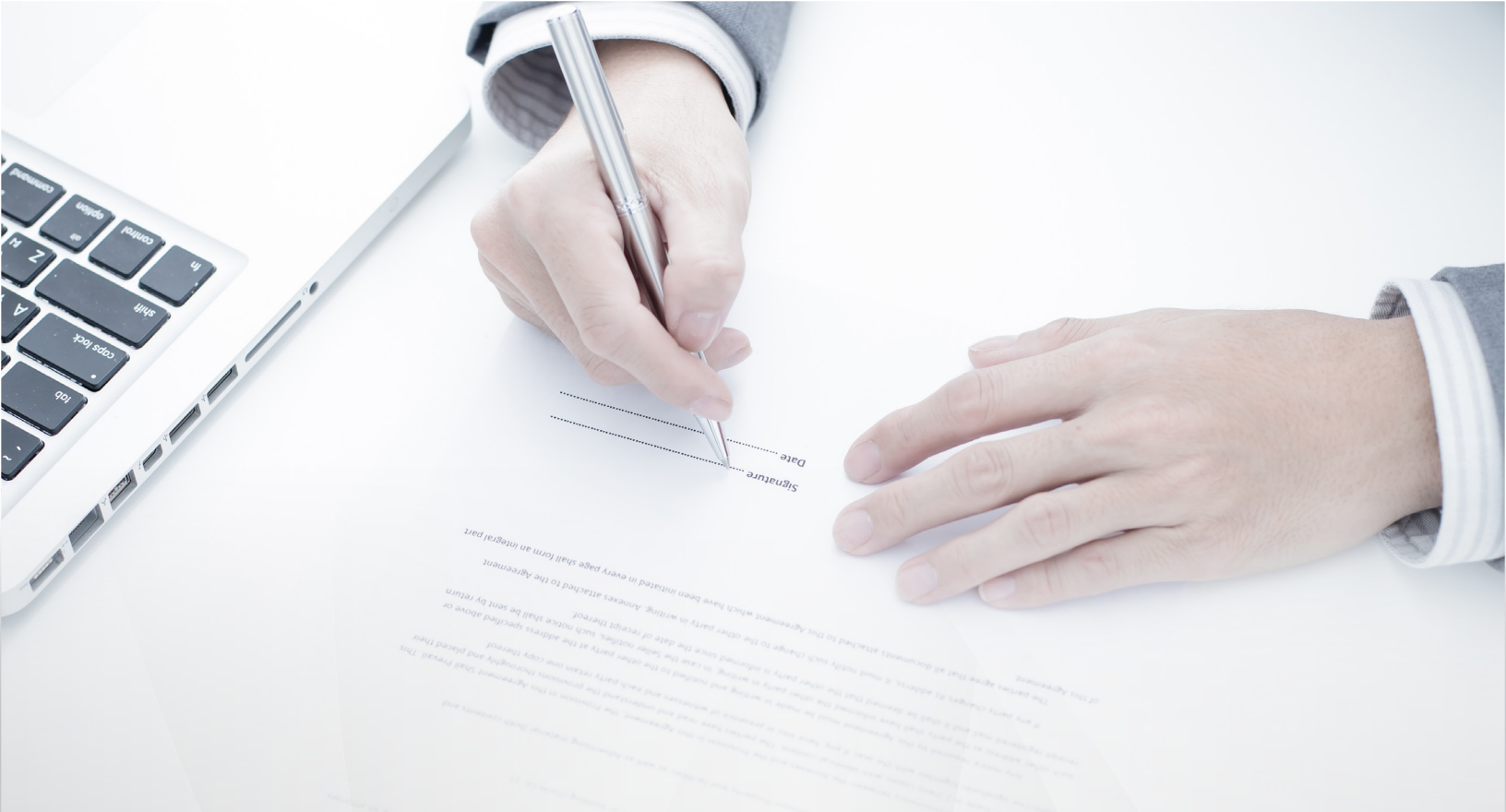

EC-Council adapts the term appeal as a reference to the mechanism by which a candidate/member can request the reconsideration of an EC-Council decision or exam. The appeal applicants should fill EC-Council Appeal Form and attach all supporting evidence. For instance, if the applicant is seeking EC-Council's 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 by raising a ticket at https://eccouncil. zendesk.com/anonymous_requests/new in seven (7) calendar days from exam date. 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 (Jan, April, July, Oct). 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 by raising a ticket at https://eccouncil.zendesk.com/anonymous_requests/new in seven (7) calendar days from exam date. 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 three (3) calendar days from exam date. All other appeals must be submitted within sixty (60) calendar days from EC-Council's written decision.

Kindly submit your appeal form to *https://eccouncil.zendesk.com/anonymous_re quests/new*

## SECTION A

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

Address (including city, state, and postal code) : .....

Phone Number : .....

Email Address : .....

.....

.....

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

## SECTION B

Membership No. : ..... Cert Award Date : .....

Title of Certification : ..... Cert Expiry Date : .....

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 : ..... Exam Title : .....

Test Centre Location : ..... Exam Version : .....

EC-Council Proctor Name (if known) : ..... Date Tested : .....

Exam Voucher No. : .....

# EC-Council Appeal Form

## SECTION D

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 (http://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

# 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 http://cert.eccouncil.org/

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 ANSI accredited certifications carry the ANSI logo", the Certified Ethical Hacker – ANSI 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

## 3. 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.



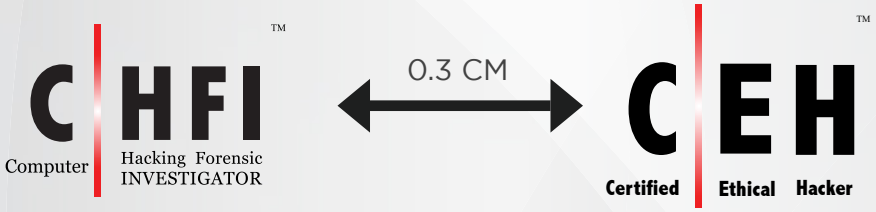
### b) Size

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.

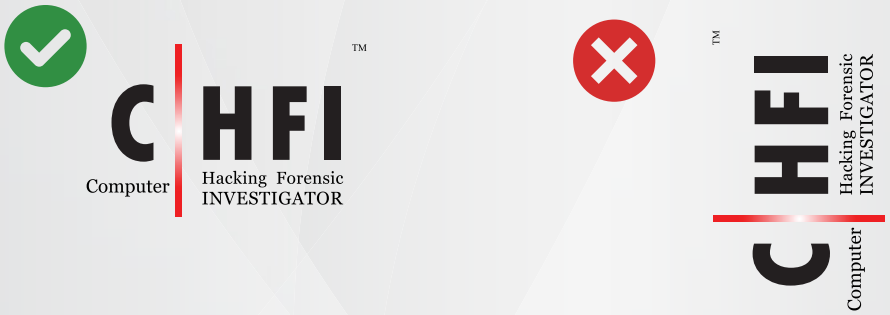



### d) Elements

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 attend CHFI training (online, instructor-led, computer-based, or academia learning), you are eligible to attempt the CHFI examination. If you opt for self-study, you must have minimum 2 years-experience in IT security, submit a complete eligibility form and email it to https://eccouncil.zendesk.com/anonymous_requests/new for approval and remit USD100 eligibility fee through our website at www.eccouncil.org/orders.htm. Once approved, you will be provided with an eligibility & voucher code that will allow you to register with ECC.

