PROJECT NOTIFICATION

Reference No.: 585

Date of Issue	27 March 2025
Project Code	25-CP-40-GE-DLN-A
Title	APO e-Course on Cybersecurity Management Systems (Basic)
Timing	29 August 2025
Hosting Country(ies)	APO Secretariat
Venue City(ies)	Not Applicable
Modality	Digital Learning
Implementing Organization(s)	APO Secretariat
Participating Country(ies)	Open
Overseas Participants	Not Applicable
Local Participants	Not Applicable
Closing Date	Not Applicable
Remarks	Timing is the launch date of the e-course.

Objectives	Understand fundamental cybersecurity concepts and risk assessment techniques; learn to identify vulnerabilities, monitor threats, and implement effective cybersecurity measures; and strengthen SME cybersecurity resilience by applying key principles and frameworks following international standards.
Rationale	In today's digital landscape, SMEs face increasing cybersecurity threats that can result in financial losses, reputational damage, and operational disruptions. Implementing effective security measures, such as those outlined in international standards, is essential to safeguard assets, maintain customer trust, and ensure business continuity.
Background	The rapid adoption of digital technologies has increased efficiency and productivity but has also led to a surge in cybersecurity threats. According to Checkpoint Research and Microsoft Security (2024), organizations experienced an average of 1,876 cyberattacks per week in Q3 2024, a 75% increase compared with 2023. Additionally, 31% of SMEs reported cyberattacks involving ransomware, phishing, and data breaches, highlighting the urgent need for improved security strategies. Building on the APO's 2023 Training Course on Cybersecurity Management Systems, this e-course provides SMEs with practical cybersecurity strategies. It covers cybercrime ecosystems, risk assessment, password management, data protection, incident response, and applications of international standards to help SMEs mitigate risks effectively and strengthen long-term security.
Topics	Introduction to cybersecurity: Global landscape and emerging threats; Cybercrime ecosystems: Cybercriminals, tactics, and underground marketplaces; Password management and safe practices: Secure authentication and browsing habits; Data protection: Encryption, secure storage, and compliance; and Incident response and cybersecurity culture: Using international frameworks.
Outcome	Participants gain a comprehensive understanding of cybersecurity, including identifying vulnerabilities, implementing security measures, and responding to cyberthreats. They will also learn to apply principles from international standard frameworks to enhance SME security and business continuity.
Qualifications	Open to all participants in APO members and nonmembers.

Please refer to the implementation procedures circulated with this document for further details.

Dr. Indra Pradana Singawinata
Secretary-General