CERTIFIED LEAD FORENSICS EXAMINER

Candidate Handbook

Table of Contents

SECTION I: INTRODUCTION

About PECB

PECB is a certification body that provides education[1], certification, and certificate programs for individuals on a wide range of disciplines.

Through our presence in more than 150 countries, we help professionals demonstrate their competence in various areas of expertise by providing valuable evaluation, certification, and certificate programs against internationally recognized standards.

Our key objectives are:

1. Establishing the minimum requirements necessary to certify professionals and to grant designations
2. Reviewing and verifying the qualifications of individuals to ensure they are eligible for certification
3. Maintaining and continually improving the evaluation process for certifying individuals
4. Certifying qualified individuals, granting designations and maintaining respective directories
5. Establishing requirements for the periodic renewal of certifications and ensuring that the certified individuals are complying with those requirements
6. Ascertaining that PECB professionals meet ethical standards in their professional practice
7. Representing our stakeholders in matters of common interest
8. Promoting the benefits of certification and certificate programs to professionals, businesses, governments, and the public

Our mission

Provide our clients with comprehensive examination, certification, and certificate program services that inspire trust and benefit the society as a whole.

Our vision

Become the global benchmark for the provision of professional certification services and certificate programs.

Our values

Integrity, Professionalism, Fairness

[1] Education refers to training courses developed by PECB and offered globally through our partners.

The Value of PECB Certification

Global recognition
PECB credentials are internationally recognized and endorsed by many accreditation bodies, so professionals who pursue them will benefit from our recognition in domestic and international markets.

The value of PECB certifications is validated by the accreditation from the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923) and the Korean Accreditation Board (KAB-PC-08) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. The value of PECB certificate programs is validated by the accreditation from the ANSI National Accreditation Board (ANAB-Accreditation ID 1003) under ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB is an associate member of The Independent Association of Accredited Registrars (IAAR), a full member of the International Personnel Certification Association (IPC), a signatory member of IPC MLA, and a member of Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine, and ITCC. In addition, PECB is an approved Licensed Partner Publisher (LPP) from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), is approved by Club EBIOS to offer the EBIOS Risk Manager Skills certification, and is approved by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer DPO certification. For more detailed information, click here.

High-quality products and services
We are proud to provide our clients with high-quality products and services that match their needs and demands. All of our products are carefully prepared by a team of experts and professionals based on the best practices and methodologies.

Compliance with standards
Our certifications and certificate programs are a demonstration of compliance with ISO/IEC 17024 and ASTM E2659. They ensure that the standard requirements have been fulfilled and validated with adequate consistency, professionalism, and impartiality.

Customer-oriented service
We are a customer-oriented company and treat all our clients with value, importance, professionalism, and honesty. PECB has a team of experts who are responsible for addressing requests, questions, and needs. We do our best to maintain a 24-hour maximum response time without compromising the quality of the services.

Flexibility and convenience
Online learning opportunities make your professional journey more convenient as you can schedule your learning sessions according to your lifestyle. Such flexibility gives you more free time, offers more career advancement opportunities, and reduces costs.

PECB Code of Ethics

The Code of Ethics represents the highest values and ethics that PECB is fully committed to follow, as it recognizes the importance of them when providing services and attracting clients.

The Compliance Division makes sure that PECB employees, trainers, examiners, invigilators, partners, distributors, members of different advisory boards and committees, certified individuals, and certificate holders (hereinafter "PECB professionals") adhere to this Code of Ethics. In addition, the Compliance Division consistently emphasizes the need to behave professionally and with full responsibility, competence, and fairness in service provision with internal and external stakeholders, such as applicants, candidates, certified individuals, certificate holders, accreditation authorities, and government authorities.

It is PECB's belief that to achieve organizational success, it has to fully understand the clients and stakeholders' needs and expectations. To do this, PECB fosters a culture based on the highest levels of integrity, professionalism, and fairness, which are also its values. These values are integral to the organization, and have characterized the global presence and growth over the years and established the reputation that PECB enjoys today.

PECB believes that strong ethical values are essential in having healthy and strong relationships. Therefore, it is PECB's primary responsibility to ensure that PECB professionals are displaying behavior that is in full compliance with PECB principles and values.

PECB professionals are responsible for:

1. Displaying professional behavior in service provision with honesty, accuracy, fairness, and independence
2. Acting at all times in their service provision solely in the best interest of their employer, clients, the public, and the profession in accordance with this Code of Ethics and other professional standards
3. Demonstrating and developing competence in their respective fields and striving to continually improve their skills and knowledge
4. Providing services only for those that they are qualified and competent and adequately informing clients and customers about the nature of proposed services, including any relevant concerns or risks
5. Informing their employer or client of any business interests or affiliations which might influence or impair their judgment
6. Preserving the confidentiality of information of any present or former employer or client during service provision
7. Complying with all the applicable laws and regulations of the jurisdictions in the country where the service provisions were conducted
8. Respecting the intellectual property and contributions of others
9. Not communicating intentionally false or falsified information that may compromise the integrity of the evaluation process of a candidate for a PECB certification or a PECB certificate program
10. Not falsely or wrongly presenting themselves as PECB representatives without a proper license or misusing PECB logo, certifications or certificates
11. Not acting in ways that could damage PECB's reputation, certifications or certificate programs
12. Cooperating in a full manner on the inquiry following a claimed infringement of this Code of Ethics

To read the complete version of PECB's Code of Ethics, go to Code of Ethics | PECB.