---

**What is 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 website at http://store.eccouncil.org/

---

**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.

---

**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.

---

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

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

---

**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

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

You will receive your welcome kit in eight weeks' time upon passing the exam.

**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.

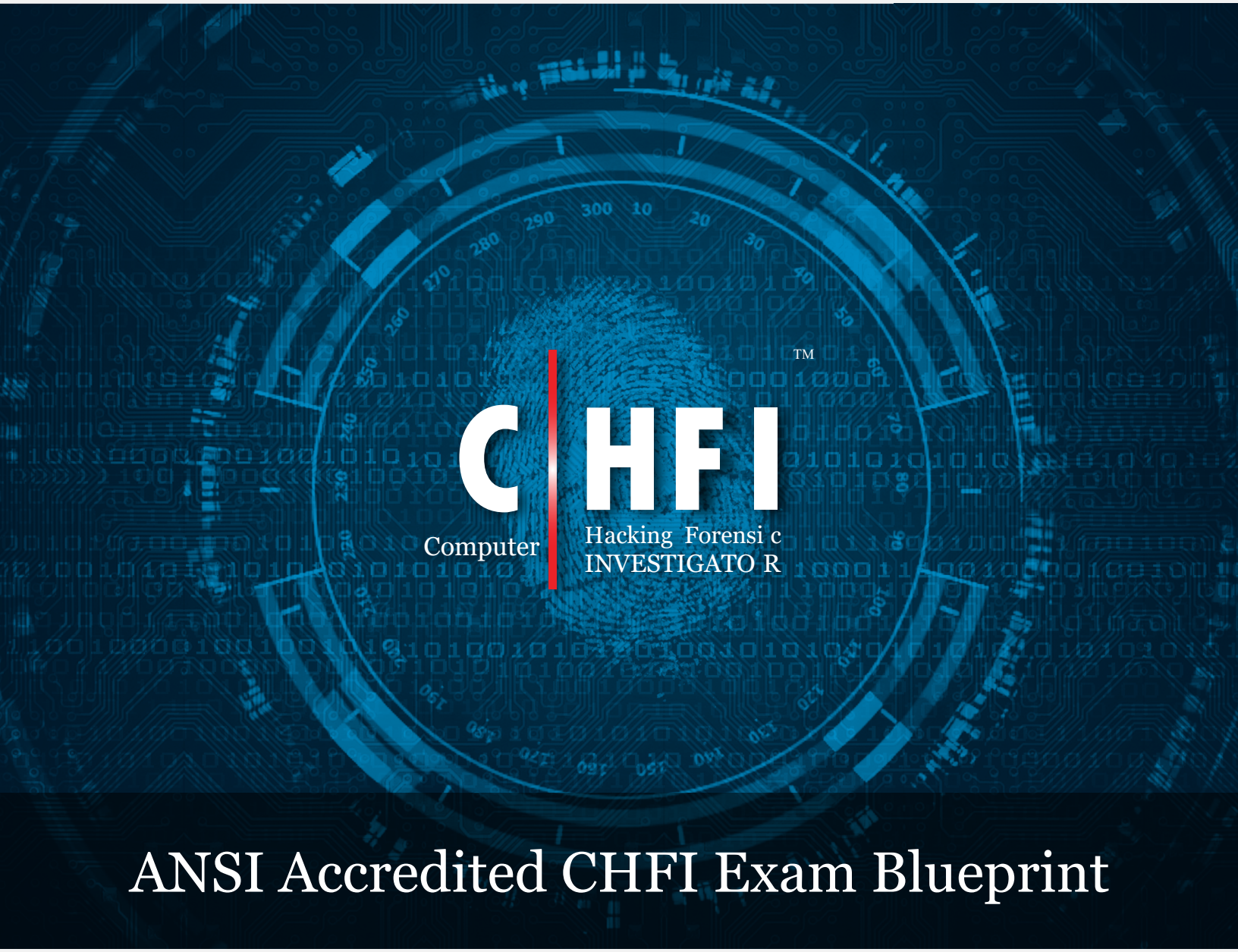
**What kind of questions can I expect in the exam? Do you have any exam pointers?**

The examination tests you on digital forensics related concepts, techniques and technology. Please refer to the 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.

EC-Council




# ANSI Accredited CHFI Exam Blueprint

## Appendix A

| Categories | Topics Covered | A minimally competent candidate will be able to: | Weightage | Items |
|---|---|---|---|---|
| **1. Forensic Science** | | | 15% | 22 |
| | 01. Computer Forensics Objective and Need | 1. Understand computer forensics, and explain the objectives and benefits of computer forensics | | |
| | | 2. Apply the key concepts of Enterprise Theory of Investigation (ETI) | | |
| | 02. Cyber Crime | 1. Fuse computer network attack analyses with criminal and counterintelligence investigations and operations | | |
| | 03. Web Applications and Webservers Attacks | 1. Identify elements of the crime | | |
| | 04. Email Crimes | 1. Understand various types of Web attacks | | |
| | 05. Network Attacks | 1. Understand various types of email attacks | | |
| | 06. Forensics on Mobile Devices | 1. Understand various types of network attacks | | |
| | 07. Cyber Crime Investigation | 1. Understand mobile based operating systems, their architectures, boot process, password/pin/pattern lock bypass mechanisms. | | |
| | 08. Computer Forensics Investigation Methodology | 1. Understand the importance of cybercrime investigation | | |
| | 09. Reporting a Cyber Crime | 1. Understand the methodology involved in Forensic Investigation | | |
| | 10. Expert Witness | 1. Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc. | | |
| | 11. Expert Witness | 1. Understand the role of expert witness in computer forensics | | |
| **2. Regulations, Policies and Ethics** | | | 10% | 15 |
| | 1. Searching and Seizing Computers with and without a Warrant | 1. Idenify legal issues and reports related to computer forensic investigations | | |
| | 2. Laws and Acts against Email Crimes | 1. Idenify legal issues and reports related to computer forensic investigations | | |
| | 3. Laws pertaining to Log Management | 1. Idenify legal issues and reports related to log management | | |
| | 4. Pertaining to Mobile Forensics | 1. Idenify internal BYOD and information security policies of the organization | | |
| | 5. Laws and Acts against Email Crimes | 1. Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action | | |
| | 6. General Ethics While Testifying | 1. Idenify legal issues and reports related to computer forensic investigations | | |

