PECB BEYOND RECOGNITION

Candidate Handbook

CERTIFIED LEAD ETHICAL HACKER

PECB

Table of Contents

SECTION I: INTRODUCTION

About PECB

PECB is a certification body which provides education[1] and certification in accordance with ISO/IEC 17024 for individuals on a wide range of disciplines.

We help professionals show commitment and competence by providing them with valuable evaluation and certification services against internationally recognized standards. Our mission is to provide services that inspire trust and continual improvement, demonstrate recognition, and benefit the society as a whole.

The key objectives of PECB are:

1. Establishing the minimum requirements necessary to certify professionals
2. Reviewing and verifying the qualifications of applicant to ensure they are eligible to apply for certification
3. Developing and maintaining reliable certification evaluations
4. Granting certifications to qualified candidates, maintaining records, and publishing a directory of the holders of a valid certification
5. Establishing requirements for the periodic renewal of certification and ensuring compliance with those requirements
6. Ensuring that candidates meet ethical standards in their professional practice
7. Representing its members, where appropriate, in matters of common interest
8. Promoting the benefits of certification to organizations, employers, public officials, practitioners in related fields, and the public

[1] Education refers to training courses developed by PECB, and offered globally through our network of resellers.

The Value of PECB Certification

Why Choose PECB as Your Certification Body?

Global Recognition

Our certifications are internationally recognized and accredited by the International Accreditation Service (IAS); signatory of IAF Multilateral Recognition Arrangement (MLA) which ensures mutual recognition of accredited certification between signatories to the MLA and acceptance of accredited certification in many markets. Therefore, professionals who pursue a PECB certification credential will benefit from PECB's recognition in domestic and international markets.

Competent Personnel

The core team of PECB consists of competent individuals who have relevant sector-specific experience.
All of our employees hold professional credentials and are constantly trained to provide more than satisfactory services to our clients.

Compliance with Standards

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

Customer Service

We are a customer-centered company and treat all our customers with value, importance, professionalism, and honesty. PECB has a team of experts dedicated to support customer requests, problems, concerns, needs, and opinions. We do our best to maintain a 24-hours maximum response time without compromising the quality of the service.

PECB Code of Ethics

PECB professionals will:

1. Conduct themselves professionally, with honesty, accuracy, fairness, responsibility, and independence
2. Act at all times solely in the best interest of their employer, their clients, the public, and the profession, by adhering to the professional standards and applicable techniques while offering professional services
3. Maintain competency in their respective fields and strive to constantly improve their professional capabilities
4. Offer only professional services for which they are qualified to perform, and adequately inform clients about the nature of the proposed services, including any relevant concerns or risks
5. Inform each employer or client of any business interests or affiliations that might influence their judgment or impair their fairness
6. Treat in a confidential and private manner the information acquired during professional and business dealings of any present or former employer or client
7. Comply with all laws and regulations of the jurisdictions where professional activities are conducted
8. Respect the intellectual property and contributions of others
9. Not, intentionally or otherwise, communicate false or falsified information that may compromise the integrity of the evaluation process of a candidate for a professional designation
10. Not act in any manner that could compromise the reputation of PECB or its certification programs
11. Fully cooperate on the inquiry following a claimed infringement of this Code of Ethics

The full version of the PECB Code of Ethics can be downloaded here.

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.

It is important to understand that PECB certifications are not a license or simply a membership. They represent peer recognition that an individual has demonstrated proficiency in, and comprehension of, a set of competences. PECB certifications are awarded to candidates that can demonstrate experience and have passed a standardized exam in the certification area.

This document specifies the PECB Lead Ethical Hacker certification scheme in compliance with ISO/IEC 17024:2012. This candidate handbook also contains information about the process by which candidates may earn and maintain their credentials. It is very important that you read all the information included in this candidate handbook before completing and submitting your application. If you have questions after reading it, please contact the PECB international office at certification@pecb.com.

SECTION II: PECB CERTIFICATION PROCESS AND EXAMINATION PREPARATION, RULES, AND POLICIES

Decide Which Certification Is Right for You

All PECB certifications have specific education and professional experience requirements. To determine the right credential for you, verify the eligibility criteria for various certifications and your professional needs.

Prepare and Schedule the Exam

All candidates are responsible for their own study and preparation for certification exams. No specific set of training courses or curriculum of study is required as part of the certification process. Nevertheless, attending a training course can significantly increase candidates' chances of successfully passing a PECB exam.