Introduction to Certified Lead Forensics Examiner

The CLFE certification is for professionals working or interested in the computer forensics evidence recovery and analysis process. The certification focuses on core skills required to collect and analyze data from Windows, Mac OS X, Linux computer systems as well as mobile devices.

Today’s employers are not just seeking computer forensics professionals, but want proof that these professionals hold a predetermined set of knowledge and skills. Companies now place a high degree of importance on hiring, contracting with, and promoting credentialed practitioners prepared to tackle today and tomorrow’s challenges.

PECB certifications are not a license or simply a membership. They attest the candidates’ knowledge and skills gained through our training courses and are issued to candidates that have the required experience and have passed the exam.

This document specifies the PECB CLFE certification scheme in compliance with ISO/IEC 17024:2012. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your application. If you have questions or need further information after reading it, please contact the PECB international office at certification.team@pecb.com.

SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

Preparing for and scheduling the exam

All candidates are responsible for their own study and preparation for certification exams. Although candidates are not required to attend the training course to be eligible for taking the exam, attending it can significantly increase their chances of successfully passing the exam.

To schedule the exam, candidates have two options:

1. Contact one of our authorized partners. To find an authorized partner in your region, please go to Active Partners. The training course schedule is also available online and can be accessed on Training Events.
2. Take a PECB exam remotely through the PECB Exams application. To schedule a remote exam, please go to the following link: Exam Events.

To learn more about exams, competency domains, and knowledge statements, please refer to *Section III* of this document.

Rescheduling the exam

For any changes with regard to the exam date, time, location, or other details, please contact online.exams@pecb.com.

Application fees for examination and certification

Candidates may take the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000[2]
- Manager Exam: $700
- Foundation Exam: $500
- Transition Exam: $500

The application fee for certification is $500.

For the candidates that have attended the training course via one of PECB's partners, the application fee covers the costs of the exam (first attempt and first retake), the application for certification, and the first year of Annual Maintenance Fee (AMF).

[2] All prices listed in this document are in US dollars.

Competency domains

The objective of the “PECB Certified Lead Forensics Examiner” examination is to ensure that the candidate understands common commercial and open source tools that may be used during computer incident investigation and digital forensic operation, and has the knowledge and the skills to support an organization in recovering and analyzing computer forensics evidence.

The target population for this examination is:

- Computer forensic specialists
- Electronic data analyst
- Specialists in computer search and evidence recovery
- Person responsible for the application or of the enforcement of one or more laws in an organization
- Person responsible for examining media to extract and disclose data

The content of the exam is divided as follows:

- **Domain 1:** Basic principles of digital evidence
- **Domain 2:** Fundamentals of incident response with computer forensic operations
- **Domain 3:** Computer forensics hardware structure
- **Domain 4:** File structure and forensics operating system
- **Domain 5:** Acquisition and computer forensics operation
- **Domain 6:** Computer crime investigations and forensic examination

Domain 1: Basic principles of digital evidence

Main objective: Ensure that the candidate can understand, interpret, and illustrate the main concepts of digital evidence.

Competencies	Knowledge statements
1. Ability to understand and explain the basic components of digital evidence. 2. Ability to understand the processes of identification, collection, acquisition and preservation of digital evidence. 3. Ability to understand and provide credibility to investigation. 4. Ability to extend the analysis of digital evidence. 5. Ability to understand jurisdiction-specific requirements. 6. Ability to evaluate and classify evidence by its nature, strength and usefulness. 7. Ability to understand basic principles of digital evidence. 8. Ability to understand the key components of handling process. 9. Ability to understand the instances of handling processes. 10. Ability to understand the four requirements of digital evidence	1. Knowledge of the purpose of digital evidence. 2. Knowledge of the activities required to maintain the integrity of digital evidence. 3. Knowledge of identification and collection process of digital evidence. 4. Knowledge of acquisition and preservation process of digital evidence. 5. Knowledge of the activities required to facilitate exchange of digital evidence between jurisdictions. 6. Knowledge of the key components of methodology applied during the digital evidence process. 7. Knowledge of methodology to manage digital evidence 8. Knowledge of investigation involving digital device and evidence. 9. Knowledge on the analysis of digital evidence. 10. Knowledge on forensic readiness. 11. Knowledge of a process creating a copy of data within a defined set. 12. Knowledge of a process of gathering the physical items that contain potential digital evidence. 13. Knowledge on information or data, stored or transmitted in binary form. 14. Knowledge on the copy of the digital evidence that has been produced to maintain reliability of the evidence by including both the digital evidence and verification means. 15. Knowledge on digital storage media, evidence preservation facility, imaging, reliability, spoilage and tampering. 16. Knowledge of auditability, repeatability, reproducibility, justifiability

Domain 2: Fundamentals of incident response with computer forensic operations

Main objective: Ensure that the candidate can understand computer forensics operation and determine the course of action to be followed to achieve the goal of the operation.

