BSB 7.0

BSBXCS303

SECURELY MANAGE PERSONALLY IDENTIFIABLE INFORMATION & WORKPLACE INFORMATION

Aspire Learning Resources

BSBXCS303

Securely manage personally identifiable information and workplace information

Release 1

Learner Guide

Aspire Version 1.1

Aspire
Learning Resources

Aspire also has learning resources available in these areas:

- Foundation skills
- LLN and employability skills (non-competency)
- Community services
- Early Childhood Education and Care
- Allied health

Aspire is committed to developing quality resources that meet the needs of our customers. However, occasionally Aspire finds, or is notified of, errors. Please refer to our website at www.aspirelr.com.au to see if there are any updates that may be relevant to you.

Every effort has been made to ensure the information in this book is accurate; however, the author and publisher accept no responsibility for any loss, damage or injury arising from such information.

Except where an information source is acknowledged, the names and details of individuals and organisations used in examples are fictitious and have been devised for learning purposes only. Any similarity to actual people or organisations is unintentional.

All websites referred to in this unit were accessed and deemed appropriate at time of publication.

Aspire Training & Consulting apologises unreservedly for any copyright infringement that may have occurred and invites copyright owners to contact Aspire so any violation may be rectified.

Acknowledgement

Aspire Learning Resources wishes to acknowledge Hivint for providing an industry validation review of this Learner Guide. Hivint is a cybersecurity consultancy with offices in Melbourne, Sydney, Perth and Brisbane that provides leading edge security advisory and assurance services. We are grateful for their contribution.

BSBXCS303 Securely manage personally identifiable information and workplace information, Release 1

Level 1, 464 St Kilda Road
MELBOURNE VIC 3004 AUSTRALIA
Phone: (03) 9820 1300

First published December 2020

Cover design: Anne-Marie Reeves Design
Printer: Doculink Australia Pty Ltd, 1d/28 Rogers Street, Port Melbourne VIC 3207

e-ISBN 978-1-76075-975-9 (PDF version)
ISBN 978-1-76075-974-2

Contact details

Participant
Name:
Start date:
Phone number:
Email:
Work location
Name:
Address:
Postal address:
Workplace supervisor name:
Phone number:
Fax:
Email:
Registered Training Organisation (RTO)
Name:
Address:
Postal address (if different):
Phone number:
Fax:
RTO contact name:
Mobile:
Email:

CONTENTS

Before you begin

This Learner Guide is based on the unit of competency *BSBXCS303 Securely manage personally identifiable information and workplace information*, Release 1. Your trainer or training organisation must give you information about this unit of competency as part of your training program. You can access the unit of competency and assessment requirements at: www.training.gov.au.

How to work through this Learner Guide

This Learner Guide contains a number of features that will assist you in your learning. Your trainer will advise which parts of the Learner Guide you need to read, and which Practice Tasks and Learning Checkpoints you need to complete. The features of this Learner Guide are detailed in the following table.

Feature of the Learner Guide	How you can use each feature
Learning content	Read each topic in this Learner Guide. If you come across content that is confusing, make a note and discuss it with your trainer. Your trainer is in the best position to offer assistance. It is very important that you take on some of the responsibility for the learning you will undertake.
Examples	These highlight key learning points and provide realistic examples of workplace situations.
Practice Tasks	Practice Tasks give you the opportunity to put your skills and knowledge into action. Your trainer will tell you which practice tasks to complete.
Summaries	Key learning points are provided at the end of each topic.
Learning Checkpoints	There is a Learning Checkpoint at the end of each topic. Your trainer will tell you which Learning Checkpoints to complete. These checkpoints give you an opportunity to check your progress and apply the skills and knowledge you have learnt.

Foundation skills

As you complete learning using this guide, you will be developing the foundation skills relevant for this unit. Foundation skills are the language, literacy and numeracy (LLN) skills and the employability skills required for participation in modern workplaces and contemporary life.

The following table provides definitions for each foundation skill.

Foundation skill area	Foundation skill description
Learning	▪ Modifies behaviour following exposure to new information
Numeracy	▪ Interprets mathematical data
Oral communication	▪ Asks open and closed probing questions and actively listens to clarify consultations
Reading	▪ Recognises and interprets information from relevant sources to determine organisational expectations and legal requirements
Planning and organising	▪ Efficiently and logically sequence the stages of data management
Technology	▪ Uses appropriate technology platforms to assist with data storage, data retrieval and data management

What do you already know?

Use the following table to identify what you may already know. This may assist you to work out what to focus on in your learning.