| **3. Digital Evidence** | | | 20% | 30 |
|---|---|---|---|---|
| | 01. Digital Evidence | 1. Apply the key concepts of Enterprise Theory of Investigation (ETI) | | |
| | 02. Types of Digital Evidence | 1. Undersand various types and nature of digital Evidence | | |
| | 03. Rules of Evidence | 1. Understand the best evidence rule | | |
| | 04. Electronic Evidence: Types and Collecting Potential Evidence | 1. Secure the electronic device or information source, Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence | | |
| | 05. Electronic Crime and Digital Evidence Consideration by Crime Category | | | |
| | 06. Computer Forensics Lab | 1. Create a forensically sound duplicate of the evidence (forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes HDD, SSD, CD/DVD, PDA, mobile phones, GPS, and all tape formats. | | |
| | 07. Understanding Hard Disks | 1. Perform MAC timeline analysis on a file system | | |
| | 08. Disk Partitions and Boot Process | 1. Undersatnd the Windows and Macintosh boot process, and handling volatile data | | |
| | 09. Understanding File Systems | 1. Understand File Systems and help in digital forensic investigations | | |
| | 10. Windows File Systems | 1. Understand Windows File Systems and help in digital forensic investigations | | |
| | 11. Linux File Systems | 1. Understand Linux File Systems and help in digital forensic investigations | | |
| | 12. Mac OS X File Systems | 1. Understand Mac OS X File Systems and help in digital forensic investigations | | |
| | 13. RAID Storage System | 1. Understand RAID Storage System and help in digital forensic investigations | | |
| | 14. File Carving | 1. Understand Carving Process and help in digital forensic investigations | | |
| | 15. Image Files | 1. Understand Image File Formats | | |
| | 16. Analyze Logs | 1. Understand Computer Security Logs | | |
| | 17. Database Forensics | 1. Perform MSSQL Forensics | | |
| | | 2. Perform MySQL Forensics | | |
| | 18. Email Headers | 1. Perform various steps involved in investigation of Email crimes | | |
| | 19. Analyzing Email headers | 1. Perform analysis of email headers and gather evidential information | | |
| | 20. Malware Analysis | 1. Perform static and dynamic malware analysis | | |

| | | | | |
|---|---|---|---|---|
| | 21. Mobile Operating Systems | 1. Understand the hardware and software characteristics of mobile devices | | |
| | | 2. Understand the different precautions to be taken before investigation | | |
| | | 3. Perform various processes involved in mobile forensics | | |
| **4. Procedures and Methodology** | | | 20% | 30 |
| | 01. Investigating Computer Crime | 1. "Exploit information technology systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property | | |
| | | 2. Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations " | | |
| | 02. Computer Forensics Investigation Methodology | 1. Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies, | | |
| | | 2. Determine and develop leads and identify sources of information in order to identify and prosecute the responsible parties to an intrusion investigation, | | |
| | | 3. Process crime scenes, | | |
| | | 4. Track and document Computer Network Defense incidents from initial detection through final resolution, | | |
| | | 5. Develop an investigative plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the internet, | | |
| | | 6. Identify outside attackers accessing the system from Internet or insider attackers, that is, authorized users attempting to gain and misuse non-authorized privileges, | | |
| | | 7. Coordinate with intelligence analysts to correlate threat assessment data | | |
| | 03. Digital Evidence Examination Process | 1. Ensure chain of custody is followed for all digital media acquired (e.g., indications, analysis, and warning standard operating procedures) | | |
| | | 2. Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration | | |
| | | 3. Assist in the gathering and preservation of evidence used in the prosecution of computer crimes | | |
| | | 4. Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures) | | |
| | | 5. Prepare reports to document analysis | | |

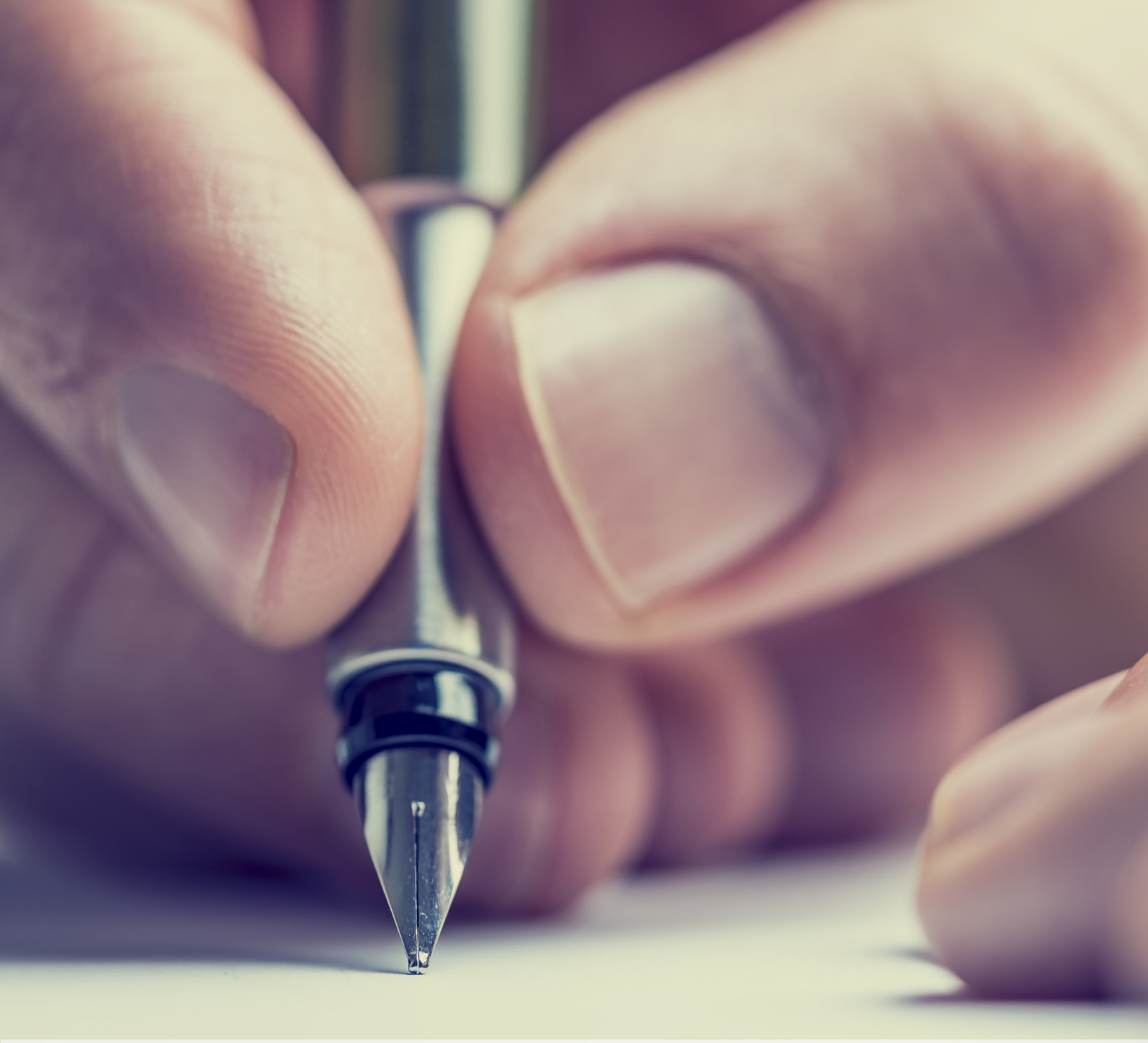
| | | | | |
|---|---|---|---|---|
| | 4. Encryption | 1. Decrypt seized data using technical means | | |
| | 5. First Responder | 1. Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals) | | |
| | | 2. Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents | | |
| | 6. First Response Basics | Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation | | |
| | 7. Roles of First Responder | 1. Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.) | | |
| | | 2. Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems | | |
| | | 3. Perform real-time Computer Network Defense Incident Handling (e.g., forensic collections, intrusion correlation/ tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs) | | |
| | | 4. Provide technical assistance on digital evidence matters to appropriate personnel | | |
| | | 5. Conduct interviews and interrogations of victims, witnesses and suspects | | |
| | | 6. Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence | | |
| | | 7. Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.) | | |
| | | 8. Independently conducts large-scale investigations of criminal activities involving complicated computer programs and networks | | |
| | 8. Data Acquisition and Duplication | 1. Examine recovered data for items of relevance to the issue at hand | | |
| | | 2. Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation | | |
| | | 3. Perform static media analysis | | |
| | | 4. Review forensic images and other data sources for recovery of potentially relevant information | | |

