



PECB

Candidate Handbook

Certified Artificial Intelligence Security
Professional

Contents

SECTION I: INTRODUCTION.....	3
About PECB	3
Accreditations and Affiliations	3
PECB Code of Ethics.....	3
Introduction to Certified Artificial Intelligence Security Professional Certification	4
SECTION II: EXAM PROCESS, RULES AND POLICIES	5
Preparing For and Scheduling the Exam.....	5
Special Accommodations.....	5
Taking the Exam.....	5
Exam Results.....	6
Exam Retake Policy.....	6
Exam Security Policy	6
Exam Competency Domains	7
Sample Exam Questions.....	13
SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES	15
PECB Certified Artificial Intelligence Security Professional Credentials	15
Applying for Certification	15
Professional Experience	16
Professional References	16
Project Experience	16
Evaluation of Certification Applications.....	16
SECTION IV: CERTIFICATION MAINTENANCE POLICY	17
Renewing the Certification	17
Upgrade Credentials	17
Suspension of Certification	17
Revocation of Certification	17
Other Statuses	17
SECTION V: OTHER POLICIES	18
Application Fees for Examination and Certification	18
Complaint and Appeal Policy	18
Exams from Other Accredited Certification Bodies.....	18
Refund Policy	18

SECTION I: INTRODUCTION

About PECB¹

PECB is a leading certification body dedicated to fostering digital trust through comprehensive education, certification, and certificate programs across various disciplines. We empower professionals to develop and demonstrate their competence in digital security and other areas of expertise by providing world-class certification programs that adhere to internationally recognized standards.

Vision: As the global leader in digital trust education and certification, our vision is to empower and inspire professionals by enhancing their skills and fostering their professional success.

Mission: Our mission is to empower professionals with the knowledge and skills to protect their digital assets and ensure business continuity. Through our comprehensive programs, we aim to foster a secure digital ecosystem where innovation thrives and risks are managed effectively.

Values: Growth, Change, Harmony, Simplicity, Reliability, and Quality

Accreditations and Affiliations

At PECB, we are driven and culturally powered by a systemic process of continual improvement and professional development. As a testament to our high standards and commitment to providing quality services to our clients, PECB is accredited by a number of bodies and is a member of many professional organizations.

For detailed information on our accreditations and affiliations, click [here](#).

PECB Code of Ethics

The Code of Ethics is the set of values that PECB is committed to following, and defines the responsibilities of PECB professionals, including employees, trainers, examiners, invigilators, members of different committees, partners, distributors, certified individuals, and certificate holders. To read the PECB's Code of Ethics, click [here](#).

¹ Notes:

- The legal name of PECB is "PECB Group Pte. Ltd."
- PECB is an acronym that stands for "Professional Evaluation and Certification Board."
- Education (used in the first sentence of this page) refers to training courses developed by PECB, and offered globally through its network of partners.
- Certification refers to certification services provided according to ISO/IEC 17024. Certificate Program refers to certificate program services provided according to ANSI/ASTM E2659.
- "Certified" refers to ISO/IEC 17024 certifications' requirements and "Certificate holder" refers to ASTM E2659 certificate programs' requirements. Certificate holders are not certified, licensed, accredited, or registered to engage in a specific occupation or profession.

Introduction to Certified Artificial Intelligence Security Professional Certification

This document specifies the PECB Certified Artificial Intelligence Security Professional certification scheme in compliance with ISO/IEC 17024. 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 certification application.

If you have questions or need further information after reading it, please contact support@pecb.com.

SECTION II: EXAM PROCESS, RULES AND POLICIES

For detailed and most up-to-date information, you are advised to refer to the online **Exam Rules and Policies** by clicking [here](#).

Preparing For and Scheduling the Exam

To schedule the exam, candidates have two options:

1. **Online:** Through the [PECB Exams application](#). To schedule a remote exam, please go to the following link: [Exam Events](#).
2. **Paper-based:** By contacting the PECB authorized partner that provided the training course. The partner arranges the date, time, and location where the candidate is going to attend the exam.

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

Special Accommodations

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of special needs (dyslexia, dyspraxia, ADHD, vision impairment, but not limited to) and temporary conditions (pregnancy, surgery, postoperative recovery, but not limited to), they can apply for such arrangements through the [myPECB](#) dashboard/ Enroll for an Exam. Any information that candidates provide regarding their special needs will be treated with confidentiality.