Competencies	Knowledge statements
1. Ability to understand computer forensic laboratory 2. Ability to understand forensic lab preparation 3. Ability to understand policies and procedures. 4. Ability to understand computers for forensic examination 5. Ability to understand forensic hardware or software 6. Ability to understand portable forensic Kit. 7. Ability to prepare and execute a computer forensics operation 8. Ability to report verbally and by writing observations related to issues that occurred during an operation, including its computer forensics operation	1. Knowledge of organizational goals in terms of forensic examination 2. Knowledge of building a forensic lab based on organizational goals 3. Knowledge of law enforcement agency and internal business requirement 4. Knowledge of forensic that can lead to civil or criminal prosecution 5. Knowledge of preventive maintenance to protect intellectual properties 6. Knowledge of acquisition unit used to acquire storage image of suspect's storage media 7. Knowledge of analysis unit used to perform analysis and search on suspect's storage image. 8. Knowledge of portable unit that can be a combination of an acquisition and or analysis unit 9. Knowledge of procedures to apply within each step of the computer forensics operation 10. Knowledge of documented forms, guidelines, policies and procedures about the operation of the forensic labs 11. Knowledge of the procedures to apply when recommending corrective measures to enhance the quality of on-site procedures

Domain 3: Forensics computer hardware structure

Main objective: Ensure that the candidate can safely handle computers, components and media containing information to be examined.

Competencies	Knowledge statements
1. Ability to identify a part of computer, understand and explain the purpose of that part and how to remove it and install it securely 2. Ability to understand and explain the physical structure of a media and where and how the information is stored and retrieved 3. Ability to identify most common types of media, understand and explain how to read its content and write to it 4. Ability to understand Common Magnetic Storage of Hard Disk 5. Ability to understand the flash memory functions 6. Ability to understand the differences of NAD and NOR flash memory types. 7. Ability to understand Solid State Drive functions	1. Knowledge of the characteristics of main computer parts, including shape and structure. 2. Knowledge of the main purpose of main computer parts 3. Knowledge of the physical location where the information is stored in a media and how it is stored and retrieved 4. Knowledge of the method used by computer forensics specialist to protect the integrity of examined data 5. Knowledge in recovering encrypted document passwords 6. Knowledge to bypass operating system native access control without knowing the password. 7. Knowledge of the flash memory chip that can be electronically erased and reprogrammed 8. Knowledge of the flash memory types 9. Knowledge on the differences between NOR and NAND flash memory types 10. Knowledge on the wear levelling flash memory process 11. Knowledge on the garbage collection flash memory process 12. Knowledge on the advantages to store data on flash memory chip 13. Knowledge on the disadvantages of Solid State Drive 14. Knowledge on the differences between HHD and SSD storage methods

Domain 4: File structure and forensics operating system

Main objective: Ensure that the candidate has a clear knowledge where information can be found on an electronic media or image of a media, whether it is operating system's or user information.

Competencies	Knowledge statements
1. Ability to identify different file system Forensic layers 2. Ability to determine file system installed on the media under examination 3. Ability to understand the anatomy of files in the context of 5 layers 4. Ability to determine common file systems. 5. Ability to understand the common operating systems 6. Ability to understand the differences between common operating systems 7. Understand and explain how an operating system works 8. Understand and explain how information is stored on a media 9. Ability to understand the different operating systems 10. Ability to analyze a file system and find, extract and secure information from it	1. Knowledge of the characteristics of the different file system Forensic layers 2. Knowledge of the function of content layer and its function 3. Knowledge of the logical structure of various media and how and where the information is stored 4. Knowledge of the characteristics of the most common file systems, including their name, id number, numbering with regards to operating system installed, zone and data structure 5. Knowledge of the characteristics of the most common operating systems, including their versions, default file systems, basic tree structure and hardware requirements 6. Knowledge of the metadata and method to extract information from it 7. Knowledge of the function of the file name layer 8. Knowledge of the function of the application layer 9. Knowledge on the different common file systems 10. Knowledge on the File Allocation Table (FAT) File System 11. Knowledge on the differences between FAT and NTFS File System Time 12. Knowledge on the EXT3 File System 13. Knowledge on the Microsoft Windows 14. Knowledge of the Linux operating systems 15. Knowledge of the OS X operating systems developed by Apply Inc 16. Knowledge of the Android Operating Systems 17. Knowledge of the Apple iOS Operating System 18. Knowledge on the three components of computer forensic operation

Domain 5: Acquisition and computer forensics operation

Main objective: Ensure that the candidate can collect and acquire the media/device containing the evidence and use various digital forensic tools available.