| | | | | |
|---|---|---|---|---|
| | | 5. Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration | | |
| | | 6. Identify data of intelligence of evidentiary value to support counterintelligence and criminal investigations | | |
| | | 7. Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise | | |
| | 9. Defeating Anti-forensics Techniques | 1. Identify Anti-Forensics Techniques | | |
| | | 2. Recover Deleted Files and Partitions | | |
| | | 3. Bypass Windows' and Applictions' Passwords | | |
| | | 4. Detect steganography and identify the hidden content | | |
| | 10. Log Management and Event Correlation | 1. Perform command and control functions in response to incidents | | |
| | | 2. Analyze computer generated threats | | |
| | 11. Network Forensics (Intrusion Detection Systems (IDS) | 1. Perform Computer Network Defense trend analysis and reporting | | |
| | | 2. Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis | | |
| | 12. Computer Forensics Reports and Investigative Report Writing | 1. Develop reports which organize and document recovered evidence and forensic processes used | | |
| | | 2. Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies | | |
| **5. Digital Forensics** | | | 25% | 37 |
| | 01. Recover Data | 1. Perform file signature analysis, Perform tier 1, 2, and 3 malware analysis | | |
| | 02. File System Analysis | 1. Analyze the file systems contents in FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 | | |
| | 03. Windows Forensics | 1. Collect Volatile and Non-Volatile Information | | |
| | | 2. Perform Windows registry analysis | | |
| | | 3. Perform Cache, Cookie, and History Analysis | | |
| | | 4. Peform Windows File Analysis | | |
| | | 5. Perform Metadata Investigation | | |
| | | 6. Analyze Windows Event Logs | | |

| | | | | |
|---|---|---|---|---|
| | 4. Linux Forensics | 1. Collect Volatile and Non-Volatile Information | | |
| | | 2. Use Various Shell Commands | | |
| | | 3. Examine Linux Log files | | |
| | 5. MAC Forensics | 1. Examine MAC Forensics Data | | |
| | | 2. Examine MAC Log Files | | |
| | | 3. Analyze MAC Directories | | |
| | 6. Recovering the Deleted Files and Partitions | 1. Examine MAC Forensics Data | | |
| | | 2. Examine MAC Log Files | | |
| | | 3. Analyze MAC Directories | | |
| | 7. Steganography and Image File Forensics | 1. Detect steganography | | |
| | | 2. Process images in a forensically sound manner | | |
| | 8. Steganalysis | 1. Perform steganalysis to recover the data hidden using steganography | | |
| | 9. Application Password Crackers | 1. Undersatnd various password cracking techniques | | |
| | | 2. Crack the password to recover protected information and data | | |
| | 10. Investigating and Analyzing Logs | 1. Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion | | |
| | | 2. Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion | | |
| | 11. Investigating Network Traffic | 1. Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts | | |
| | 12. Investigating Wireless Attacks | 1. Investigate wireless attacks | | |
| | 13. Web Attack Investigation | 1. Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security | | |
| | 14. Investigating Email Crime and Violation | 1. Perform various steps involved in investigation of email crimes | | |
| | 15. Mobile Forensic Process | 1. Perform various processes involved in mobile forensics | | |
| | 16. Cloud Forensics | 1. Perform investigation on cloud storage services such as Google Drive and Dropbox. | | |
| | 17. Malware Forensics | 1. Understand and perform static and dynamic malware analysis | | |
| | 18. Defeating Anti-Forensic Techniques | 1. Bypass anti-forensic techniques and access the required resources | | |

| **6. Tools/Systems/ Programs** | | | 10% | 16 |
|---|---|---|---|---|
| | 01. First Responder Toolkit | 1. Maintain deployable Computer Network Defense toolkit (e.g., specialized Computer Network Defense software/hardware) to support incident response team mission | | |
| | 02. Windows Forensic Tools (Helix3 Pro, X-Ways Forensics, Windows Forensic Toolchest (WFT), Autopsy, The Sleuth Kit (TSK), etc.) | 1. Recognize and accurately report forensic artifacts indicative of a particular operating system | | |
| | | 2. Perform live forensic analysis (e.g., using Helix in conjunction with LiveView) | | |
| | | 3. Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment | | |
| | | 4. Use data carving techniques (e.g., Autposy) to extract data for further analysis | | |
| | | 5. Decrypt seized data using technical means | | |
| | 03. Data Acquisition Software Tools UltraKit Forensic Falcon, etc.) | 1. Perform data acquisition (using UltraKit, Active@ Disk Image, DriveSpy, etc.) | | |
| | 04. Tools to defeat Anti-Forensics | 1. Use File Recovery Tools (e.g., Recover My Files, EaseUS Data Recovery Wizard, etc.), Partition Recovery Tools (e.g., Active@ Partition Recovery, 7-Data Partition Recovery, Acronis Disk Director Suite, etc.), Rainbow Tables Generating Tools (e.g., rtgen, Winrtgen), Windows Admin Password Resetting Tools (e.g., Active@ Password Changer, Windows Password Recovery Bootdisk, etc.). | | |
| | | 2. Understand the usage of Application Password Cracking Tools (e.g., Passware Kit Forensic, SmartKey Password Recovery Bundle Standard, etc.), Steganography Detection Tools (e.g., Gargoyle Investigator™ Forensic Pro, StegSecret, etc.) | | |
| | 05. Steganography Tools | 1. Use tools to locate and recover image files | | |
| | 06. Database Forensics Tools | 1. Use tools to perform database forensics (e.g., Database Forensics Using ApexSQL DBA, SQL Server Management Studio, etc. ) | | |
| | 07. Password Cracking Tools | 1. Use tools to recover obstrcted evidence | | |
| | 8. Network Forensics Tools | 1. Use network monitoring tools to capture real-time traffic spawned by any running malicious code after identifying intrusion via dynamic analysis | | |
| | | 2. Understand the working of wireless forensic tools (e.g., NetStumbler, NetSurveyor, Vistumbler, WirelessMon, Kismet, OmniPeek, CommView for Wi-Fi, Wi-Fi USB Dongle: AirPcap, tcpdump, KisMAC, Aircrack-ng Suite<br>AirMagnet WiFi Analyzer, MiniStumbler, WiFiFoFum, NetworkManager, KWiFiManager, Aironet Wireless LAN, | | |