Taking the Exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts. Candidates who arrive late will not receive additional time to make up for the delay and may not be allowed to sit for the exam.

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

Online Exam Rules	Paper-Based Exam Rules
• Exams are provided electronically via the PECB Exams application. • The use of secondary electronic devices, such as tablets and phones, is not allowed during the exam. • The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera. • If requested on the day of the exam, 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	• 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. • If requested on the day of the exam, 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

For specific information on exam types, languages available, and other details, please check the [List of PECB Exams](#).

Exam Results

Exam results will be communicated via email.

- The time span for the communication of exam results 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.

If candidates disagree with the evaluation, they may request a re-evaluation of their exam results within 30 days from the date they receive their exam results. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

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. For more information, please visit this link: [Exam Rules and Policies - PECB](#).

Exam Security Policy

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 who violate such rules and policies, including permanently banning individuals from pursuing PECB credentials and revoking/invalidating any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam Competency Domains

The content of the exam is divided as follows:

Domain 1: Security foundations for AI and ML

Main objective: Ensure that the candidate is able to explain and apply the fundamental concepts, principles, technologies, and security considerations of artificial intelligence (AI), machine learning (ML), deep learning, and modern AI systems.

Competencies	Knowledge statements
1. Ability to explain the fundamental concepts, terminology, and evolution of artificial intelligence and machine learning	1. Knowledge of the history, evolution, terminology, and key concepts of artificial intelligence and machine learning
2. Ability to distinguish between AI, ML, deep learning, generative AI, and large language models (LLMs)	2. Knowledge of characteristics, capabilities, limitations, and use cases of AI, ML, deep learning, generative AI, and LLMs
3. Ability to explain the main types of ML and their practical applications	3. Knowledge of supervised, unsupervised, semi-supervised, and reinforcement learning approaches
4. Ability to interpret the architecture, components, and life cycle of modern AI systems	4. Knowledge of neural networks, deep learning architecture, and their role in modern AI systems
5. Ability to explain the role of data in AI systems, including data collection, preparation, training, validation, and testing	5. Knowledge of AI system components, including data sources, models, training environments, inference systems, APIs, and supporting infrastructure
6. Ability to identify common AI security, privacy, and ethical risks affecting AI systems	6. Knowledge of the AI and ML life cycle, including data acquisition, preprocessing, training, validation, deployment, monitoring, and retirement
7. Ability to explain the principles and operation of deep learning models and neural networks	7. Knowledge of data quality, data governance, bias, fairness, and explainability concepts in AI systems
8. Ability to identify key components, stakeholders, and assets within AI ecosystems	8. Knowledge of AI-specific security risks, including model manipulation, adversarial attacks, data poisoning, model theft, and privacy leakage
9. Ability to explain the security implications of AI adoption in organizational environments	9. Knowledge of ethical principles applicable to AI systems, including transparency, accountability, fairness, and privacy
10. Ability to differentiate between traditional cybersecurity risks and AI-specific threats	10. Knowledge of the business, operational, and security challenges associated with deploying and maintaining AI-enabled systems

Domain 2: AI attack techniques and adversarial threats

Main objective: Ensures that the candidate is able to analyze and respond to AI-specific attack techniques, adversarial threats, and vulnerabilities affecting machine learning systems, large language models (LLMs), and modern AI applications.

Competencies	Knowledge statements
1. Ability to explain the threat landscape of AI and ML systems 2. Ability to identify adversarial attacks targeting AI models throughout the AI life cycle 3. Ability to explain the objectives, methods, and impact of data poisoning attacks 4. Ability to explain model evasion and adversarial example attacks against ML systems 5. Ability to analyze threats targeting LLMs, including prompt injection and jailbreaking attacks 6. Ability to identify risks related to model extraction, model inversion, and unauthorized disclosure of sensitive information 7. Ability to explain AI supply chain attacks affecting models, datasets, libraries, and third-party AI components 8. Ability to interpret adversarial tactics and techniques using AI threat frameworks and knowledge bases 9. Ability to assess the security implications of AI system compromise, manipulation, and misuse 10. Ability to recommend security controls and mitigation strategies against AI-specific attacks	1. Knowledge of the AI threat landscape and differences between traditional cybersecurity threats and AI-specific attacks 2. Knowledge of adversarial ML concepts, objectives, and attack methodologies 3. Knowledge of data poisoning attacks, label poisoning, backdoor attacks, and data integrity compromise techniques 4. Knowledge of evasion attacks, adversarial examples, and manipulation of model decision boundaries 5. Knowledge of prompt injection, indirect prompt injection, jailbreaking, and other attacks targeting LLM applications 6. Knowledge of model extraction, model stealing, model inversion, membership inference, and privacy leakage attacks 7. Knowledge of AI supply chain threats, including malicious model files, poisoned LoRA adapters, compromised dependencies, and untrusted model repositories 8. Knowledge of AI attack tactics, techniques, and procedures (TTPs) documented in frameworks such as MITRE ATLAS and OWASP Top 10 for LLM Applications 9. Knowledge of attack surfaces across AI systems, including training environments, inference endpoints, APIs, plugins, agents, and retrieval mechanisms 10. Knowledge of preventive, detective, and corrective security controls used to mitigate adversarial threats against AI systems