Competencies	Knowledge statements
1. Understand and explain definition of collection and acquisition 2. Ability to understand and describe the cloning process 3. Ability to describe actions performed from a higher level of assurance of integrity 4. Understand and describe live forensics how basically works and understand its issues 5. Understand the conventional digital forensic approach 6. Ability to describe the rational behind Live Forensic and to be able to justify to the authority those changes are confined within a calculated boundary 7. Ability to understand the deciding factors based on the digital forensic case that CLFE is working on 8. Ability to understand conventional forensic approach 9. Ability to understand popular encoding schemes. 10. Understand Windows Digital Forensic 11. Ability to understand investigation using Autopsy 12. Ability to understand the Image Forensic process	1. Basic knowledge of definitions of collection and acquisition 2. Knowledge of basic safe techniques to acquire and preserve evidence 3. Knowledge of the components of cloning process 4. Knowledge of the live forensics methods and tools 5. Knowledge on the live forensic impacts 6. Knowledge on the conventional digital forensic approach 7. Knowledge on the Live Forensic impacts 8. Knowledge on performing basic memory examination 9. Knowledge to describe practical examples on analyzing live memory 10. Knowledge to determine what type of encodings are being used on the saved documents 11. Knowledge on the code encoding language and standard 12. Knowledge on the practical example on file carving 13. Knowledge on the windows digital forensic 14. Knowledge on the process of mounting the file 15. Basic knowledge on recovering deleted files using autopsy 16. Knowledge on investigation using Autopsy

Domain 6: Computer crime investigations and forensic examination

Main objective: Ensure that the candidate can justify the way how the evidence was acquired or left behind in an ordered, standard and forensically sound manner.

Competencies	Knowledge statements
1. Ability to understand essential digital forensic topics 2. Ability to understand decision-making process of collection or acquisition of potential digital evidence 3. Ability to understand additional digital forensic topics 4. Ability to describe e-mail investigation process 5. Ability to follow the path for web browser forensic. 6. Ability to understand the forensic emerging threats 7. Ability to understand the Anti Computer Forensic to uncover evidence 8. Ability to apply technologies that affect the field of Digital Forensic 9. Ability to completely and accurately report the findings including the result of the analysis of the digital evidence examination. 10. Ability to deliver complete, accurate and comprehensive documentation 11. Ability to apply appropriate measures to assure continuity during digital forensic examinations 12. Ability to identify and understand the presence of your audience during the presentation of digital forensic findings 13. Ability to translate complex forensic scenarios into simple stories 14. Ability to understand the purpose of the presentation and best practices used for presenters 15. Ability to determine what you have found in the evidence 16. Ability to apply appropriate measures to assure continuity of possession along the path followed by the evidence	1. Knowledge on the e-mail investigation process 2. Knowledge on the collection of power on and off devices 3. Knowledge on the acquisition of powered-off Digital Devices 4. Knowledge of the path followed during the process of e-mail investigations 5. Knowledge of the procedures including the e-mail attributes 6. In-depth knowledge of e-mail forensic 7. Knowledge on the web browser Forensic 8. In-depth knowledge of all Anti forensic Techniques. 9. Knowledge of the emerging technologies that affect the field of Digital Forensic 10. Knowledge of documentation procedures throughout the examination 11. In-depth knowledge of the documentation procedures to CLDE professional ethics 12. Knowledge of the audience and the ways to present to them digital forensic findings 13. Knowledge of the complex forensic scenarios 14. Knowledge on the translating complex forensic scenarios into simple stories 15. Knowledge of the facts how to deliver complete, accurate and comprehensive documentation 16. Knowledge of the best practices used in the presentation 17. Knowledge to understand the purpose of the presentation 18. In-depth knowledge of the measures to assure continuity during digital forensic findings 19. Knowledge of the facts and circumstances classically taken in account to justify the examination report

	20. Knowledge to apply appropriate measures to assure the continuity of possession along the path followed by the evidence

Based on the above-mentioned domains and their relevance, the exam contains 14 questions, as summarized in the table below:

			Level of understanding (Cognitive/Taxonomy) required					
		Points per question	Questions that measure comprehension, application, and analysis	Questions that measure evaluation	Number of questions per competency domain	% of the exam devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency domains	Basic principles of digital evidence	5	X		2	14.2	10	13.3
		5	X					
	Fundamentals of incident response with computer forensics operations	5	X		3	21.5	20	26.7
		10	X					
		5	X					
	Computer forensic hardware structure	5		X	1	7.1	5	6.7
	File structure forensic and forensic operating system	5		X	3	21.5	15	20
		5		X				
		5		X				
	Acquisition and computer forensics operation	5	X		3	21.5	15	20
		5		X				
		5		X				
	Computer crime investigations and forensic examination	5	X		2	14.2	10	13.3
		5	X					
	Total points	75						
	Number of questions per level of understanding		8	6				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		57.1	42.9				

The passing score of the exam is **70%**.