| | | | | |
|---|---|---|---|---|
| | 9. Web Security Tools, Firewalls, Log Viewers, and Web Attack Investigation Tools | 1. Understand the working of web Security Tools, Firewalls, Log Viewers, and Web Attack Investigation Tools (e.g., Acunetix Web Vulnerability Scanner, Falcove Web Vulnerability Scanner, Netsparker, N-Stalker Web Application Security Scanner, Sandcat, Wikto, WebWatchBot, OWASP ZAP, dotDefender, IBM AppScan, ServerDefender, Deep Log Analyzer, WebLog Expert, etc.) | | |
| | 10. Cloud Forensics Tools | 1. Use Cloud Forensics Tools (e.g., UFED Cloud Analyzer, WhatChanged Portable, WebBrowserPassView, etc.) | | |
| | 11. Malware Forensics Tools | 1. Use Malware Analysis Tools (e.g., VirusTotal, Autoruns for Windows, RegScanner, MJ Registry Watcher, etc.) | | |
| | 12. Email Forensics Tools | 1. Use email forensic tools (e.g.,Stellar Phoenix Deleted Email Recovery, Recover My Email, Outlook Express Recovery, Zmeil, Quick Recovery for MS Outlook, Email Detective, Email Trace - Email Tracking, R-Mail, FINALeMAIL, eMailTrackerPro, Paraben's email Examiner, Network Email Examiner by Paraben, DiskInternal's Outlook Express Repair, Abuse.Net, MailDetective Tool, etc.) | | |
| | 13. Mobile Forensics Software and Hardware Tools | 1. Use mobile forensic software tools (e.g., Oxygen Forensic Suite 2011, MOBILedit! Forensic, BitPim, SIM Analyzer, SIMCon, SIM Card Data Recovery, Memory Card Data Recovery, Device Seizure, Oxygen Phone Manager II, etc.) | | |
| | | 2. Use mobile forensic software tools | | |
| | 14. Report Writing Tools | 1. Create well formatted computer forensic reports | | |



# AGREEMENTS

## Appendix B

# NON-DISCLOSURE AGREEMENT

## EC-Council

# EC-Council NON-DISCLOSURE AGREEMENT

EC-Council ("Disclosing Party") intends to make available or have made available to you ("Receiving Party")certain proprietary and confidential information including but not limited to exam items in connection with EC-Council certification ("Purpose"), in accordance with the terms of this Confidentiality and Non-Disclosure Agreement ("Agreement"). Such information so provided to the Receiving Party 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 prepared by Receiving Party or any of its affiliates or Representatives which contain or reflect, or are generated from, such information shall be collectively referred to herein as the "Confidential Information." The parties now agree as set forth below.

Receiving Party 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. Receiving Party further agrees not to disclose that they have received Confidential Information without the prior written consent of Disclosing Party.

Disclosing Party shall be deemed the owner of all Confidential Information, including all patent, copyright, trademark and other proprietary rights and interests therein. Receiving Party acknowledges and agrees that nothing contained in this Agreement shall be construed as (i) granting any rights 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.

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 BY RECEIVING PARTY AS A RESULT OF RECEIVING PARTY'S RECEIPT OR USE OF ANY INFORMATION 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 Receiving Party or its affiliates or Representatives, and all electronically stored copies) will be returned or destroyed.

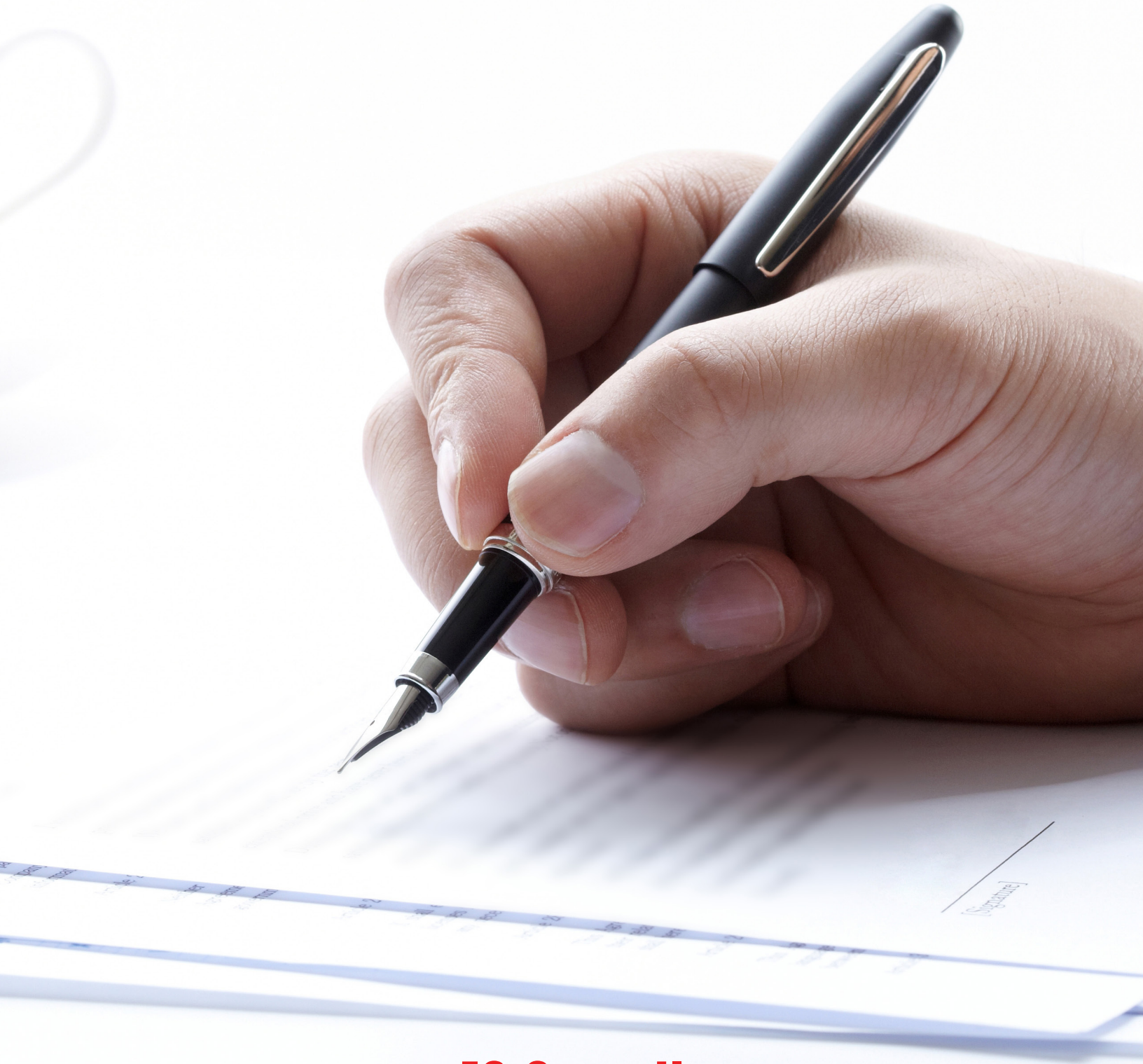
All Confidential Information shall continue to be subject to the terms of this Agreement until three years from the disclosure thereof. This Agreement shall be governed by and construed in accordance with the laws of the State of New Mexico, without regard to its conflict of law principles.