Domain 3: AI security controls and defensive operations

Main objective: Ensure that the candidate can implement, monitor, and evaluate AI security controls and defensive operations, including preventive, detective, and corrective measures, security monitoring and logging, anomaly and drift detection, and SIEM/SOAR integration, in order to detect, analyze, and respond to threats affecting AI systems throughout their operational life cycle.

Competencies	Knowledge statements
1. Ability to explain the purpose and application of AI security controls AI systems and operations	1. Knowledge of security control categories and defense-in-depth principles applicable to AI systems
2. Ability to identify preventive, detective, and corrective controls used to protect AI assets	2. Knowledge of AI-specific security controls for data protection, model protection, input validation, output filtering, access control, and runtime security
3. Ability to implement monitoring and logging mechanisms for AI systems and AI-enabled environments	3. Knowledge of monitoring, logging, telemetry collection, and audit trail requirements for AI systems
4. Ability to analyze AI security events, anomalies, and indicators of compromise	4. Knowledge of anomaly detection, model drift detection, concept drift detection, and performance monitoring techniques
5. Ability to explain the role of threat hunting and continuous monitoring in AI-security operations	5. Knowledge of Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) integration for AI environments
6. Ability to explain the role of threat hunting and continuous monitoring, detection, and analysis	6. Knowledge of AI-driven security monitoring, threat detection, and threat-hunting methodologies
7. Ability to identify and address abnormal AI model behavior, including drift and performance degradation	7. Knowledge of indicators of compromise, attack patterns, and suspicious behaviors affecting AI and ML systems
8. Ability to integrate AI systems into security operations processes, including SIEM and incident response workflows	8. Knowledge of AI-enhanced threat intelligence, threat analysis, and security analytics processes
9. Ability to evaluate the effectiveness of AI security controls in protecting models, data, and infrastructure	9. Knowledge of AI-assisted security analysis, reverse engineering, and operational decision-support capabilities
10. Ability to support the continuous improvement of AI security operations through threat intelligence, automation, and operational feedback	10. Knowledge of operational best practices for maintaining the security, resilience, availability, and trustworthiness of AI systems throughout their life cycle

Domain 4: AI enhanced security analysis and threat intelligence

Main objective: Ensure that the candidate is able to analyze and apply AI-enhanced security analysis and threat intelligence techniques to improve threat detection, threat investigation, cyber threat intelligence production, and security decision-making in AI-enabled environments

Competencies	Knowledge statements
1. Ability to explain the role of AI in cybersecurity analysis and threat intelligence operations	1. Knowledge of the principles, objectives, and processes of cyber threat intelligence and security analysis
2. Ability to identify opportunities for applying AI technologies to threat detection, investigation, and intelligence activities	2. Knowledge of AI technologies used to support threat intelligence, security analytics, and cyber defense operations
3. Ability to analyze cyber threat information using AI-assisted tools and techniques	3. Knowledge of threat intelligence life cycle activities, including collection, processing, analysis, dissemination, and feedback
4. Ability to interpret indicators of compromise (IoCs), indicators of attack (IoAs), and threat intelligence findings generated or enhanced by AI systems	4. Knowledge of indicators of compromise (IoCs), indicators of attack (IoAs), threat actors, attack campaigns, and adversarial TTPs
5. Ability to explain the use of AI for threat intelligence collection, correlation, enrichment, and prioritization	5. Knowledge of AI-assisted threat intelligence collection, correlation, enrichment, summarization, and prioritization techniques
6. Ability to assess the reliability, accuracy, and limitations of AI-generated security analysis and threat intelligence outputs	6. Knowledge of AI applications for threat hunting, anomaly detection, pattern recognition, and predictive analysis
7. Ability to support threat hunting and proactive security operations using AI-enhanced analytical capabilities	7. Knowledge of AI-assisted malware analysis, reverse engineering, code analysis, and forensic investigation techniques
8. Ability to explain the role of AI in malware analysis, reverse engineering, and security investigations	8. Knowledge of threat intelligence frameworks and knowledge bases, including MITRE ATT&CK, MITRE ATLAS, OWASP Top 10 for LLM Applications, and other relevant intelligence resources
9. Ability to identify risks associated with the use of AI in security analysis and threat intelligence processes	9. Knowledge of the strengths, limitations, biases, and risks of AI-generated intelligence and security analysis
10. Ability to integrate AI-enhanced intelligence and analytical outputs into security operations and decision-making processes	10. Knowledge of governance, validation, and human oversight mechanisms necessary to ensure trustworthy AI-assisted security analysis and threat intelligence operations