After successfully passing the exam, candidates will be able to apply for obtaining the “PECB Certified Lead Forensics Examiner” credential.

Taking the exam

General information about the exam
Candidates are required to arrive/be present at least 30 minutes before the exam starts.

Candidates who arrive late will not be given additional time to compensate for the late arrival and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (a national ID card, driver's license, or passport) and show it to the invigilator.

If requested on the day of the exam (paper-based exams), additional time can be provided to candidates taking the exam in a non-native language, as follows:

- 10 additional minutes for Foundation exams
- 20 additional minutes for Manager exams
- 30 additional minutes for Lead exams

PECB exam format and type

1. **Paper-based:** Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. The use of electronic devices, such as laptops, tablets, or phones, is not allowed. The exam session is supervised by a PECB approved Invigilator at the location where the Partner has organized the training course.
2. **Online:** Exams are provided electronically via the PECB Exams application. The use of electronic devices, such as tablets and cell phones, is not allowed. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

For more information about online exams, go to the PECB Online Exam Guide.

PECB exams are available in two types:

1. Essay-type question exam
2. Multiple-choice question exam

This exam comprises essay-type questions. Essay-type questions are used to determine and evaluate whether a candidate can clearly answer questions related to the defined competency domains. Additionally, problem-solving techniques and arguments that are supported with reasoning and evidence will also be evaluated. The exam aims to evaluate candidates' comprehension, analytical skills, and applied knowledge. Therefore, candidates are required to provide logical and convincing answers and explanations in order to demonstrate that they have understood the content and the main concepts of the competency domains.

This is an open-book exam. The candidate is allowed to use the following reference materials:

- A hard copy of the ISO/IEC 27037 standard
- Training course materials (accessed through the PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
- A hard copy dictionary

A sample of exam questions will be provided below.

Note: PECB will progressively transition to multiple-choice exams. They will also be open book and comprise scenario-based questions that will allow PECB to evaluate candidates' knowledge, abilities, and skills to use information in new situations (apply), draw connections among ideas (analyze), and justify a stand or decision (evaluate).

For specific information about exam types, languages available, and other details, please contact examination.team@pecb.com or go to the List of PECB Exams.

Sample exam questions

Question 1:
After deleting a file from a FAT file system, what happen to the content of the file?

Possible answer:
The content will still remain on the file system, however:
a) *1st byte in the FAT directory entry of the file will changed to hex 0xe5*
b) *Value in the FAT indicate the clusters changed to 'unallocated'*
c) *Unless the clusters are re-used, the data residing on the blocks can be recovered*

If the deleted file was fragmented, it's possible that wrong cluster may be obtained during recovery process.

Question 2:
The CLFE has discovered that other than laptop and cell phones, THI also provide an additional standard USB hard drive to each of their senior employee. The standard issued USB hard drive is not encrypted and the owners are responsible to protect the issued hard drive.

THI have not done an auditing on any of the issued hard drives, nor have been keeping track of the issued hard drives on their corporate IT asset list. Nevertheless, based on THI Information Security Policies, all senior employees are required to submit their hard drives to the IT Operation department for back up at monthly basis.

Describe what is the next course of action shall be taken by the CLFE, and why.

Possible answer:
At this point in time, the list of evidence that need to be acquired from Mr. Jones, includes:
- *Hard disk drive from his laptop*
- *Company issued Cell Phone*
- *And the company issued USB hard disk drive.*

Notice that the IT Department is also performing backup for the management personnel, the backup date will be part of the areas of interest.
a) *Perform acquisition on all devices above.*
b) *Conduct audit to determine number of issued hard drives to Mr. Jones*
c) *Con duct audit on the back up log of Mr. Jones's company issued USB disks.*

Triage
CLFE shall acquire all data listed on the devices above, plus performing triage on the backup data from the IT Department. Triage process shall based on the search criterias set forth by THI management.