Topic	Key outcome	Rate your confidence in each section
Topic 1: Handle sensitive information responsibly	1A Review sensitive information standards, practices and procedures	❑ Confident ❑ Basic understanding ❑ Not confident
	1B Identify and classify sensitive information	❑ Confident ❑ Basic understanding ❑ Not confident
	1C Apply privacy policies to data devices	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 2: Store and share sensitive information	2A Organise and confirm accuracy of data	❑ Confident ❑ Basic understanding ❑ Not confident
	2B Implement access protocols	❑ Confident ❑ Basic understanding ❑ Not confident
	2C Identify and report infrastructure malfunctions and attacks	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 3: Apply information protection protocols	3A Conduct data back-ups	❑ Confident ❑ Basic understanding ❑ Not confident
	3B Conduct privacy impact assessments	❑ Confident ❑ Basic understanding ❑ Not confident
	3C Confirm adherence to data protection standards	❑ Confident ❑ Basic understanding ❑ Not confident

Topic 1 | Handle sensitive information responsibly

1A Review sensitive information standards, practices and procedures

1B Identify and classify sensitive information

1C Apply privacy policies to data devices

1A Review sensitive information standards, practices and procedures

Sensitive information in the workplace must be handled in line with relevant standards, practices and procedures.

This unit is about securely managing sensitive information, such as personally identifiable information and workplace information. The management-sensitive information is controlled by both legislative requirements and workplace policies and procedures.

Legislative requirements

You need to comply with the law when working with sensitive information.

Legislation regarding sensitive information exists at Australian state, Australian Commonwealth, and international levels. You will generally need to comply with requirements at all three levels, specifically to the ones relating to the geographical location of the individual or of the business operation.

Australian Commonwealth requirements

The Privacy Act

The *Privacy Act 1988* (Cth) is the most important piece of federal legislation relating to the management of personal information. The Privacy Act includes requirements around the:

- collection of personal information
- use of personal information
- storage of personal information
- disclosure of personal information.

The Privacy Act applies to:

- Australian Government agencies
- private organisations (e.g. companies) with an annual turnover more than $3 million.
- The Privacy Act generally does not apply to:
- state and territory government agencies
- small businesses with a turnover less than $3 million*

*NOTE: Some small businesses are covered by the Privacy Act. Please check the following link for full details of the types of businesses that are covered and not covered: aspirelr.link/oaic-privacy-act

Australian Privacy Principles (APPs)

The Commonwealth Privacy Act provides 13 Australian Privacy Principles (APPs). These principles apply to all organisations that have responsibilities under the Privacy Act. The APPs relate to all stages of handling personal information (i.e. collecting, using, storing and disclosing information).

For a helpful summary of the 13 APPs, download the information poster from the Australian Government Office of the Australian Information Commissioner (OAIC) website: aspirelr.link/oaic-privacy-principles

Notifiable Data Breach (NDB) scheme

The Notifiable Data Breach (NDB) scheme commenced in 2018 and applies to organisations that have responsibilities under the Privacy Act. Under the NDB, organisations must report data breaches to both the individuals whose data is affected by the breach and the OAIC.

A data breach occurs when personal information is:

- accessed or disclosed without authorisation
- lost.

Data breaches can be generally categorised in the following areas:

- a device with an individual's personal information is lost or stolen (e.g. a credit card theft)
- a database with personal information is accessed without authorisation
- personal information is mistakenly given to a wrong party.

We will look at what types of information are classified as 'personal information' shortly.

Implications of the NDB scheme on an organisation

Failure to comply with NDB laws can incur penalties for organisations.

Non-compliance could mean serious fines, for example:

- companies face a fine of up to $1.8 million
- individuals face a fine of up to $360,000.

The NDB scheme means that organisations and individuals need to take proactive steps when dealing with personal information.

Australian state and territory requirements

Commonwealth laws and state/territory laws have many similarities. However, there are differences specific to each state and territory. It is important to identify and adhere to the legislation applicable to the location in which your organisation operates. When state/territory and Commonwealth laws are in conflict, the overarching Commonwealth law prevails.

Here is a list of privacy legislation in each state and territory.

ACT	*Information Privacy Act 2014* (ACT)
NSW	*Privacy and Personal Information Protection Act 1998* (NSW)
NT	*Information Act 2002* (NT)
QLD	*Information Privacy Act 2009* (Qld)
SA	None, SA refers to the *Privacy Act 1988* (Cth)
TAS	*Personal Information and Protection Act 2004* (Tas)
VIC	*Privacy and Data Protection Act 2014* (Vic)
WA	*Freedom of Information Act 1992* (WA)

International requirements

In today's global world, you also need to be aware of international data protection laws.