Domain 5: AI governance, risk management, and secure architecture

Main objective: Ensure that the candidate is able to implement and evaluate AI governance, risk management, compliance, incident readiness, and secure architecture principles to support the secure, trustworthy, and responsible development and operation of AI systems.

Competencies	Knowledge statements
1. Ability to explain the principles, objectives, and components of AI governance 2. Ability to establish governance mechanisms that support accountability, transparency, fairness, and privacy in AI systems 3. Ability to identify, assess, and manage risks throughout the AI life cycle 4. Ability to perform threat modeling for AI systems using established methodologies and frameworks 5. Ability to interpret legal, regulatory, and standards-based requirements applicable to AI systems 6. Ability to explain the principles and implementation of AI incident readiness and AI-specific incident response planning 7. Ability to design secure AI architectures that address both traditional cybersecurity threats and AI-specific risks 8. Ability to apply Zero Trust principles to AI data, models, pipelines, and inference environments 9. Ability to evaluate AI supply chain security controls, model provenance, and model integrity mechanisms 10. Ability to support continuous governance, compliance, monitoring, and improvement activities for AI systems	1. Knowledge of AI governance principles, objectives, organizational structures, policies, roles, and responsibilities 2. Knowledge of ethical AI principles, including transparency, accountability, fairness, explainability, human oversight, and privacy 3. Knowledge of AI risk management concepts, methodologies, and risk treatment approaches throughout the AI system life cycle 4. Knowledge of AI threat modeling methodologies and frameworks, including STRIDE, DREAD, MITRE ATLAS, and other AI security knowledge bases 5. Knowledge of applicable AI-related laws, regulations, and standards, including the EU AI Act, ISO/IEC 42001, and the NIST AI Risk Management Framework 6. Knowledge of AI incident readiness, incident classification, response planning, recovery activities, and post-incident improvement processes 7. Knowledge of secure AI architecture principles, defense-in-depth strategies, and Zero Trust architectures for AI systems 8. Knowledge of AI security control domains, including identity and access management, model and data protection, runtime security, observability, safety guardrails, and governance controls 9. Knowledge of AI supply chain security concepts, including model provenance, model signing, Software Bill of Materials (SBOM), AI Bill of Materials (AIBOM), and third-party AI component risk management 10. Knowledge of AI red teaming, security validation, continuous monitoring, compliance assessment, auditing, and continual improvement practices for secure and trustworthy AI systems

Based on the above-mentioned domains and their relevance, the exam contains **80 multiple-choice questions**, as summarized in the table below:

				Level of understanding (Cognitive/Taxonomy) required	
		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Questions that measure comprehension, application, and analysis	Questions that measure evaluation
Competency domains	Security foundations for AI and ML	30	37.5%	X	
	AI attack techniques and adversarial threats	10	12.5%	X	
	AI security controls and defensive operations	15	18.75%		X
	AI enhanced security analysis and threat intelligence	10	12.5%		X
	AI governance, risk management, and secure architecture	15	18.75%		X
Total		80	100%		
Number of questions per level of understanding				40	40
% of the exam devoted to each level of understanding (cognitive/taxonomy)				50%	50%

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

This exam comprises multiple-choice questions: The multiple-choice exam can be used to evaluate candidates' understanding of both simple and complex concepts. It comprises both stand-alone and scenario-based questions. Stand-alone questions stand independently within the exam and are not context-dependent, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario that a candidate is asked to read and is expected to provide answers to five questions related to that scenario. When answering stand-alone and scenario-based questions, candidates will have to apply various concepts and principles explained during the training course, analyze problems, identify and evaluate alternatives, combine several concepts or ideas, etc.

