Unit code	BSBXXX139
Unit title	Develop Digital Cyber Security Skills
Unit outcomes	This unit describes a progressive pathway for developing workplace cyber security capability across four proficiency levels: Basic, Intermediate, Advanced and Highly Advanced. Learners may enter at a proficiency level aligned to existing capability and may exit upon successful completion of their target proficiency level without completing the entire progression. Recognition of Prior Learning and assessment-only pathways are supported. Learners develop progressive capability across five competence (C) areas: C1. Cyber security threat management C2. Workplace security C3. Data protection and privacy C4. Incident response C5. Security culture No licensing, legislative or certification requirements apply to this unit at the time of publication.
Knowledge (K)	Basic level Required knowledge includes: K1. Common workplace cyber security threats such as phishing, suspicious links, malware indicators, social engineering, and their impact. K2. Workplace security policies and procedures for protecting digital systems and information, including approved practices and prohibited activities. K3. Workplace requirements for handling sensitive information securely, including data classification, secure storage, sharing, and access controls. K4. Workplace incident response procedures, including threat reporting requirements, escalation pathways, and communication channels. K5. How individual security practices contribute to organisational cyber security culture and objectives. Intermediate level Required knowledge includes: K6. Common workplace cyber security threats, unauthorised access attempts and their operational impact. K7. Workplace security procedures for protecting digital systems, devices, and information. K8. Workplace requirements for protecting sensitive information, including access controls, secure storage, and data handling procedures.

	K9. Workplace procedures for reporting and escalating security concerns, and participating in response activities. K10. Approaches for supporting workplace security awareness and promoting secure workplace practices. Advanced level Required knowledge includes: K11. Examples of how emerging technologies, including Artificial Intelligence (AI) systems, are used in cyber attacks and cyber security controls. K12. Approaches for identifying and assessing cyber security threats and vulnerabilities. K13. Methods for implementing and monitoring security measures across organisational environments. K14. Data protection and privacy requirements, including compliance and access management. K15. Incident response coordination, recovery processes and stakeholder communication. K16. Strategies for promoting security awareness and building organisational security culture. Highly Advanced level Required knowledge includes: K17. Emerging trends in cyber security technologies, threat intelligence, data security, privacy governance, and compliance. K18. Frameworks and methodologies for threat management ecosystem design, data security strategy, incident response, and security culture governance. K19. Approaches for ethical security practices and proportionate use of technologies in cyber security contexts. K20. Principles for building capability in others across threat management, data protection, incident response and security culture. K21. Relevant legislative and governance frameworks relating to cyber security, data protection and privacy.
Skills (S)	Basic level Required skills include: S1. Recognise common workplace cyber security threats using workplace identification techniques. S2. Follow workplace security policies when using digital systems and handling information. S3. Handle data securely in accordance with organisational classification and protection requirements. S4. Report cyber security threats and incidents through appropriate workplace channels. S5. Demonstrate security-conscious behaviours that support workplace cyber security culture.

	Intermediate level Required skills include: S6. Recognise common workplace cyber security threats and determine appropriate responses. S7. Apply workplace security procedures to protect digital systems, devices, and information. S8. Protect sensitive workplace information using access controls, secure storage, and appropriate data handling. S9. Report security concerns and participate in response activities. S10. Support workplace security awareness and contribute to security culture. Advanced level Required skills include: S11. Assess cyber security threats, evaluate risk and advise colleagues on mitigation strategies. S12. Implement and monitor security measures across workplace systems. S13. Protect data, ensure privacy, maintain compliance, and lead data protection initiatives. S14. Coordinate incident response activities, support recovery processes and improve incident management capability. S15. Promote security awareness and develop programmes that build organisational security capability. Highly Advanced level Required skills include: S16. Maintain awareness of emerging cyber security, data security and governance developments to inform strategic decision-making. S17. Design and implement threat management ecosystems using security intelligence and emerging technologies. S18. Develop data security frameworks with privacy governance and compliance mechanisms. S19. Establish organisational incident response approaches and recovery strategies. S20. Create and govern security culture frameworks and support others to build advanced capabilities in workplace cyber security practices.
Application of Knowledge & Skills	Basic level Learners apply knowledge and skills under direct guidance and supervision, following clear instructions in straightforward routine tasks within familiar workplace contexts; accountable for completing assigned tasks accurately; escalate when encountering unfamiliar situations. Intermediate level Learners apply knowledge and skills with some autonomy under limited supervision, making informed decisions in varied tasks of moderate complexity; accountable for quality of their own work and supporting others with routine tasks; seek guidance when facing unfamiliar situations or ethical considerations.