On 25 May 2018, the European Union (EU) enacted the General Data Protection Regulation (GDPR). This is designed to protect the personal data of EU citizens and residents by increasing the obligations of organisations that collect and process data.

The GDPR offers EU citizens more rights over:

- who has access to their data
- where and how their data is stored and used
- having their personal information removed or deleted from databases.

There are large fines associated for organisations that breach the GDPR, even if they are not located in the EU.

Australian organisations and the GDPR

Australian organisations need to comply with the GDPR if they;

- have a presence in the EU
- offer goods or services in the EU
- monitor and process data relating to EU citizens and residents.

This regulation is far reaching and overlaps with the NDB scheme. Both promote the confidentiality of identifiable data on individuals, and the unauthorised sharing of individual data would be in breach of both the GDPR and the NDB laws.

Organisational policies and procedures

Organisations use policies and procedures to protect sensitive information.

All organisations covered by the Commonwealth Privacy Act are required to have a privacy policy.

Organisations generally make their privacy policy publicly available on their website in order to meet the APPs (specifically APP 1, which relates to the open and transparent management of personal information.)

In addition to meeting APP requirements, the purpose of a privacy policy is to outline how personal information gathered from customers (and potential customers) will be managed. There is no template for a privacy policy, and it should reflect the specific operations of the organisation. However, the following information is usually contained in a privacy policy.

Information commonly included in a privacy policy:

- What types of personal information are collected by the organisation
- How this information is collected and stored
- The purposes for collecting, holding, using and disclosing personal information
- Instructions for a person seeking to access or correct any personal information held by the organisation
- Instructions for a person seeking to complain about a breach of the APPs and how this complaint will be dealt with
- Information about whether any personal information will be disclosed by the organisation to overseas recipients (and, if so, the countries in which these recipients are located)

A privacy policy should not be written in complex legal language. It should be written in a simple manner that can be understood by any individual who interacts with the organisation.

While you may not be involved in writing or maintaining your organisation's privacy policy, you do need to know how it applies to any interactions you have with personal information.

Confidentiality agreement

Organisations generally require employees to sign a confidentiality agreement at the start of their employment period. This agreement is also sometimes referred to as a non-disclosure agreement. This is a legally binding document that usually includes the following information.

Information commonly included in a confidentiality agreement:

- The names of the parties to the agreement (typically the employer and the employee)
- Commencement date and duration of the agreement
- Details of the types of information that are to be treated as 'confidential' for the duration of the agreement (examples of information that is usually required to be kept confidential will be looked at shortly)
- Details of the types of information that are *not* to be treated as 'confidential' for the duration of the agreement (examples of information that is usually not required to be kept confidential will be looked at shortly)
- What will happen if the employee makes unauthorised disclosures of confidential information
- Ownership details of confidential information
- Governing law relating to the agreement (e.g. relevant state or territory law)

When handling workplace information, you need to remember your obligations under the confidentiality agreement. A confidentiality agreement should be read carefully at the commencement of employment to ensure all obligations are clearly understood.

Example

Review sensitive information standards, practices and procedures

Louise recently started employment as a developer at GardenMart, an online gardening supplies store based in Sydney with an annual turnover of $10 million. Based on the size and location of GardenMart, Louise is aware the organisation needs to comply with the Commonwealth Privacy Act, the New South Wales Privacy and Personal Information Protection Act, and international GDPR laws. As an organisation with responsibilities under the Commonwealth Privacy Act, GardenMart has a privacy policy that is publicly available on its website. By reviewing this in detail, Louise understands that GardenMart gathers and holds customer data. GardenMart commits to not disclosing this data to other third parties, and customers are able to access their data by contacting the company's help desk.

When starting work for the organisation, Louise was required to sign a confidentiality agreement. The confidentiality agreement specifies that Louise must not disclose any information regarding GardenMart's finances, intellectual property or customer data. If Louise breaches any of this confidential information, she may face disciplinary and legal action.

Practice Task 1

Question 1

Draw a line to match each term– regarding sensitive information management standard to its correct definition.

» *Privacy Act 1988*	» Requires organisations whose data is compromised to contact the affected individuals as well as relevant Australian authorities
» General Data Protection Regulation (GDPR)	» Commonwealth legislation that applies to all federal bodies and private sector organisations with annual revenue above $3 million
» Notifiable Data Breach (NDB) scheme	» Developed by organisations to inform their customers about how their personal information will be handled
» Privacy policy	» International requirements relating to the handling of personal information

Question 2

Which of the following are found in an organisation's privacy policy? Tick all that apply.