To schedule an exam, candidates have two options:

1. Contact one of our resellers who provide training courses and exam sessions. To find a training course provider in a particular region, candidates should go to Active Resellers. The PECB training course schedule is also available on Training Events.
2. Take a PECB exam remotely from their home or any location they desire through the PECB Exam application, which can be accessed here: Exam Events.

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

Application Fees for Examination and Certification

PECB offers direct exams, where a candidate can sit for the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000
- Manager Exam: $700
- Foundation and Transition Exam: $500

The application fee for certification is $500.

For all candidates that have followed the training course and taken the exam with one of PECB's resellers, the application fee includes the costs associated with examination, application for certification, and the first year of Annual Maintenance Fee (AMF) only.

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 Certified 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

PECB

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

PECB

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

PECB

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

PECB

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

PECB

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

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. The tasks that are included in the exam are summarized in the table below:

			Level of understanding (Cognitive/Taxonomy) required					
		Points per tasks	Tasks that measure comprehension, application, and analysis	Tasks that measure synthesis and evaluation	Number of tasks per competency domain	% of the exam devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency domains	Domain 1: Information gathering	5		X	3	25	15	15
		5		X				
		5		X				
	Domain 2: Threat modeling and vulnerability identification	5		X	1	8.33	5	5
	Domain 3: Exploitation techniques	10	X		3	25	30	30
		10	X					
		10	X					
	Domain 4: Privilege Escalation	25	X		3	25	25	25
	Domain 5: Pivoting and file transfers	15	X		1	8.33	15	15
	Reporting	10		X	1	8.33	10	10
	Total points	100						
	Number of tasks per level of understanding		7	5				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		58.3	41.66				

The passing score of the exam is **70%**. That score can be reached by successfully documenting the process of compromising at least two machines in a written report.

After successfully passing the exam, candidates will be able to apply for the "PECB Certified Lead Ethical Hacker" credential depending on their level of experience.

Taking the Exam

General Information on 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.

PECB Exam Format and Type

- **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 detailed information about the online format, please refer to the PECB Online Exam Guide.

The PECB Certified Lead Ethical Hacker Exam comprises of two parts:

1. Practical exam
2. Report writing

The duration of the exam is a **six-hour session for the practical exam**, where you are required to use the CherryTree note-taking application to save all the evidence related to the completion of the exam objectives (the CherryTree application, featuring rich text and syntax highlighting, must be downloaded prior to the exam from this link: https://www.giuspen.com/cherrytree/), and **twenty-four hours for writing the report**, after the practical exam has ended.

For uploading the exam report and the CherryTree notes, after completing the practical exam and writing the report respectively, please log in to "myPECB dashboard," go to the "Scheduled Exams" tab, and under the Lead Ethical Hacker exam click on "Upload Exam Reports." You can download an exam report template by using the same tab, in order to get familiar with the exam report.

As a summary, after six hours of your exam start time, you are required to submit the CherryTree notes. After this six-hour period has passed, the practical part of the exam will end and the reporting part will start. You will have twenty-four hours to complete the reporting section, for which you are required to download the exam report template. Once you complete the report, including the addition of screenshots that were taken during the practical exam from the CherryTree application, you are required to submit the exam report. The screenshots in the exam report should match the notes that have already been submitted after the practical exam. No new information different from the CherryTree notes will be accepted.

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.

The exam is open book and is not intended to measure memorizing or recalling information. It aims to evaluate candidates' comprehension, analytical skills, and applied knowledge. Therefore, candidates should be able to justify their answers by providing explanations using screenshots. You will find a sample of one of the exam tasks provided below.

Since the exam is "open book," candidates are authorized to use the following reference materials:

- Training course materials (accessed through PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through PECB Exams app and/or printed)
- Books and online materials
- A hard copy dictionary

Any attempt to cheat during the exam session will lead to automatic failure.

PECB exams are available in English and other languages. To learn if the exam is available in a particular language, please contact examination@pecb.com.

Sample Exam Tasks

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.

Receiving the Exam Results

Exam results will be communicated via email. The only possible results are *pass* and *fail*; no specific grade will be included. The time span for the communication starts from the exam date and lasts three to eight weeks.

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 results@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 allowed time span between exam retakes.