Each multiple-choice question has three options, of which one is the correct response option (keyed response) and two incorrect response options (distractors).

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)

A sample of exam questions will be provided below.

Sample Exam Questions

MedAI Health Services deploys an AI platform called MedAssist that uses machine learning models and an LLM to support patient services and detect fraudulent insurance claims. The LLM processes each prompt by evaluating the relationships among its words and assigning greater importance to the words most relevant to the context. The platform relies on healthcare datasets, APIs connected to medical systems, and third-party AI models obtained from external repositories. The company follows an AI life cycle that includes data collection, training, validation, deployment, and continuous monitoring.

Several months after deployment, the security team discovers that manipulated records were added to a training dataset, used to retrain the fraud detection model. By compromising the integrity of the training data, the attackers altered the model's learned behavior, causing fraudulent claims to receive lower risk scores and be incorrectly classified as legitimate. At the same time, attackers used specially crafted prompts to make the chatbot reveal internal information.

Analysts also observe large numbers of automated queries designed to understand and reproduce the model's behavior, while a third-party model package is suspected of being tampered with before deployment. Before loading the model into production, the security team verifies its digital signature, and the verification succeeds, conforming that the model comes from the claimed sources and has not been modified since it was signed.

The SOC activates the AI incident response plan and, as a containment measure, temporarily reverts the chatbot to a previously trusted model version. Additional controls are implemented, including input validation, output filtering, enhanced logging, and SIEM integration. The threat intelligence team uses AI-assisted tools to extract IP addresses, domains, and file hashes from incident reports and normalize them into a standard format before correlating indicators of compromise (IoCs) and mapping attacker activities to MITRE ATLAS.

Following the incident, the AI Governance Committee conducts risk assessments, threat modeling, and compliance reviews. The company implements model signing for third-party models obtained from external repositories. The company also adopts a Zero Trust architecture, including a Model Supply Chain Trust Layer to validate AI models and dependencies before deployment.

As part of its governance activities, the committee establishes policies, assigns roles and responsibilities, defines accountability, and maintains oversight of AI risk management across the organization. These arrangements support and enable the identification, analysis, measurement, and treatment of AI risks throughout the AI system life cycle.

Based on the scenario above, answer the following questions.

1. **MedAI's LLM evaluates the relationships among words in a prompt and determines which words are most relevant when generating a response. Which LLM capability enables this process?**
 - A. Rate Limiting
 - B. **Self-attention mechanism**
 - C. Model signing

2. During the investigation, analysts determined that manipulated records were inserted into the dataset used to retrain the fraud detection model. As a result, fraudulent transactions received lower risk scores and bypassed detection. Which attack technique most likely enabled this outcome?
 - A. Model extraction
 - B. **Data poisoning**
 - C. Membership inference

3. While analyzing a suspected attack against *MedAI*, the threat intelligence team used an LLM-based tool to identify IP addresses, domains, and file hashes from unstructured reports before converting them into a standard format for correlation. Which threat intelligence activity is being performed?
 - A. Model provenance verification
 - B. Model rollback
 - C. **IOC extraction and normalization**

4. The security team suspects that a third-party model obtained from a public repository may have been modified before deployment. Before loading the model into production, they verify its digital signature. What conclusion can the team make if the signature verification succeeds?
 - A. The model is free from vulnerabilities and bias.
 - B. **The model's integrity and authenticity can be verified.**
 - C. The model will achieve higher accuracy.

5. Following the incident, *MedAI's* Governance Committee evaluates AI risks, measures their impact, and implements treatment plans while maintaining oversight of the entire process. Which NIST AI RMF function supports and enables all other AI risk management activities?
 - A. **Govern**
 - B. Measure
 - C. Manage

SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES

PECB Certified Artificial Intelligence Security Professional Credentials

All PECB certifications have specific requirements regarding 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 Artificial Intelligence Security Professional** scheme have the following requirements:

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Provisional Artificial Intelligence Security Professional	PECB Certified Artificial Intelligence Security Professional exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified Artificial Intelligence Security Professional		5 years (2 in information or cybersecurity)	Project activities: A total of 300 hours	

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

1. Assessing the security posture of AI and ML systems, including LLM-based applications, AI agents, and automated pipelines
2. Analyzing adversarial threats targeting AI systems, including prompt injection, data poisoning model extraction, and supply chain compromise
3. Implementing security controls for AI systems, including input validation and output filtering
4. Supporting incident response activities involving AI system failures, security compromise using SIEM integration, and AI-specific telemetry
5. Conducting or supporting AI red team engagements, including capabilities testing and prompt testing

For detailed and most up-to-date information, you are advised to refer to the online **Certification Process** by clicking [here](#).

