APCICT
Asian and Pacific Training Centre for Information and Communication Technology for Development
ESCAP

Training on Cybersecurity and Information Security for the Public Sector

28-29 July 2026, Double Tree by Hilton, Vientiane [Draft]

COURSE SYNOPSIS

In an era of rapidly advancing digital technologies, countries are increasingly exposed to a wide range of cybersecurity threats, including cyber intrusions. These threats can pose significant risks to national security, economic stability, critical infrastructure, and the protection of personal data. Many countries, however, continue to face challenges in developing the institutional capacity, legal frameworks, and technical expertise required to effectively prevent, detect, and respond to such risks. Strengthening national cybersecurity governance through comprehensive policies, strategies, and coordinated institutional mechanisms has therefore become a critical priority.

Training on Cybersecurity and Information Security for the Public Sector is a two-day intensive executive training, which aims to strengthen participants' understanding of key concepts related to information security and data protection, raise awareness of emerging cyber threats, and support the assessment of existing national policies against international good practices and standards. It also seeks to build participants' capacity to formulate, implement, and recommend effective cybersecurity and information security policies that contribute to a safer and more resilient digital environment.

COURSE FOCUS

This programme focuses on the executive's role in securing the digital frontier, with emphasis on:

- Developing coordinated institutional mechanisms and strategies.
- Identifying and mitigating intrusions, and data breaches.
- Aligning national policies with international standards.
- Building the technical and legal expertise required for rapid response.

COURSE OBJECTIVES

By the end of the programme, participants will be able to:

- Evaluate the impact of cybersecurity threats on national security and economic stability.
- Distinguish between various cyber-risks.
- Benchmark existing national policies against international best practices and privacy standards.
- Assess institutional capacity for preventing and detecting advanced digital threats.
- Formulate high-level recommendations for resilient information security policies.

LEARNING OUTCOMES

At the end of the programme, participants are expected to:

- Define information security, privacy and related concepts;
- Identify threats to information security;
- Assess existing information security policy in terms of international standards of information security, freedom of expression and privacy and data protection; and
- Formulate or make recommendations regarding information security policy that would be appropriate to their countries.

RESOURCE PERSON

Mr. Freddy Tan is the Managing Director of EPIC Cybersecurity, a Singapore-based cybersecurity firm. He holds a Master of Science in Information Systems Security from the London School of Economics & Political Science and is a long-standing Certified Information Systems Security Professional (CISSP). With a distinguished career spanning over 25 years, Mr. Tan began his work in cybersecurity with Singapore's Ministry of Defence, where he established the 24/7 Computer Security Monitoring & Investigation Centre (COSMIC) and the Computer Emergency Response Team (SAFCERT). He has also held senior leadership roles in industry, including with Singtel, StarHub, and Microsoft, and is recognised for his contributions to the profession with honours such as the $(ISC)^2$ President's Award and Singapore's Long Service Medal (Pingat Bakti Setia). Mr. Tan is active in the professional community and has served as a founding member and committee leader in regional cybersecurity associations.

TARGET AUDIENCE

This training targets officials involved in national cybersecurity strategies, digital government, and IT and network security officers within the Ministry and affiliated agencies.

CONTACTS

- Ms. Nuankae Wongthawatchai, Programme Management Officer, APCICT/ESCAP, wongthawatchai@un.org

PROGRAMME AGENDA

	Day 1
Time	Description
09:00 – 09:30 (30 Minutes)	**Opening Session** **Group Photo**
09:30 – 10:45 (75 minutes)	**Session 1: Need for Information Security** • Explain the concept of information and information security • Present information security as a risk-based governance function that supports national security, public service continuity, and citizen trust; and • Describe international standards applied to information security activities and the right to privacy
10:45 – 11:00 (15 Minutes)	*Morning Break*
11:00 – 12:30 (90 Minutes)	**Session 2: Information Security Trends and Directions** • Provide an overview of threats to cybersecurity; and • Describe countermeasures against such threats
12:30 – 13:30 (60 Minutes)	*Lunch Break*
13:30 – 14:15 (45 Minutes)	**Session 3: Information Security Activities** • Give examples of information security activities of various countries to serve as a guide in information security policymaking • Highlight government data governance, including data ownership, data classification and responsibility for data handling; and • Emphasize the role of international and inter-agency cooperation in implementing information security policy

14:15 – 15:00 (45 Minutes)	**Session 4: Information Security Methodology** • Describe internationally used administrative, physical and technical information security methodology • Explain how these controls are applied using a risk-based approach in the public sector
15:00 – 15:10 (10 Minutes)	*Afternoon Break*
15:10 – 16:00 (50 Minutes)	**Session 5: Group discussion**

	Day 2
Time	Description
09:00 – 10:30 (90 Minutes)	**Session 6: Protection of Privacy** • Trace changes in the concept of privacy • Describe international trends in privacy protection; and • Give an overview and examples of Privacy Impact Assessment
10:30 – 10:40 (10 Minutes)	*Morning Break*
10:40 – 12:00 (80 Minutes)	**Session 7: CSIRT Establishment and Operation** • Explain how to establish and operate a national Computer Security Incident Response Team (CSIRT); and • Provide models of CSIRT from various countries
12:00 – 13:00 (60 Minutes)	*Lunch Break*
13:00 – 14:00 (60 minutes)	**Session 8: Lifecycle of Information Security Policy** • Give an overview of the information security policymaking lifecycle; and • Discuss key policy issues including procurement and supply-chain security risks and vendor access to government data

14:00-14:15 (15 Minutes)	*Afternoon Break*
14:15 – 15:00 (45 Minutes)	**Closing**