Question 3:
What are some of the common limitations face by the forensic examiners during keywords search? List down 5 examples:

Possible answer:

- *Keyword search may not be useful when searching compounded files*
- *Keyword search is based on the correct encoding, if the file is encoded in different encoding scheme, keyword search will fail. e.g. searching a 7 bit word in an 8 bit encoded file content*
- *Keyword search may not be useful searching binary files*
- *Keyword search is literal based. unlike regular expression, keyword search is confine to the scope of the word, e.g. if search for the word “books”, we will missed out the word “book”, “booking”, “bookie” etc.*
- *Keyword search is useless in encrypted files*

Exam Security Policy

PECB is committed to protect the integrity of its exams and the overall examination process, and relies upon the ethical behavior of applicants, potential applicants, candidates and partners to maintain the confidentiality of PECB exams. This Policy aims to address unacceptable behavior and ensure fair treatment of all candidates.

Any disclosure of information about the content of PECB exams is a direct violation of this Policy and PECB's Code of Ethics. Consequently, candidates taking a PECB exam are required to sign an Exam Confidentiality and Non-Disclosure Agreement and must comply with the following:

1. The questions and answers of the exam materials are the exclusive and confidential property of PECB. Once candidates complete the submission of the exam to PECB, they will no longer have any access to the original exam or a copy of it.
2. Candidates are prohibited from revealing any information regarding the questions and answers of the exam or discuss such details with any other candidate or person.
3. Candidates are not allowed to take with themselves any materials related to the exam, out of the exam room.
4. Candidates are not allowed to copy or attempt to make copies (whether written, photocopied, or otherwise) of any exam materials, including, without limitation, any questions, answers, or screen images.
5. Candidates must not participate nor promote fraudulent exam-taking activities, such as:
   - Looking at another candidate's exam material or answer sheet
   - Giving or receiving any assistance from the invigilator, candidate, or anyone else
   - Using unauthorized reference guides, manuals, tools, etc., including using "brain dump" sites as they are not authorized by PECB

Once a candidate becomes aware or is already aware of the irregularities or violations of the points mentioned above, they are responsible for complying with those, otherwise if such irregularities were to happen, candidates will be reported directly to PECB or if they see such irregularities, they should immediately report to PECB.

Candidates are solely responsible for understanding and complying with PECB Exam Rules and Policies, Confidentiality and Non-Disclosure Agreement and Code of Ethics. Therefore, should a breach of one or more rules be identified, candidates will not receive any refunds. In addition, PECB has the right to deny the right to enter a PECB exam or to invite candidates for an exam retake if irregularities are identified during and after the grading process, depending on the severity of the case.

Any violation of the points mentioned above will cause PECB irreparable damage for which no monetary remedy can make up. Therefore, PECB can take the appropriate actions to remedy or prevent any unauthorized disclosure or misuse of exam materials, including obtaining an immediate injunction.
PECB will take action against individuals that violate the rules and policies, including permanently banning them from pursuing PECB credentials and revoking any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam results

Exam results will be communicated via email.

- The time span for the communication starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams.
- For online multiple-choice exams, candidates receive their results instantly.

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

Candidates that disagree with the results may request a re-evaluation by writing to examination.team@pecb.com within 30 days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 days from the date they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Any complaint received after 30 days will not be processed.

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes.

If a candidate does not pass the exam on the 1st attempt, they must wait 15 days after the initial date of the exam for the next attempt (1st retake).

Note: Candidates who have completed the training course with one of our partners, and failed the first exam attempt, are eligible to retake for free the exam within a 12-month period from the date the coupon code is received (the fee paid for the training course, includes a first exam attempt and one retake). Otherwise, retake fees apply.

For candidates that fail the exam retake, PECB recommends they attend a training course in order to be better prepared for the exam.

To arrange exam retakes, based on exam format, candidates that have completed a training course, must follow the steps below:

1. Online Exam: when scheduling the exam retake, use initial coupon code to waive the fee
2. Paper-Based Exam: candidates need to contact the PECB Partner/Distributor who has initially organized the session for exam retake arrangement (date, time, place, costs).

Candidates that have not completed a training course with a partner, but sat for the online exam directly with PECB, do not fall under this Policy. The process to schedule the exam retake is the same as for the initial exam.

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB CLFE credentials

All PECB certifications have specific requirements regarding education and professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB Certified Lead Forensics Examiner scheme have the following requirements:

Credential	Education	Exam	Professional experience	CFMS project experience	Other requirements
PECB Certified Lead Forensics Examiner	At least secondary education	PECB Certified Lead Forensics Examiner Exam or equivalent	Five years: Two years of work experience in computer forensics	Forensics activities: a total of 300 hours	Signing the PECB Code of Ethics

To be considered valid, the activities should follow best audit practices and include the following:

1. Conducting forensic investigation
2. Post incident response activities
3. Network management
4. Computer forensics examination and analysis planning
5. Analysis of file systems and digital media
6. Forensics analysis of operating systems and networks
7. Forensics analysis of computer and mobile devices
8. Gathering digital evidence

Applying for certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credential they were assessed for. Specific educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB account), including contact details of individuals who will be contacted to validate the candidates' professional experience. Candidates can submit their application in English, French, German, Spanish or Korean languages. They can choose to either pay online or be billed. For additional information, please contact certification.team@pecb.com.