Applying for Certification

All participants who successfully pass their certification exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific professional requirements will need to be fulfilled to be PECB certified.

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

- [Create](#) your account
- Check your email for the confirmation link
- [Log in](#) and click on Apply for Certificate

The approval of the application occurs when the Certification Department validates that you fulfil all the certification requirements regarding the credential you have applied for. An email will be sent to the address you provided during your application to update you on your application status. If approved, you will then be able to download your certificate and digital badge from your member account.

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 CV.

Professional References

For each application, two professional references are required. Professional references shall be individuals who have worked with you in a professional environment and can validate your expertise in the respective field, current, and previous work history. You cannot use as a reference the persons who fall under your supervision or are a relative of yours.

Project Experience

The candidate's project log will be checked to ensure that the candidate has the required number of implementation hours.

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 can deny certification/certificate program if candidates:

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

If applicants have any concerns regarding the denial of certification/certificate program, they may file an appeal by following the complaint and appeal process [Complaint and Appeal Policy](#).

The application payment for the certification/certificate program is nonrefundable. This is due to the application verification process, the evidence submitted by the candidates, and the involvement of the relevant departments.

If candidates pass the exam, they can apply for the certificate within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats. 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.

SECTION IV: CERTIFICATION MAINTENANCE POLICY

For detailed and most up-to-date information, you are advised to refer to the online **Certification Maintenance Policy** by clicking [here](#).

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 continuing professional development (CPD) hours. In addition, they need to pay the annual maintenance fee.

Upgrade Credentials

PECB Certifications can be upgraded online through your dashboard by logging in [here](#), clicking **View Certificate**, and then clicking the **Upgrade** button. For more information on the upgrade requirements and fees, go to the [Certification Maintenance](#) page on the PECB website.

Suspension of Certification

Failure to submit the CPD and AMF payment during the certification cycle will result in a 12-month suspension period, during which you can address any outstanding AMFs and CPDs. In addition to these, the certification may be suspended for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been suspended are not authorized to further promote their certification while it is suspended.

Suspended members must remediate their suspension within a maximum period of 12 months.

Revocation of Certification

PECB can revoke (that is, withdraw) certification if the candidate fails to address the outstanding AMFs and CPDs during the 12-month suspension period. In addition to these, certification may be revoked for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been revoked are not authorized to use any references to a certified status.

If candidates disagree with any certification decision (certification level, suspension, or revocation) they may request a re-evaluation within 30 days from the date they receive their certification decision. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntary withdrawn, or designated as Emeritus. For more information, go to the [Certification Maintenance](#) page on the PECB website.

SECTION V: OTHER POLICIES

Application Fees for Examination and Certification

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

- Lead Exam: \$1000²
- Manager Exam: \$700
- Foundation Exam: \$500
- Transition Exam: \$500

The application fee for certification is as follows:

- Master Certification: \$100
- Foundation Certification: \$200
- Transition Certification: \$200
- All other Certifications: \$500

For candidates who complete a training, eLearning, or self-study course delivered by a PECB Partner, the training fee includes the first exam attempt, one free retake, the certification application fee, and the first year of the Annual Maintenance Fee (AMF). This cycle must be completed within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats.

Complaint and Appeal Policy

A person wishing to file a complaint or an appeal can do so by submitting a [service ticket](#) and selecting the corresponding category in the topic dropdown menu: “file a complaint” or “file a certification/certificate program appeal”. Before filing a complaint or an appeal, make sure to follow the [complaint and appeal policy](#).

Exams from Other Accredited Certification Bodies

PECB accepts exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective exam(s) can be accepted as equivalent to the respective PECB certification.

Refund Policy

PECB will refund your payment if the requirements of the Refund Policy are met. To read the Refund Policy, click [here](#).

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



Contact PECB Support at
support@pecb.com



Telephone number
+1-844-426-7322



Visit our [Help Center](#) to access manuals, FAQs, and quick guides, or reach us directly via Live Chat or by submitting a ticket [here](#).

Follow us on:



www.pecb.com