- If a candidate does not pass the exam on the 1st attempt, they must wait 15 days from the initial date of the exam for the next attempt (1st retake). Retake fees apply.
  Note: *Candidates who have completed the training course but failed the exam are eligible to retake the exam once for free within a 12-month period from the initial date of the exam*.
- If a candidate does not pass the exam on the 2nd attempt, they must wait three months after the initial date of the exam for the next attempt (2nd retake). Retake fees apply.
  Note: For candidates that fail the exam in the 2nd retake, PECB recommends them to attend a training course in order to be better prepared for the exam.
- If a candidate does not pass the exam on the 3rd attempt, they must wait six months after the initial date of the exam for the next attempt (3rd retake). Retake fees apply.
- After the 4th attempt, the waiting period for further retake exams is 12 months from the date of the last attempt. Retake fees apply.

To arrange exam retakes (date, time, place, costs), candidates need to contact the PECB Reseller/Distributor who has initially organized the session.

Exam Security

A significant component of a professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certification holders and applicants to maintain the security and confidentiality of PECB exams. Any disclosure of information about the content of PECB exams is a direct violation of PECB's Code of Ethics. PECB will take action against any individuals that violate such rules and policies, including permanently banning individuals 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.

Reschedule the Exam

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

Apply for Certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined 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 online profile), including contact details of references who will be contacted to validate the candidate's professional experience. Candidates can submit their application in various languages. Candidates can choose to either pay online or be billed. For additional information, contact certification@pecb.com.

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

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

For more information about the application process, follow the instructions on this manual Apply for Certification.

The application is approved as soon as the Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. An email will be sent to the email address provided during the application process to communicate the application status. If approved, candidates will then be able to download the certification from their PECB Account.

PECB provides support in both English and French.

Renew your Certification

PECB certifications are valid for three years. To maintain them, candidates must demonstrate that they are still performing tasks that are related to the certification. PECB certified professionals must annually provide Continual Professional Development (CPD) credits to demonstrate at least one year of professional experience acquired over the past three years, in activities or tasks related to the certification field, and pay $100 as the Annual Maintenance Fee (AMF) to maintain the certification. For more information, please visit the Certification Maintenance page on the PECB website.

Closing a Case

If candidates do not apply for certification within three years, 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 and pay the required fee.

PECB

SECTION III: CERTIFICATION REQUIREMENTS

Certified Lead Ethical Hacker

The requirements for PECB Certified Lead Ethical Hacker certifications are:

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Lead Ethical Hacker	PECB Certified Lead Ethical Hacker exam	Two years of 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

PECB

SECTION IV: CERTIFICATION RULES AND POLICIES

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.

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.

Evaluation of Certification Applications

The Certification Department will evaluate each application to validate the candidate's eligibility for certification. 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 can eventually lead to its downgrade to a lower credential.

Denial of Certification

PECB can deny certification if candidates:

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

For more detailed information, refer to "Complaint and Appeal" section.

The application payment for the certification is non-refundable.

Suspension of Certification

PECB can temporarily suspend certification if the candidate fails to satisfy the requirements. Other reasons for suspending certification include:

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

Revocation of Certification

PECB can revoke certification if the candidate fails to fulfill the PECB requirements. Candidates are then no longer allowed to represent themselves as PECB certified professionals. Other reasons for revoking certification can be if candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of the certification
- Break any other PECB rules

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. More information about these statuses and the permanent cessation status, and how to apply, please visit Certification Status Options.

PECB

SECTION V: PECB GENERAL POLICIES

PECB Code of Ethics

Adherence to the PECB Code of Ethics is a voluntary engagement. It is important that PECB certified professionals not only adhere to the principles of this Code, but also encourage and support the same from others. More information can be found here.

Other Exams and Certifications

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 candidate's age, gender, race, religion, nationality, or marital status.

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the Reseller/Distributor in order for them to make proper arrangements. Any information candidates provide regarding their disability/need will be treated with strict confidentiality.

Click here to download the Candidates with Disabilities Form.

Complaints and Appeals

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 they do not find the response satisfactory, the candidate has the right to file an appeal. For more information about the complaints and appeal procedures, click here.

(1) 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.

(2) 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

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.

Emails:
Examination: examination@pecb.com
Certification: certification@pecb.com
Customer Service: customer@pecb.com