Office of the Commissioner of Critical Infrastructure (Computer-system Security)
Security Bureau
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

Sectoral Code of Practice

for the Energy Sector

Pursuant to the Protection of Critical Infrastructures (Computer Systems) Ordinance

28 January 2026

Version 1.0

Office of the Commissioner of Critical Infrastructure (Computer-system Security)
Security Bureau
The Government of the Hong Kong Special Administrative Region of
the People's Republic of China

Amendment History

Change Number	Revision Description	Revision Number	Date
1	First release	1.0	28 January 2026

1. INTRODUCTION

1.1 Purpose and Scope

1.1.1 This Sectoral Code of Practice ("Sectoral Code") is published by the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") and is applicable to the Critical Infrastructure ("CI") operators in the Energy Sector only.

1.1.2 In addition to the generic Code of Practice published by the Commissioner ("the Generic Code"), this Sectoral Code aims to provide supplementary practical guidance on how CI operators in the Energy Sector comply with their obligations. Unless otherwise specified in this Sectoral Code, all the requirements in the Generic Code should prevail.

2. OBLIGATIONS OF CI OPERATORS

2.1 Security measures for the Energy Sector

2.1.1 The sections 2.1.2 – 2.1.6 provide alternative security measures for critical computer systems ("CCSs") that are Operational Technology ("OT") systems, or refine the scope of security requirements for OT systems.

2.1.2 Alternative to section 6.2.10(e) in the Generic Code, if timely revocation of user privileges and data access rights in OT systems is not technically feasible when they are no longer required, the CI operator should implement compensating controls, including stringent physical security controls, air-gapped environments and prohibition on remote access. The CI operator should also define and document the timeline for revoking user privileges and data access rights for each CCS in the computer-system security management plan.

2.1.3 With reference to section 6.2.14(d) in the Generic Code, communication cables of OT systems refer to cables used to interconnect computer systems. Cable labels, or alternative identification measures best suited to the environmental conditions and enabling effective tracing of cabling routes, shall be applied.

2.1.4 Alternative to section 6.2.15(c) in the Generic Code, the CI operator should perform OT system hardening based on the latest recommendations directly provided by the system manufacturer or original equipment manufacturer ("OEM"). The hardening should also be supported by documented testing evidence and risk evaluation.

2.1.5 Alternative to sections 6.2.21(b) and (c) in the Generic Code, a CI operator should implement monitoring measures at supervisory control and data acquisition ("SCADA") or human-machine interface ("HMI") level to identify operational anomalies such as abnormal network traffic, abnormal system behaviors, or unauthorized commands within the OT environment.

2.1.6 Alternative to section 6.2.22(c) in the Generic Code, packaged OT software and scripts for OT systems are not considered as part of the software development of CCSs.