Australian Government

BSBDIG207X Develop Basic Digital Cyber Security Skills

DRAFT

Release: 1

BSBDIG207X Develop Basic Digital Cyber Security Skills

Modification History

Release	Comments
1	This unit of competency was first released in BSB Business Services Training Package Release 9.0.

Unit outcomes

This unit describes the skills and knowledge required to recognise common workplace cyber security threats and follow established workplace cyber security procedures. It applies to learners across all industries, who follow workplace cyber security procedures as part of their day-to-day work.

The primary purpose of this unit is to develop foundation and employability digital capabilities that support participation in the digital workplace and underpin further vocational training. It is delivered under direct guidance and supervision, using established workplace cyber security procedures in familiar digital environments, at a basic level.

Learners develop capability across five competence areas:

- Cyber security threat awareness
- Workplace security protocols
- Data protection
- Incident response
- Security culture contribution.

Licensing/Regulatory Information

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Knowledge

On successful completion of this unit, learners will have basic knowledge of:

- Common workplace cyber security threats and their potential impact on workplace systems and information
- Workplace cyber security policies and procedures for protecting digital systems and information
- Workplace security requirements for handling sensitive information securely: data classification, secure storage, appropriate sharing, and access controls
- Workplace incident response procedures, including threat reporting requirements, escalation pathways and appropriate communication channels

DRAFT

© Commonwealth of Australia, 2026 Future Skills Organisation

- The role of individual behaviours and practices in supporting workplace cyber security culture and organisational security objectives.

Skills

On successful completion of this unit, learners will have skills to:

- Use established identification methods to recognise common workplace cyber security threats
- Apply workplace security policies and procedures when using organisational digital systems
- Handle workplace data securely in line with organisational data classification and protection requirements
- Report cyber security threats and incidents through workplace channels
- Demonstrate security-conscious behaviours that support workplace cyber security practices.

Application of Knowledge & Skills

Learners apply their knowledge and skills under direct guidance and supervision, following established workplace cyber security procedures within familiar digital environments.

This applies to straightforward, routine workplace cyber security tasks using workplace-approved procedures and protective practices.

Learners will follow:

- Clear instructions and established workplace cyber security procedures
- Escalation processes when encountering suspicious activity, suspected security incidents, or unfamiliar threats requiring guidance.

Learners are responsible for:

- Making routine decisions about applying workplace cyber security procedures within established guidelines.

Learners are accountable for:

- Completing assigned cyber security tasks accurately, using workplace-approved cyber security procedures and protective practices within established guidelines.

Pre-requisite unit(s)

No pre-requisite units

Competency field(s)

Digital Competence

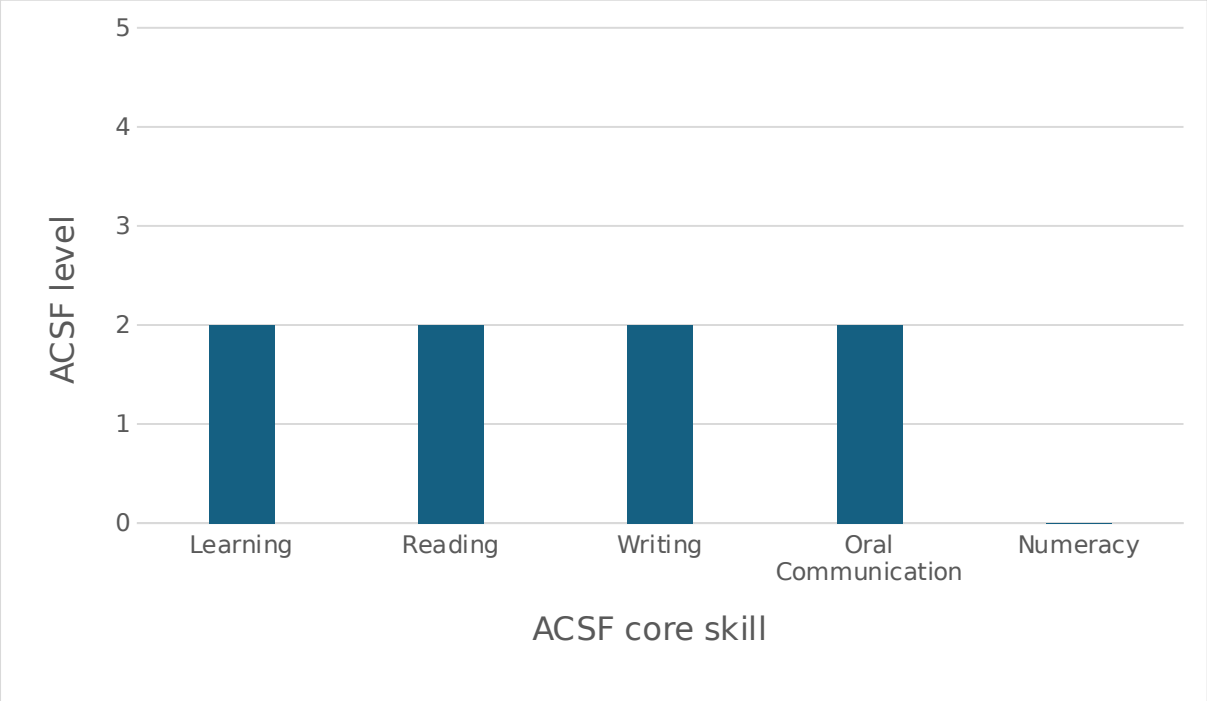
© Commonwealth of Australia, 2026 Future Skills Organisation