The online certification application process is very simple and takes only a few minutes:

- Register your account
- Check your email for the confirmation link
- Log in to apply for certification

For more information on how to apply for certification, click here.

The Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. The candidate will receive an email about the application status, including the certification decision.

Following the approval of the application by the Certification Department, the candidate will be able to download the certificate and claim the corresponding Digital Badge. For more information about downloading the certificate, click here, and for more information about claiming the Digital Badge, click here.

PECB provides support both in English and French.

Professional experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the résumé.

Professional references

For each application, two professional references are required. They must be from individuals who have worked with the candidate in a professional environment and can validate their forensics implementation project experience, as well as their current and previous work history. Professional references of persons who fall under the candidate’s supervision or are their relatives are not valid.

Audit experience

The candidate’s audit log will be checked to ensure that they have completed the required number of audit hours. The following audit types constitute valid audit experience: pre-audit, internal audits, second party audits, or third party audits.

Evaluation of certification applications

The Certification Department will evaluate each application to validate the candidates’ eligibility for certification or certificate program. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which may lead to the candidates’ credential downgrade.

SECTION IV: CERTIFICATION POLICIES

Denial of certification

PECB can deny certification/certificate program if candidates:

- Falsify the application
- Violate the exam procedures
- Violate the PECB Code of Ethics

Candidates whose certification/certificate program has been denied can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

The application payment for the certification/certificate program is nonrefundable.

Certification status options

Active

Means that your certification is in good standing and valid, and it is being maintained by fulfilling the PECB requirements regarding the CPD and AMF.

Suspended

PECB can temporarily suspend candidates' certification if they fail to meet the requirements. Other reasons for suspending certification include:

- PECB receives excessive or serious complaints by interested parties (suspension will be applied until the investigation has been completed.)
- The logos of PECB or accreditation bodies are willfully misused.
- The candidate fails to correct the misuse of a certification mark within the determined time by PECB.
- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification.

Revoked

PECB can revoke (that is, to withdraw) the certification if the candidate fails to satisfy its requirements. In such cases, candidates are no longer allowed to represent themselves as PECB Certified Professionals. Additional reasons for revoking certification can be if the candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of certification
- Break any other PECB rules
- Any other reasons that PECB deems appropriate

Candidates whose certification has been revoked can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

Other statuses

Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. To learn more about these statuses and the permanent cessation status, go to Certification Status Options.

Upgrade and downgrade of credentials

Upgrade of credentials

Professionals can upgrade their credentials as soon as they can demonstrate that they fulfill the requirements.

To apply for an upgrade, candidates need to log into their PECB account, visit the “My Certifications” tab, and click on “Upgrade.” The upgrade application fee is $100.

Downgrade of credentials

A PECB Certification can be downgraded to a lower credential due to the following reasons:

- The AMF has not been paid.
- The CPD hours have not been submitted.
- Insufficient CPD hours have been submitted.
- Evidence on CPD hours has not been submitted upon request.

Note: *PECB certified professionals who hold Lead certifications and fail to provide evidence of certification maintenance requirements will have their credentials downgraded. The holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.*

Renewing the certification

PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continual professional development (CPD) hours. In addition, they need to pay the annual maintenance fee ($120). For more information, go to the Certification Maintenance page on the PECB website.

Closing a case

If candidates do not apply for certification within one year, their case will be closed. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing to certification.team@pecb.com and pay the required fee.

Complaint and Appeal Policy

Any complaints must be made no later than 30 days after receiving the certification decision. PECB will provide a written response to the candidate within 30 working days after receiving the complaint. If candidates do not find the response satisfactory, they have the right to file an appeal.

For more information about the Complaint and Appeal Policy, click here.

SECTION V: GENERAL POLICIES

Exams and certifications from other accredited certification bodies

PECB accepts certifications and exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective certification(s) or exam(s) can be accepted as equivalent to the respective PECB certification (e.g., ISO/IEC 27001 Lead Auditor certification).

Non-discrimination and special accommodations

All candidate applications will be evaluated objectively, regardless of the candidates' age, gender, race, religion, nationality, or marital status.

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations[3] for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the partner/distributor in order for them to make proper arrangements[4]. Any information that candidates provide regarding their disability/special needs will be treated with confidentiality. To download the Candidates with Disabilities Form, click here.

Behavior Policy

PECB aims to provide top-quality, consistent, and accessible services for the benefit of its external stakeholders: distributors, partners, trainers, invigilators, examiners, members of different committees and advisory boards, and clients (trainees, examinees, certified individuals, and certificate holders), as well as creating and maintaining a positive work environment which ensures safety and well-being of its staff, and holds the dignity, respect and human rights of its staff in high regard.

