Unit code	BSBXXX123
Unit title	Develop Advanced Digital Cyber security Skills
Unit outcomes	This unit describes the skills and knowledge required to apply cyber security practices and security initiatives across workplace contexts. Learners develop advanced capability across five competence (C) areas: C1. cyber security threat assessment C2. security implementation C3. data protection and privacy C4. incident response coordination C5. security culture development. No licensing, legislative or certification requirements apply to this unit at the time of publication.
Knowledge (K)	Required knowledge includes: K1. Identify examples of how emerging technologies are used in cyber attacks and cyber security. K2. Describe approaches for identifying, analysing and evaluating cyber security threats and vulnerabilities in workplace contexts. K3. Analyse methods for implementing security measures and maintaining secure systems. K4. Analyse data protection and privacy requirements, including security controls, access management and compliance considerations. K5. Evaluate incident response procedures, recovery processes and stakeholder communication approaches. K6. Evaluate strategies for promoting security awareness and building organisational security culture.
Skills (S)	Required skills include: S1. Identify and analyse cyber security threats in workplace contexts. S2. Evaluate risk levels using appropriate methods. S3. Promote organisation-wide security awareness and mitigation strategies. S4. Determine, implement and apply protective practices to maintain secure environments. S5. Monitor security effectiveness through systematic checking. S6. Lead data protection initiatives using appropriate security controls that build organisational capability. S7. Maintain privacy standards across systems and processes. S8. Manage access controls and compliance requirements.

	S9. Implement and coordinate incident response and recovery activities during security events. S10. Lead initiatives that improve incident management capability.
Application of Knowledge & Skills	At the Advanced level, learners apply knowledge (K1-K6) and skills (S1-S10) across all competence areas (C1-C5) with the following characteristics: • Autonomy: With significant autonomy and initiative, making strategic decisions and judgements based on analysis of cyber security requirements and organisational objectives. • Accountability: Accountable for outcomes of their own and others' work, quality of cyber security solutions, and effectiveness of security strategies implemented. • Responsibility: Responsible for guiding and supporting others, evaluating cyber security approaches, and contributing to organisational cyber security capability development. • Context: Workplace cyber security tasks requiring analysis, evaluation and strategic application across diverse organisational contexts, including situations with multiple variables and stakeholder considerations. • Decision-Making: Make strategic decisions about cyber security implementation and risk management approaches; evaluate effectiveness of security strategies; identify when specialist expertise or organisational policy development is required.
Assessment Requirements	
Performance evidence (PE)	Learners must demonstrate ability to: PE1. identify and assess at least three different cyber security threats in workplace contexts PE2. evaluate risk levels and advise colleagues on appropriate protective responses PE3. implement, monitor and systematically review security measures across workplace systems PE4. promote safe security practices PE5. protect workplace data and maintain privacy standards PE6. ensure compliance and lead data protection initiatives PE7. coordinate cyber security incident response and recovery activities PE8. communicate with stakeholders during security events PE9. review incident outcomes and lead improvements to incident management capability PE10. promote cyber security awareness and culture through awareness initiatives

	PE11. develop and implement programmes that embed sustainable organisational cyber security capability. Performance evidence must be demonstrated across at least two different workplace scenarios.
Knowledge evidence (KE)	Learners must demonstrate knowledge of: KE1. how emerging technologies are used in cyber attacks and cyber security KE2. approaches for identifying and assessing cyber security threats, including threat indicators and risk evaluation methods KE3. methods for implementing security measures and maintaining secure systems KE4. data protection and privacy requirements, including security controls, access management and compliance considerations KE5. incident response procedures, recovery processes and stakeholder communication approaches KE6. strategies for promoting security awareness and building organisational security culture.
Assessment conditions	Assessment must occur in conditions that reflect real or simulated workplace environments, including access to: • digital environments with relevant security systems and tools • opportunities to implement and evaluate security measures across varied workplace contexts and stakeholders • scenarios involving risk assessment, data protection, incident response, and awareness promotion • resources to support evaluation of security effectiveness, compliance and incident outcomes • assistive technologies where required to support diverse learner needs. 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.