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.

# CANDIDATE APPLICATION AGREEMENT

(Version 3.0) w.e.f. February 1st, 2012



EC-Council

# EC-Council
# CANDIDATE APPLICATION AGREEMENT

## 1. PURPOSE

1.1 International Council of E-Commerce Consultants ("EC-COUNCIL") distributes, licenses, and promotes e-Business and Security certification programs. To provide appropriate support for its programs, EC-COUNCIL has created the following credentials below whereby individuals may become certified subject to submitting this Agreement.

- CEP – Certified e-Business Professional
- CEH – Certified Ethical Hacker
- CHFI – Computer Hacking Forensic Investigator
- CNDA – Certified Network Defense Architect
- CCISO – Certified Chief Information Security Officer
- Wireless5
- Network5
- ECSS - EC-Council Certified Security Specialist
- LPT – Licensed Penetration Tester
- MSS – Master of Security Science
- CEI – Certified EC-Council Instructor
- ENSA – EC-Council Network Security Administrator
- ECSP – EC-Council Certified Secure Programmer
- CSAD – Certified Secure Application Developer
- ECVP – EC-Council Certified Voice over IP Professional.

1.2 Through passing certification exams, successful participants in these programs may become authorized to provide corresponding services and to use the EC-COUNCIL Marks pertaining to the certification program(s) that the participant has completed. Individuals may participate in one or more of these certification programs. Successful completion of one certification program allows the participant make claims regarding certification only with respect to the scope for which certification has been granted and does not entitle participant to use the Marks or provide the services pertaining to any other program.

## 2. DEFINITIONS

2.1 Program means one of the certification programs offered by EC-COUNCIL under this EC-COUNCIL Candidate Application Agreement ("Agreement"). Each Program includes a formally documented process whereby individuals may demonstrate competence relating to infrastructure software and one or more EC-COUNCIL products. The Programs include the CEP, CEH, CHFI, CNDA, CCISO, Wireless5, Network5, ECSA, ECSS, LPT, MSS, CEI, ECSP, ECVP and CSAD.

2.2 MARKS means, as the case may be, the EC-COUNCIL marks and logos, and the certification and Program marks and logos.

# EC-Council
# CANDIDATE APPLICATION AGREEMENT

## 3. CERTIFICATION

Your Program certification is based on Your successful completion of the required testing and Your compliance with the requirements described in the current corresponding Program brochure. You acknowledge that EC-COUNCIL has the right to change at any time the requirements for obtaining any Program certification. NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, EC-COUNCIL HAS THE RIGHT NOT TO GRANT YOUR CERTIFICATION IF EC-COUNCIL DETERMINES IN GOOD FAITH THAT YOUR CERTIFICATION OR USE OF THE CORRESPONDING MARKS WILL ADVERSELY AFFECT EC-COUNCIL.

## 4. TRANSFER OF CERTIFICATION

In the event that You have attained Your certification, You will retain Your certification status if You leave Your current employment and/or begin working with a new organization. However, You may not transfer Your certification to another person.

## 5. YOUR OBLIGATIONS

5.1 You must adhere to the following EC-Council Policies:

- Code of Ethics (https://cert.eccouncil.org/code-of-ethics.html)
- Certification Exam (https://cert.eccouncil.org/certification-exam-policy.html)
- Exam Retake (https://cert.eccouncil.org/exam-retake-policy.html)
- Exam Extension (https://cert.eccouncil.org/exam-voucher-extension-policy.html)
- Exam Voucher (https://cert.eccouncil.org/exam-voucher-policy.html)

5.2 You must accept the terms stated under EC-Council Non-Disclosure Agreement. (url:https://cert.eccouncil.org/wp-content/uploads/2011/11/Non-Disclosure Agreement-v1.0-15112011.pdf)

5.3 Should your application be approved, you would be furnished with a Candidate Certification Agreement which you need to agree with in order to become a candidate of a program certification examination.

## 6. TERM AND TERMINATION

6.1 Term. This Agreement will begin on the date you receive written notice from EC-COUNCIL that you have met all the requirements necessary to sit for a particular certification examination and will terminate as provided in this Agreement. THIS AGREEMENT WILL NOT TAKE EFFECT UNTIL EC-COUNCIL HAS NOTIFIED you IN WRITING THAT ALL PROGRAM REQUIREMENTS HAVE BEEN MET, INCLUDING your ACCEPTANCE OF THE TERMS OF THIS AGREEMENT.

6.2 Termination by EC-COUNCIL. Without prejudice to any rights it may have under this Agreement or in law, equity, or otherwise, EC-COUNCIL may terminate this Agreement upon the occurrence of any one or more of the following events (each a “Default”):

6.2.1 If You fail to perform any of Your obligations under this Agreement;
6.2.2 If You engage in any unlawful activities or have previous conviction(s) of unlawful activity.
6.2.3 In the event of a Default, EC-COUNCIL may immediately terminate this Agreement with no period for correction and without further notice.

6.3 Effect of Termination. Upon termination of this Agreement for any reason, You must immediately cease all display, advertising, and other use of the MARKS and will return any and everything that bears EC-COUNCIL. Marks. Upon termination, all rights granted under this Agreement will immediately and automatically revert to EC-COUNCIL.

## 7. OWNERSHIP

No title to or ownership of the MARKS that may be provided to You pursuant to this Agreement is transferred to You. EC-COUNCIL owns and retains all title and ownership of all intellectual property rights in the products, documentation, and related materials. 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 products acquired by reason of Your certification under this Agreement.

## 8. RESERVATION OF RIGHTS AND GOOD WILL IN EC-Council

EC-COUNCIL retains all rights not expressly conveyed to You by this Agreement. You 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 have no rights of any kind whatsoever with respect to the MARKS licensed under this Agreement.

## 9. NO REGISTRATION BY YOU

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 agree not to register or use as Your own any internet domain name which contains EC-COUNCIL's MARKS or other trademarks in whole or in part or any other name which is confusingly similar thereto. This section will survive the expiration or other termination of this Agreement.

## 10. PROTECTION OF RIGHTS

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. In addition, if at any time EC-COUNCIL requests that You discontinue using the MARKS and/or substitute using a new or different mark, You will 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.

## 11. INDEMNIFICATION BY YOU

You 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 by reason of Your performance or non-performance under this Agreement. In the event EC-COUNCIL seeks indemnification under this Section, EC-COUNCIL will immediately notify You in writing of any claim or proceeding brought against it for which it seeks indemnification under this Agreement. In no event may You enter into any third party agreements that would in any manner whatsoever affect the rights of, or bind, EC-COUNCIL in any manner, without the prior written consent of EC-COUNCIL.

