

Specification of Competency Standards
for the Manufacturing Technology.
Unit of Competency.

Functional Area - Business Intelligence and Information Technology

Title	Implement cybersecurity for Industry 4.0, promote network and information security control measures that simultaneously enable information exchange and ensure information system security in Industry 4.0
Code	111547L3
Range	This unit of competency is applicable to the business intelligence and information technology departments, marketing, sales and customer management departments / marketing departments, process design and development departments / engineering departments, and supply chain management departments of companies in the manufacturing technology industry. Practitioners should be capable to identify and implement appropriate Industry 4.0 cybersecurity controls and measures to maintain the integrity of business transactions, enterprise operations, and daily information exchanges, and prevent various types of cyber threats and attacks
Level	3
Credit	6
Competency	Performance Requirements - Understand relevant knowledge of implement Industry 4.0 cybersecurity - Understand foundation of Industry 4.0 network infrastructure - Understand principles of Industry 4.0 databases and server management - Understand current market solutions for Industry 4.0 network and information security - Understand principles and functions of industrial firewalls and control system security - Implement Industry 4.0 cybersecurity practices - Able to understand and interpret latest global cybersecurity trends - Able to identify types of cyber attacks, their methods, and apply appropriate prevention strategies - Able to assist management in identifying the most suitable cybersecurity solutions and vendors for enterprise's website and systems - Able to monitor and maintain stability of network security systems - Able to identify and collect various types of security vulnerabilities and threats within enterprise - Professional handling of cybersecurity for Industry 4.0 - Able to collaborate with management and cybersecurity vendors to assess and review enterprise network security risks and risk management - Able to promote awareness of enterprise and personal information security across all departments - Able to effectively install and maintain cybersecurity software to protect network from viruses and hacker attacks - Able to comply with relevant regulations and guidelines of telecommunications and network security laws - Able to continuously update knowledge on network architecture, cyber threats, and cybersecurity developments
Assessment Criteria	The integrated outcome requirements of this unit of competency are: Able to understand and implement appropriate Industry 4.0 network and information security control measures

	• Able to promote enterprise and personal information security awareness across departments according to the enterprise’s specific needs • Able to regularly assist management in conducting Industry 4.0 cybersecurity risk reviews, and ensure security measures are updated in response to technological advancements and changes in systems, networks, or the enterprise environment
Remark	