PECB

BEYOND RECOGNITION

CERTIFIED LEAD ETHICAL HACKER

Candidate Handbook

PECB

Table of Contents

PECB

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 Ethical Hacker

The Certified Lead Ethical Hacker training course enables participants to master the penetration testing techniques and acquire the necessary knowledge and skills for conducting information system penetration testing by completing the labs included in the training course using a virtual machine.

Being an ethical hacker is one of the most required professions in the market which enables organizations to search for and discover exploitable vulnerabilities. The PECB Certified Ethical Hacker training course provides a new hands-on experience of ethical hacking methodologies and tools used by ethical hackers and information security professionals.

The "Lead Ethical Hacker" credential is a professional certification for individuals aiming to demonstrate the competence to plan, perform, and manage information security penetration tests. This internationally recognized certification can help you exploit your career potential and reach your professional objectives.

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 Lead Ethical Hacker 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.

PECB

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 “Certified Lead Ethical Hacker” credential is a professional certification that demonstrates a candidate’s ability to conduct information system penetration tests. The objective of the Certified Lead Ethical Hacker exam is to ensure that the candidate has acquired the necessary knowledge and expertise to conduct a penetration test based on a pre-defined framework.

The Lead Ethical Hacker certification is intended for:

- Cybersecurity professionals and information system team members
- Information security professionals seeking to master ethical hacking techniques
- Managers or consultants seeking to master the penetration testing process
- Individuals responsible for maintaining information system security within an organization
- Technical experts seeking to prepare for performing penetration tests
- Auditing experts wishing to conduct professional penetration tests

The content of the exam is divided as follows:

- **Domain 1:** Information gathering tools and techniques
- **Domain 2:** Threat modeling and vulnerability identification
- **Domain 3:** Exploitation techniques
- **Domain 4:** Privilege escalation
- **Domain 5:** Pivoting and file transfers
- **Domain 6:** Reporting

Domain 1: Information gathering tools and techniques

Main objective: Ensure that the candidate understands and is able to select and adapt the penetration testing approach based on the gathered information.

Competencies	Knowledge statements
1. Ability to understand and interpret fundamental concepts and principles of ethical hacking and cybersecurity	1. Knowledge of the main concepts and terminology of ethical hacking and cybersecurity
2. Ability to understand penetrating testing standards and frameworks	2. Knowledge of penetration testing strategies and methodologies
3. Ability to understand ethical hacking methodologies	3. Knowledge of common hacking techniques
4. Ability to collect information during the reconnaissance phase	4. Knowledge on the different methods of collecting and analyzing valuable information
5. Ability to select and adapt the penetration testing approach based on the gathered information	5. Knowledge of reconnaissance tools included in the ethical hacker's toolkit and their usage
6. Ability to understand and use appropriate tools and techniques for gathering valuable information	6. Knowledge of information gathering techniques that avoid detection
7. Ability to effectively gather information on the target using open source intelligence	7. Knowledge of open source intelligence tools and techniques and their usage, including OSINT Framework, Shodan, Maltego, and Google Hacking
8. Ability to understand and explain the difference between passive and active reconnaissance	8. Knowledge of passive and active reconnaissance tools and techniques and their application

Domain 2: Threat modeling and vulnerability identification

Main objective: Ensure that the candidate understands and is able to conduct threat modeling on the target and uncover hidden vulnerabilities that can be exploited.

Competencies	Knowledge statements
1. Ability to understand and explain the relationship between threats and vulnerabilities 2. Ability to create an offensive threat model using the information gathered during the reconnaissance phase 3. Ability to analyze the information and adapt the threat model 4. Ability to use the appropriate vulnerability scanning tools and techniques 5. Ability to understand and explain the difference between vulnerability types and their effectiveness 6. Ability to adapt the threat model based on new collected information	1. Knowledge of the main methods for collecting and analyzing valuable information to create an effective threat model 2. Knowledge of zero-day vulnerabilities and other vulnerabilities and threats 3. Knowledge of vulnerability scanning tools found in the ethical hacker's toolkit 4. Knowledge on how to evaluate different vulnerability types and determine which one to use to ensure an effective vulnerability exploitation 5. Knowledge of attack plan categories

Domain 3: Exploitation techniques

Main objective: Ensure that the candidate understands and is able to interpret and apply the main exploitation techniques.

Competencies	Knowledge statements
1. Ability to evade intrusion detection systems (IDS) and intrusion prevention systems, firewalls, and honeypots 2. Ability to understand, interpret, and perform server-side attacks 3. Ability to understand and perform client-side attacks 4. Ability to perform web application attacks 5. Ability to understand and perform attacks on wireless networks	1. Knowledge of different types of intrusion detection systems and IDS evading process 2. Knowledge of protection measures against server-side attacks 3. Knowledge of the latest trends regarding exploits for performing server-side attacks 4. Knowledge of the latest tools and exploit techniques for performing client-side attacks 5. Knowledge of web server hardening methods, web application vulnerabilities, threats, and countermeasures 6. Knowledge of wireless technology and wireless hacking methods 7. Knowledge of wireless network security tools and techniques and their usage

Domain 4: Privilege escalation

Main objective: Ensure that the candidate is able to understand and implement the processes required to gain access into a network or system and escalate the privileges.