## 12. LIMITATION OF LIABILITY

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

## 13. GENERAL PROVISIONS

13.1 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 provisions, and venue of any actions will be proper either in the courts of the State of New Mexico of the United States of America or in the country of EC-COUNCIL's residence, if other than the United States.

13.2 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.

13.3 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.

13.4 Independent Contractors. You acknowledge that You and EC-COUNCIL are independent contractors and You agree that You will not represent Yourself as, an employee, agent, or legal representative of EC-COUNCIL.

13.5 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.

13.6 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.

13.7 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.

## 14. CONFIDENTIALITY

14.1. EC-COUNCIL may, from time to time provide information to You which it considers to be confidential shall, if tangible, be marked as such or, if communicated orally, designated at the time and promptly confirmed in writing as such. Information that is so marked or designated and confirmed, and the Licensed Software regardless of form or designation, shall be "Confidential Information" under this Agreement.

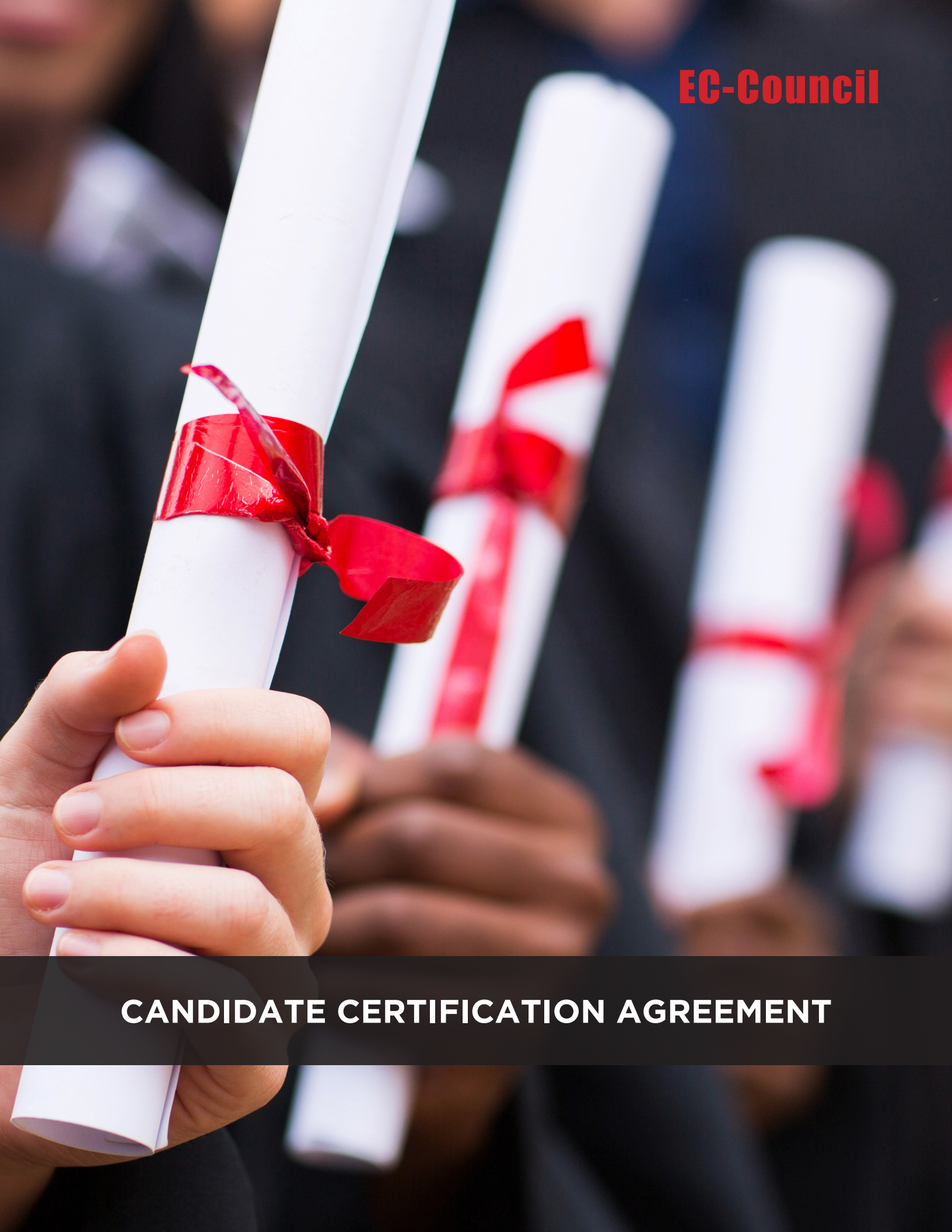
14.2. Confidential Information shall be held in trust and used only as necessary for the performance of this Agreement. Confidential Information shall be treated with the same degree of care to avoid disclosure to third parties as is used with respect to the Your own Confidential Information, but not less than a reasonable degree of care.

14.3 Confidential Information shall be disclosed only to those employees or agents of a party who have a need to know such information and are under binding obligation of confidentiality with respect to any such information received. Confidential Information shall not be disclosed by You to any other third party without the prior written consent of EC-COUNCIL. You agree to defend, indemnify and save EC-COUNCIL harmless from and against any and all damages, including reasonable attorney's fees, sustained as a result of the unauthorized use or disclosure of the other party's Confidential Information.

14.3.1 Your obligation of confidentiality hereunder shall terminate when You can establish that the Confidential Information (a) at the time of its disclosure was known by You; (b) is already in the public domain or becomes generally known or published without breach of this Agreement; (c) is lawfully disclosed by a third party free to disclose such information; (d) is subsequently independently developed by You without reference to or use of the Confidential Information; or (d) is legally required to be disclosed provided that You promptly notify EC-COUNCIL so as to permit suchEC-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.

14.3.2 You further agree that, except as otherwise stated in this Agreement, You will not use the name of EC-COUNCIL either expressed or implied in any of its advertising or sales promotional material.

**Prior to attempting an EC-Council exam, candidates are required to agree to EC-Council Candidate Application Agreement 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 EC-Council Candidate Application Agreement 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.**




# CANDIDATE CERTIFICATION AGREEMENT

# EC-Council
# CANDIDATE CERTIFICATION AGREEMENT

## 1. PURPOSE

1.1 International Council of E-Commerce Consultants ("EC-Council") distributes, licenses, and promotes e-Business and Security certification programs. To provide appropriate support for its programs, EC-Council has created the following credentials below whereby individuals may become certified subject to submitting this Agreement.

- CEP – Certified e-Business Professional
- CEH – Certified Ethical Hacker
- CHFI – Computer Hacking Forensic Investigator
- CNDA – Certified Network Defense Architect
- SCUS
  Security5
- Wireless5
  Network5
- ECSA – EC-Council Certified Security Analyst
- ECSS - EC-Council Certified Security Specialist
- LPT – Licensed Penetration Tester
- MSS – Master of Security Science
- CEI – Certified EC-Council Instructor
- ENSA – EC-Council Network Security Administrator
- ECSP – EC-Council Certified Secure Programmer
- CSAD – Certified Secure Application Developer
- ECVP – EC-Council Certified Voice over IP Professional.

