Unit code	BSBXXX107
Unit title	Develop Basic Digital Cyber Security Skills
Unit outcomes	This unit describes the skills and knowledge required to recognise common workplace cyber security threats and follow established workplace cyber security procedures. Learners develop capability across five competence (C) areas: C1. Cyber security threat awareness C2. Workplace security protocols C3. Data protection C4. Incident response 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. Identify common workplace cyber security threats and the potential impact of these threats on workplace systems and information. K2. Identify workplace cyber security policies and procedures for protecting digital systems and information. K3. Identify workplace security requirements for handling sensitive information securely, including data classification, secure storage, appropriate sharing, and access controls. K4. Identify workplace incident response procedures including threat reporting requirements, escalation pathways, and appropriate communication channels. K5. Identify how individual behaviours and practices contribute to workplace cyber security culture and organisational security objectives.
Skills (S)	Required skills include: S1. Use established identification methods to recognise common workplace cyber security threats. S2. Follow workplace security policies and procedures when using organisational digital systems. S3. Follow organisational data classification and protection requirements to handle workplace data securely. S4. Follow workplace channels to report cyber security threats and incidents. S5. Follow security-conscious behaviours that support workplace cyber security practices.

Application of Knowledge & Skills	At the Basic level, learners apply knowledge (K1-K5) and skills (S1-S5) across all competence areas (C1-C5) with the following characteristics: • Autonomy: Under direct guidance and supervision, following clear instructions and established workplace procedures. • Accountability: Accountable for completing assigned cyber security tasks accurately and following workplace security policies and incident reporting requirements. • Context: Straightforward, routine workplace cyber security tasks using workplace-approved security measures and established threat identification procedures within familiar workplace contexts. • Decision-Making: Make routine decisions about security practices and threat identification within established guidelines; escalate to security team when encountering security threats, suspicious activity, or situations requiring specialist cyber security expertise.
Assessment Requirements	
Performance evidence (PE)	Learners must demonstrate ability to: PE1. use workplace recognition procedures to identify at least one common workplace cyber security threat PE2. follow workplace security policies and procedures when using organisational digital systems PE3. follow organisational data protection requirements to handle workplace data securely PE4. follow appropriate workplace channels to report cyber security threats and incidents PE5. follow security-conscious behaviours that contribute to workplace cyber security culture 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 impact on organisational security KE2. workplace cyber security policies and procedures KE3. workplace requirements for handling sensitive information KE4. workplace incident reporting and escalation processes KE5. the role of individual behaviour in supporting workplace cyber security culture Knowledge evidence must be demonstrated across at least two different workplace scenarios.
Assessment conditions	Assessment must be conducted in conditions typical of a workplace or simulated environment that reflects real workplace practices, including access to: • organisational digital systems and cyber security procedures

	• workplace-relevant scenarios involving threat identification, data handling, and incident reporting • assessment methods including direct observation, scenario-based activities, and supervisor or assessor feedback • 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.