Unit sector(s)

Digital Capability

Foundation skills

The foundation skills in this unit are outlined below



Core Skills	ACSF Indicators and Performance Features
Learning	Applies a limited range of strategies in structured, familiar contexts. Taking responsibility for some aspects of learning in familiar contexts and using familiar scaffolding such as templates and checklists.
Reading	Identifies and interprets information in familiar texts on familiar topics. Understanding the main ideas of short, unambiguous texts and beginning to recognise bias.
Writing	Conveys meaning on familiar topics using familiar text types. At least two familiar text types, such as an email message, and factual information in notes or lists.
Oral Communication	Uses everyday language in familiar spoken contexts. Giving explanations, making enquiries and seeking clarification.
Numeracy	No ACSF level assigned.

© Commonwealth of Australia, 2026 Future Skills Organisation

Range of conditions

N/A

DRAFT

© Commonwealth of Australia, 2026 Future Skills Organisation

Assessment Requirements for BSBDIG207X Develop Basic Digital Cyber Security Skills

Performance Evidence

Learners must demonstrate ability to:

- Recognise at least two common workplace cyber security threats encountered in routine workplace tasks, with reference to their likely impact on organisational systems or information
- Complete a routine workplace task using organisational digital systems in line with workplace security policies and access controls
- Handle at least one item of sensitive workplace information in accordance with organisational data classification, storage and sharing requirements
- Report a suspected cyber security threat or incident through the correct workplace channel, using appropriate communication and escalation pathways
- Describe, using a workplace example, how individual practices and behaviours contribute to the organisation's cyber security culture.

Knowledge Evidence

Learners must demonstrate basic knowledge of:

- Common workplace cyber security threats and their potential impact on workplace systems and information
- Workplace cyber security policies and procedures, including their role in protecting digital systems and information
- The classification, storage, sharing and access control requirements for handling sensitive workplace information
- Workplace incident response procedures, including reporting requirements, escalation pathways and communication channels
- Individual behaviours and practices that contribute to workplace cyber security culture and organisational security objectives.

Assessment Conditions

N/A

Mandatory Workplace Requirements

Assessment of performance evidence may be in a workplace setting or an environment that accurately represents a real workplace.

Unit Mapping Information

Previous Code and Title	Equivalence	Comments

DRAFT

© Commonwealth of Australia, 2026 Future Skills Organisation

	Newly created	This unit has been created to address a skill or task required by industry that is not covered by an existing unit of competency

Links

Companion volumes, including implementation guides, are found on the national training register - https://training.gov.au/training/details/BSB.

DRAFT

© Commonwealth of Australia, 2026 Future Skills Organisation