Competencies	Knowledge statements
1. Ability to understand and interpret the concept of privilege escalation 2. Ability to understand and explain privilege escalation methods 3. Ability to perform privilege escalation on a machine 4. Ability to understand and perform privilege escalation on a system 5. Ability to perform privilege escalation on a network	1. Knowledge of privilege escalation process and its advantages 2. Knowledge of the different methods of privilege escalation: credential harvesting and structured passwords 3. Knowledge of privilege escalation process in web applications 4. Knowledge of appropriate tools and techniques for escalating user privileges on machines and networks

Domain 5: Pivoting and file transfer

Main objective: Ensure that the candidate is able to understand and perform the appropriate actions for pivoting from one machine to another and transfer relevant files.

Competencies	Knowledge statements
1. Ability to understand and explain the definition of pivoting process 2. Ability to pivot to a different network 3. Ability to understand and appropriately use the pivoting tools and techniques 4. Ability to understand and explain the definition of file transfer 5. Ability to safely transfer files from the target host 6. Ability to understand and use different tools for maintaining the access to a network 7. Ability to clean up and destroy artifacts	1. Knowledge of appropriate tools and techniques for pivoting to another network, such as netcat or SSH 2. Knowledge of file transfer methods and tools, including FTP, HTTP, netcat, wget, and curl 3. Knowledge of tools and approaches used to maintain access to a network, such as keylogger, rootkits, and Trojans 4. Knowledge of the process of cleaning and destroying artifacts, such as agents, scripts, executables, and backdoors

Domain 6: Reporting

Main objective: Ensure that the candidate is able to create a comprehensible penetration testing report.

Competencies	Knowledge statements
1. Ability to effectively gather information during all penetration testing phases	1. Knowledge of the information gathering and structuring tools, such as CherryTree
2. Ability to interpret attack vectors and mechanisms	2. Knowledge of attack mechanisms and mitigation vectors
3. Ability to propose appropriate recommendations on mitigation techniques to be included in the testing report	3. Knowledge of the approaches that should be followed to define recommendations for mitigating vulnerabilities
4. Ability to establish a penetration testing report	4. Knowledge on how to protect the information gathered during the penetration testing process and avoid vulnerabilities disclosure
5. Ability to understand the classification of the penetration testing report based on the client's information classification policy	5. Knowledge on how to draft a concise report and use visualization tools to better present the penetration testing findings
6. Ability to draft the penetration testing report in a way that is understandable and clear	

Based on the abovementioned domains and their relevance, the candidates will be required to compromise at least two out of three machines and properly document the process through an exam report, 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	Information gathering	5		X	3	30	15	15
		5		X				
		5		X				
	Threat modelling and vulnerability identification	5		X	1	10	5	5
	Exploitation techniques	10	X		3	30	30	30
		10	X					
		10	X					
	Privilege escalation	25	X		1	10	25	25
	Pivoting and file transfer	15	X		1	10	15	25
	Reporting	10		X	1	10	10	10
	Total points	100						
	Number of questions per level of understanding		5	5				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		50	50				

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 Ethical Hacker" 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. **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. Practical exam
2. Report writing exam

The duration of the exam is a six hour session for the practical exam and twenty four hours for writing the report.

The PECB Certified Lead Ethical Hacker Exam is an online exam. The exam is used to determine and evaluate whether a candidate is able to gain remote access to the target network by compromising no less than two machines. This type of exam format was selected as a means of determining whether a candidate can apply the knowledge gained during the training course in a real-word environment. In addition, the exam requires the candidate to document this process in the exam report.

This is an open-book exam. The candidate is allowed to use the following reference materials:
- 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)
- Books and online materials
- A hard copy dictionary

A sample of exam questions will be provided below.

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

Task 1:
Conduct a network scan on the target system to gather information on the IP range.

Possible answer:
To understand the IP range of a network we must conduct a network scan using nmap. Nmap will provide us with the information necessary to proceed to the next stage.

```
kali@kali:~$ nmap -sP 192.168.10.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 14:48 UTC
Nmap scan report for ip-192-168-10-10.us-east-2.compute.internal (192.168.10.10)
Host is up (0.000058s latency).
Nmap scan report for ip-192-168-10-25.us-east-2.compute.internal (192.168.10.25)
Host is up (0.00099s latency).
Nmap scan report for ip-192-168-10-54.us-east-2.compute.internal (192.168.10.54)
Host is up (0.00052s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.55 seconds
```

Based on the scan we determine that there are two machines other than ours are active on the network, the machines have the following internal IPs: 192.168.10.25 and 192.168.10.54.

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.

PECB

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB Certified Lead Ethical Hacker 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 Ethical Hacker scheme have the following requirements:

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Lead Ethical Hacker	PECB Certified Lead Ethical Hacker exam or equivalent	Two years penetration testing and cybersecurity experience	None	Signing the PECB Code of Ethics, and the PECB CLEH Code of Conduct

To be considered valid, the penetration testing and cybersecurity experience should include the following:

1. Determining the scope of ethical hacking
2. Defining a penetration testing approach
3. Performing the steps that should be followed during a penetration testing
4. Defining the penetration testing criteria
5. Evaluating penetration test scenarios and treatment options
6. Using the methods that help to increase the security of operation systems
7. Reporting the penetration testing results

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 penetration testing and cybersecurity 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.

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.

PECB

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.

PECB

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., Lead Ethical Hacker 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