1.2 Through passing certification exams, successful participants in these programs may become authorized to provide corresponding services and to use the EC-Council Marks pertaining to the certification program(s) that the participant has completed. Individuals may participate in one or more of these certification programs. Successful completion of one certification program allows the participant make claims regarding certification only with respect to the scope for which certification has been granted and does not entitle participant to use the Marks or provide the services pertaining to any other program.

## 2. DEFINITIONS

2.1 Program means one of the certification programs offered by EC-Council under this EC-Council Candi-date Certification Agreement ("Agreement"). Each Program includes a formally documented process whereby individuals may demonstrate competence relating to infrastructure software and one or more EC-Council products.

2.2 MARKS means, as the case may be, the EC-Council marks and logos, and the certification and Program marks and logos.

2.3 EC-COUNCIL Accredited Training Center or ATC means professional instructors, training organiza-tions, or businesses. They deliver top-notch professional training on e-Business subjects. EC-Council Test Center or ETC means any organization that has been approved

2.4 EC-Council Test Center or ETC means any organization that has been approved by EC-Council to administer EC-Council certification exams to students.

## 3.CERTIFICATION

Your Program certification is based on Your successful completion of the required testing and Your compli-ance with the requirements described in the current corresponding Program brochure. You acknowledge that EC-Council has the right to change at any time the requirements for obtaining or maintaining any Program certification. Once certification is granted, You may maintain Your certification by completing, within the time frame specified by EC-Council, all continuing certification requirements (if any) that corre-spond with Your particular Program certification. You also agree to comply with the relevant provisions of the certification program. You are solely responsible for keeping Yourself informed of EC-Council's continu-ing certification requirements and for maintaining Your certification. If You do not complete the continuing certification requirements within the time frame specified by EC-Council, Your certification for that particu-lar Program will be suspended or revoked without further notice, and all rights pertaining to that certifica-tion (including the right to use the applicable Marks) will terminate. NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, EC-COUNCIL HAS THE RIGHT NOT TO GRANT OR RENEW YOUR CERTIFICA-TION IF EC-COUNCIL DETERMINES IN GOOD FAITH THAT YOUR CERTIFICATION OR USE OF THE CORRE-SPONDING MARKS WILL ADVERSELY AFFECT EC-COUNCIL.

## 4.TRANSFER OF CERTIFICATION

You retain Your certification status if You leave Your current employment and/or begin working with a new organization. However, You may not transfer Your Program certification to another person.

## 5. YOUR OBLIGATIONS

5.1 You must adhere to the following EC-Council Policies:

- Code of Ethics (https://cert.eccouncil.org/?page_id=330)
- Certification Exam (https://cert.eccouncil.org/?page_id=358)
- Exam Retake (https://cert.eccouncil.org/?page_id=1234)
- Exam Extension (https://cert.eccouncil.org/?page_id=1239)
- Exam Voucher (https://cert.eccouncil.org/?page_id=1241)

5.2 mustacceptthetermsstatedunderEC-CouncilNon-DisclosureAgreement.(url:https://cert.eccouncil.org/wp-content/uploads/2011/11/Non-Disclosure-Agreement-v1.0-15112011.pdf)

## 6. TERM AND TERMINATION

6.1 Term. This Agreement will begin on the date You receive written notice from EC-Council that You have met all the requirements necessary to receive Your particular Program certification and will terminate as provided in this Agreement. THIS AGREEMENT WILL NOT TAKE EFFECT UNTIL EC-COUNCIL HAS NOTI-FIED YOU IN WRITING THAT ALL PROGRAM REQUIREMENTS HAVE BEEN MET, INCLUDING YPUR ACCEPT-ANCE OF THE TERMS OF THIS AGREEMENT. You also agree to

comply with this Agreement when you open the certification welcome kit envelope seal. If You later upgrade Your status to include any other Program certifications, this Agreement will remain in effect and govern Your right to use any new certifi-cation MARKS.

6.2 Termination by EC-COUNCIL. Without prejudice to any rights it may have under this Agreement or in law, equity, or otherwise, EC-Council may terminate this Agreement upon the occurrence of any one or more of the following events (each called a "Default"):

6.2.1 If You fail to perform any of Your obligations under this Agreement;

6.2.2 If any actual or potential adverse publicity or other information about You or Your use of the MARKS causes EC-Council, in its sole judgment, to believe that EC-Council's reputation will be adversely affected.

6.3 In the event of a Default, EC-Council will give You thirty (30) days from receipt of notice to correct the Default. If You fail to correct the Default within the notice period, this Agreement will automatically terminate on the last day of the notice period without further notice. EC-Council will have no liability to You under any circumstances for termination of this Agreement.

6.4 Effect of Termination. Upon termination of this Agreement for any reason, You must immediately cease all display, advertising, and other use of the MARKS and will return all certificates, badges or other trademark collateral to EC-Council. Upon termination, all rights granted under this Agreement will immediately and automatically revert to EC-Council.

## 7. OWNERSHIP

No title to or ownership of the MARKS or of any ATC courseware provided to You pursuant to this Agreement is transferred to You. EC-Council owns and retains all title and ownership of all intellectual property rights in the products, documentation, and related materials and, all modifications to and derivative works from software acquired as a Program certification holder which are made by You, EC-Council or any third party. 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 products acquired by reason of Your certification under this Agreement.

## 8. RESERVATION OF RIGHTS AND GOOD WILL IN EC-Council

EC-Council retains all rights not expressly conveyed to You by this Agreement. You 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 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.

## 9. NO REGISTRATION BY YOU

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, certifi-cation 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 agree not to register or use as Your own any internet domain name which contains EC-Council's MARKS or other trade-marks in whole or in part or any other name which is confusingly similar thereto. This section will survive the expiration or other termination of this Agreement.

## 10.PROTECTIONOFRIGHTS

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. In addition, if at any time EC-Council requests that You discontinue using the MARKS and/or substitute using a new or different mark, You will 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.

## 11. INDEMNIFICATION BY YOU

You 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 performance or nonperformance 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 LICENSED SERVICES. In the event EC-Council seeks indemnification under this Section, EC-Council will immediately notify You in writing of any claim or proceeding brought against it for which it seeks indemnifi-cation under this Agreement. In no event may You enter into any third party agreements that would in any manner whatsoever affect the rights of, or bind, EC-Council in any manner, without the prior written consent of EC-Council.

## 12.LIMITATION OF LIABILITY

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

## 13. GENERAL PROVISIONS

13.1 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 provisions, and venue of any actions will be proper either in the courts of the State of New Mexico of the United States of America or in the country of EC-Council's residence, if other than the United States.

13.2 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.

13.3 Assignment. Neither this Agreement nor any of Your rights or obligations arising under this Agree-ment 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.

13.4 Independent Contractors. You acknowledge that You and EC-Council are independent contractors and You agree that You will not represent Yourself as, an employee, agent, or legal representative of EC-Council.

13.5 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.

13.6 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.

13.7 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.