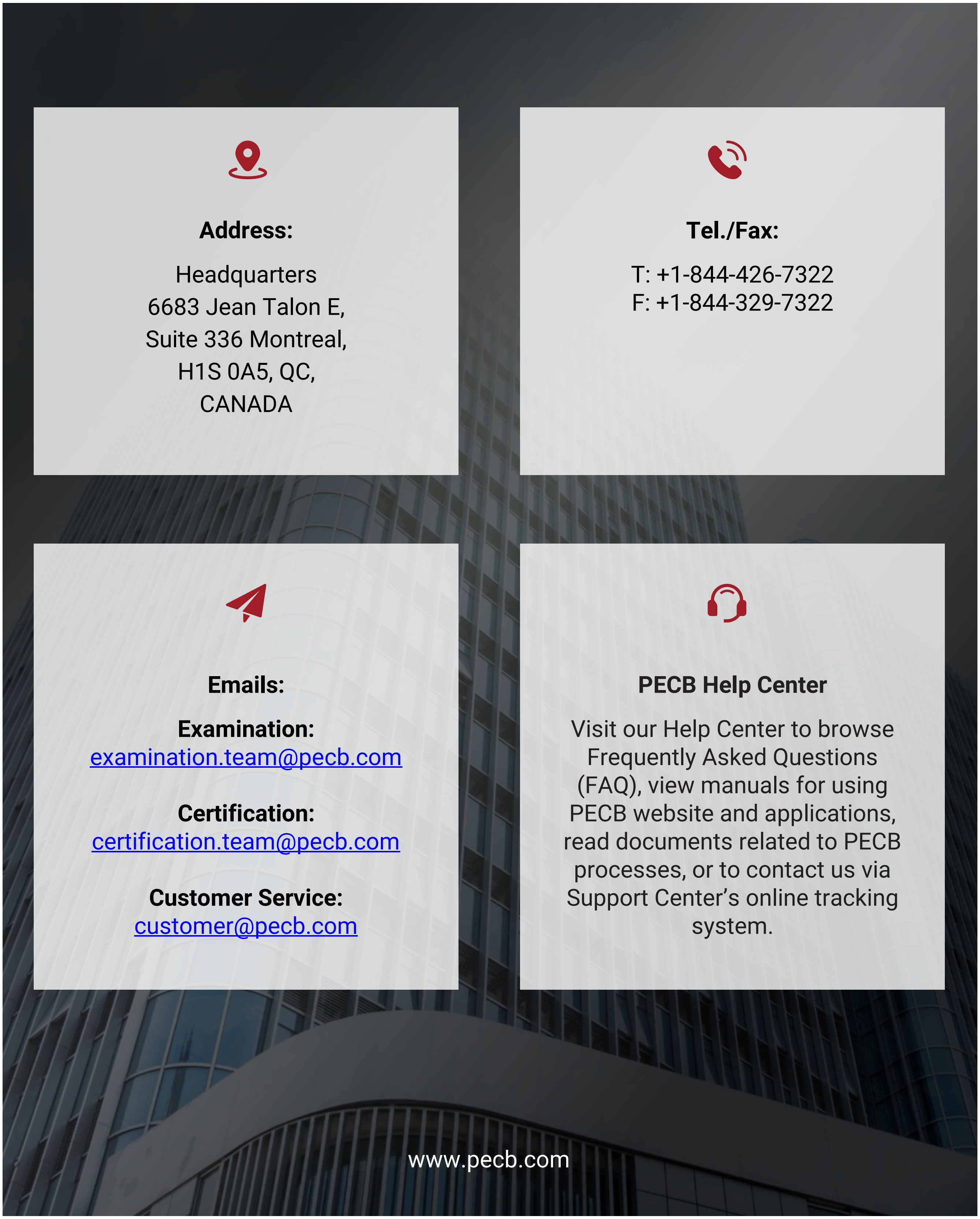
The purpose of this Policy is to ensure that PECB is managing unacceptable behavior of external stakeholders towards PECB staff in an impartial, confidential, fair, and timely manner. To read the Behavior Policy, click here.

Refund Policy

PECB will refund your payment, if the requirements of the Refund Policy are met. To read the Refund Policy, click here.

[3] According to ADA, the term "reasonable accommodation" may include: (A) making existing facilities used by employees readily accessible to and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.

[4] ADA Amendments Act of 2008 (P.L. 110–325) Sec. 12189. Examinations and courses. [Section 309]: Any person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or post-secondary education, professional, or trade purposes shall offer such examinations or courses in a place and manner accessible to persons with disabilities or offer alternative accessible arrangements for such individuals.



Address:

Headquarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax:

T: +1-844-426-7322
F: +1-844-329-7322

Emails:

Examination:
examination.team@pecb.com

Certification:
certification.team@pecb.com

Customer Service:
customer@pecb.com

PECB Help Center

Visit our Help Center to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center’s online tracking system.

www.pecb.com