	Advanced level Learners apply knowledge and skills with significant autonomy and initiative, making strategic decisions in tasks requiring analysis across diverse contexts; accountable for outcomes of their own and others' work; responsible for guiding others and contributing to capability development; identify when specialist expertise is required. Highly Advanced level Learners apply knowledge and skills independently with full accountability, exercising leadership in strategy development and organisational transformation; accountable for organisational capability and strategic outcomes; responsible for leading initiatives, establishing governance frameworks, and driving cultural change; determine when external expertise or board-level approval is required.
Assessment Requirements	
Performance evidence (PE)	Assessment must be conducted at the learner's target proficiency level, with assessors recognising that higher-level performance inherently incorporates lower-level competencies. Basic level Learners must demonstrate ability to: PE1. Recognise at least one common workplace cyber security threat using workplace recognition procedures under guidance. PE2. Follow workplace security policies when using digital systems and handling workplace information. PE3. Handle workplace data in accordance with organisational classification and protection requirements. PE4. Report cyber security threats or incidents through appropriate workplace channels. PE5. Demonstrate security-conscious behaviours that support workplace cyber security culture. Intermediate level Learners must demonstrate ability to: PE6. Recognise and respond to at least two different common workplace cyber security threats using established workplace procedures. PE7. Apply workplace security procedures to protect digital systems, devices, and information across varied contexts. PE8. Protect sensitive information using access controls, secure storage, and appropriate data handling. PE9. Report and escalate security concerns and participate in incident response activities.

	PE10. Support workplace security awareness and assist colleagues to apply secure practices. Advanced level Learners must demonstrate ability to: PE11. Identify and assess at least three different cyber security threats, evaluate risk, and advise colleagues on mitigation strategies. PE12. Implement and monitor security measures across workplace systems and processes. PE13. Protect workplace data, maintain privacy standards, ensure compliance, and lead data protection initiatives. PE14. Coordinate incident response activities, communicate with stakeholders, and improve incident management capability. PE15. Lead security awareness initiatives and develop programmes that build organisational security capability. Highly Advanced level Learners must demonstrate ability to: PE16. Design and implement threat management approaches that integrate security intelligence and emerging technologies. PE17. Develop data security frameworks incorporating privacy governance and compliance mechanisms. PE18. Establish organisational incident response approaches, including communication protocols and recovery strategies. PE19. Create and govern security culture frameworks and support others to build advanced cyber security capability. Performance evidence must be demonstrated across at least two different workplace scenarios.
Knowledge evidence (KE)	Basic level Learners must demonstrate knowledge of: KE1. Common workplace cyber security threats and their impact on organisational security. KE2. Workplace security policies and procedures for protecting digital systems and information. KE3. Workplace requirements for handling sensitive information, including data classification, secure storage and access controls. KE4. Workplace incident reporting and escalation procedures. KE5. How individual security practices contribute to workplace cyber security culture and organisational security objectives. Intermediate level

	Learners must demonstrate knowledge of: KE6. Common workplace cyber security threats, including unauthorised access attempts, and their organisational impact. KE7. Workplace security procedures for protecting digital systems, devices and information in routine contexts. KE8. Data protection requirements, including access controls, secure storage, and handling procedures. KE9. Procedures for reporting and escalating security concerns, and participating in incident response. KE10. Approaches for supporting workplace security awareness and contributing to security culture. Advanced level Learners must demonstrate knowledge of: KE11. The use of emerging technologies, including AI systems, in cyber attacks and cyber security. KE12. Approaches for identifying and assessing cyber security threats and vulnerabilities. KE13. Methods for implementing and monitoring security measures across organisational environments. KE14. Data protection, privacy and compliance requirements, including access management approaches. KE15. Incident response coordination, recovery processes and stakeholder communication. KE16. Strategies for promoting security awareness and building organisational security culture. Highly Advanced level Learners must demonstrate knowledge of: KE17. Emerging trends in cyber security technologies, threat intelligence, data security, privacy governance, and compliance. KE18. Frameworks and methodologies for threat management ecosystem design, data security strategy, incident response, and security culture governance. KE19. Approaches for ethical security practices and proportionate use of technologies in cyber security contexts. KE20. Principles for building capability in others across threat management, data protection, incident response and security culture. KE21. Relevant legislative and governance frameworks relating to cyber security, data protection and privacy.

	Knowledge evidence must be demonstrated across at least two different workplace scenarios.
Assessment conditions	Assessment must occur in conditions that reflect typical or simulated workplace environments appropriate to the target proficiency level, with higher-level assessment inherently incorporating lower-level requirements. All levels require access to: • workplace digital systems and organisational security procedures • assistive technologies where required to support diverse learner needs. Additionally, by proficiency level: Basic: • opportunities to identify cyber security threats in workplace contexts under guidance and supervision • workplace-relevant scenarios requiring security procedure application and incident reporting following established protocols. Intermediate: • security tools commonly used in organisational contexts • opportunities to recognise security threats and apply workplace security procedures across varied situations • workplace-relevant scenarios that require security protocol application, data protection, and incident reporting. Advanced: • digital environments with security systems and tools enabling realistic workplace implementation and evaluation • opportunities to implement security measures across varied workplace processes and contexts with diverse stakeholder groups • scenarios requiring risk assessment, data protection, incident response coordination, and awareness promotion across organisational settings • resources for implementing and assessing security effectiveness, compliance requirements, and incident management outcomes. Highly Advanced: • comprehensive cyber security platforms requiring strategic governance and integration • scenarios involving specialised security threats and cross-functional cyber security needs • opportunities to design, implement, and evaluate cyber security transformation initiatives

	• contexts requiring leadership and capability building of others in advanced digital cyber security • emerging security technologies and platforms requiring strategic evaluation and integration. Assessors must satisfy the requirements for assessors under applicable VET legislation, frameworks and standards.
Unit Mapping information	No equivalent unit.
Links	Link to BSB TP Companion Volume Implementation Guide.