Unit code	BSBXXX115
Unit title	Develop Intermediate Digital Cyber Security Skills
Unit outcomes	This unit describes the skills and knowledge required to apply workplace cyber security procedures in workplace contexts. Learners develop intermediate capability across five competence (C) areas: C1. Cyber security threat awareness C2. Workplace security protocols C3. Data protection C4. Incident response participation C5. Security culture contribution. No licensing, legislative or certification requirements apply to this unit at the time of publication.
Knowledge (K)	Required knowledge includes: K1. Describe common workplace cyber security threats and their potential impact on organisational operations. K2. Identify workplace security procedures and protocols used to protect digital systems, devices, and information in routine workplace contexts. K3. Describe workplace requirements for protecting sensitive information, including access controls, secure storage methods, and appropriate data handling procedures. K4. Outline workplace procedures for reporting security concerns, escalating incidents, and participating in response activities in accordance with organisational protocols. K5. Compare approaches for supporting workplace security awareness and promoting secure workplace practices.
Skills (S)	Required skills include: S1. Recognise common workplace cyber security threats and suspicious activities. S2. Apply workplace security procedures and protocols to protect digital systems, devices, and information. S3. Protect sensitive workplace information by applying access controls using secure storage methods. S4. Report security concerns and incidents through appropriate workplace channels. S5. Support workplace security awareness by sharing security knowledge with colleagues.

Application of Knowledge & Skills	At the Intermediate level, learners apply knowledge (K1-K5) and skills (S1-S5) with some autonomy across all competence areas (C1-C5) with the following characteristics: • Autonomy: With some autonomy under limited supervision, making informed decisions about cyber security approaches within established workplace frameworks and procedures. • Accountability: Accountable for quality and effectiveness of their own cyber security practices and for supporting others with routine security tasks. • Responsibility: Responsible for selecting appropriate security procedures and protocols to achieve workplace outcomes within defined parameters. • Context: Varied workplace cyber security tasks of moderate complexity, adapting approaches to different contexts while working within organisational guidelines. • Decision-Making: Make informed decisions about threat identification, security procedures and incident reporting; seek guidance when facing unfamiliar situations, ethical considerations, or requirements beyond established procedures.
Assessment Requirements	
Performance evidence (PE)	Learners must demonstrate the ability to: PE1. recognise and respond to at least two different common workplace cyber security threats using established identification procedures and response procedures PE2. apply workplace security procedures to protect digital systems, devices and information PE3. protect sensitive workplace information using appropriate access controls, secure storage methods, and data handling procedures PE4. report security concerns and incidents through appropriate workplace channels and participate in response activities PE5. support workplace security culture through security awareness activities and assistance to colleagues. Performance evidence must be demonstrated across at least two different workplace scenarios.
Knowledge evidence (KE)	Learners must demonstrate knowledge of: KE1. common workplace cyber security threats and their organisational impact KE2. workplace security procedures and protocols for protecting digital systems and information KE3. data protection requirements, including access controls, secure storage, and handling procedures

	KE4. procedures for reporting and escalating incidents and participating in incident response KE5. approaches for supporting workplace security awareness and contributing to security culture. Knowledge evidence must be demonstrated across at least two different workplace scenarios.
Assessment conditions	Assessment must be conducted in workplace or simulated environments that accurately reflect real workplace conditions, including access to: workplace digital systems and security tools commonly used in organisational contexts opportunities to recognise cyber security threats and apply security procedures across varied situations workplace-relevant scenarios requiring the application of security protocols, data protection, and incident reporting assessment methods such as direct observation, scenario-based responses, and security procedure demonstrations 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.