- ◯ How long it has been since the organisation last had a data breach
- ◯ How an individual can access or correct any information held by the organisation
- ◯ What types of personal information are collected by the organisation
- ◯ How personal information is stored by the organisation
- ◯ What types of servers are used to store customer information

1B Identify and classify sensitive information

Knowing how to identify and classify the sensitive information you deal with in your work will help you to handle it correctly.

Regardless of what type of job you do, you deal with a lot of information every day. Every email you receive, every conversation you have and every document you look at contains information. Some of this information is sensitive and some of it isn't. The way you use and handle the sensitive information is governed by the different types of legislation and workplace policies we looked at previously. If you don't know how to identify the sensitive information, you may accidentally handle it incorrectly, which could have legal consequences. So it's important that you know how to tell the difference between sensitive and non-sensitive information.

We can classify sensitive information as either personally identifiable information or workplace information.

Personally identifiable information

Personally identifiable information is any information that can be used to identify a specific person.

A large focus of the Australian and international legislation we looked at earlier relates to how personally identifiable information (PII) is managed by organisations. If PII gets into the wrong hands (e.g. as the result of a data breach), the consequences can be huge. Examples of how PII in the wrong hands can be used include:

- making fraudulent credit card purchases
- creating bank accounts and taking out loans
- conducting criminal acts in an innocent person's name.

If a person's PII is compromised, it can take many years for them to recover complete control of their identity. This is why it's so important to know how to identify PII and take the appropriate steps to protect it.

PII can generally be classified as either 'linked' or 'linkable'. These terms are similar, so let's take a look at what the difference is.

Linked information

Linked information is any data that can be used to directly identify a person. The following table outlines some common examples of linked information.

Common examples of linked information:

- Full name (given name plus family name)
- Date of birth
- Home address
- Email address
- Telephone number
- Tax file number (TFN)
- Passport number
- Driver's licence details
- Credit card details
- Login details (username and password) for websites
- Credit information
- Health information
- Criminal record

Other linked information may be relevant in specific contexts. For example, a customer's purchase history with a particular online store would be considered linked information. An individual's posts on social media would also be considered linked information.

Linkable information

Linkable information is usually less specific than linked information. On its own, a piece of linkable information may not be able to identify a specific person. However, when used with other information, linkable information may enable a specific person to be identified. For example, combining several of the pieces of linkable information provided in the following table could enable a specific person to be identified.

Common examples of linkable information:

- Common given names (e.g. John or Sarah)
- Common family names (e.g. Smith or Jones)
- Gender
- Race
- Age range (e.g. 18–25)
- Job position

Even though linkable information on its own may not be 'about' an individual, it is generally recommended to err on the side of caution when handling this.

Workplace information

In addition to personal information relating to customers, you are likely to encounter workplace information that must also be handled sensitively.

Much of what we have looked at so far has related to sensitive data and the personal information of individuals, such as the customers of an organisation. However, in your day-to-day work, you are also likely to be dealing with information that does not relate to customers, but must also be handled carefully. The confidentiality of this workplace information will often be outlined in a confidentiality agreement.

Common types of sensitive workplace information

The specific types of workplace information that need to be handled sensitively will vary from workplace to workplace. The following table outlines some of the common areas requiring sensitivity:

Customer and supplier information	Current customers and suppliers of the business, including details about services provided, size of contract, number and type of goods provided, etc.
Intellectual property	Trade secrets held by the organisation; this could include (but is not limited to) development methods, technology innovations, research findings, etc.
Operational information	Information about how work is performed in the organisation (e.g. internal policies and procedures)
Accounting information	Internal financial data, including financial statements, balance sheets, current debts and liabilities, payroll information, etc.
Product/production information	Internal specifications for products created by the organisation, including methods of production and manufacturing
Computing technology and code	Computing technology, code and processes used by the organisation to create and deliver its products and services

Classifying workplace information

Not all workplace information is necessarily sensitive. The following table identifies four levels of classification for workplace information.

Public

Workplace information that can be freely shared inside and outside your organisation

Examples include:

- marketing materials
- contact information details for sales representatives
- price lists for retail products.

Internal

Workplace information that is potentially sensitive and should not be shared outside the organisation

Examples include:

- organisational charts
- unfinished documents.

Confidential

Workplace information that is sensitive and could negatively affect the organisation's operations if compromised

Examples include:

- contracts with suppliers
- salary details for each member of staff.

Restricted

Workplace information that is extremely sensitive; if this information is compromised, it could put the organisation at financial or legal risk

Examples include:

- customer information such as credit card details
- intellectual property.

Labelling relevant documents and information with the correct classification will help to ensure that the information is handled correctly. For example, before sending an email, consider the classification of the subject being discussed. If the information is confidential or restricted, you need to ask yourself:

- Is email the best way to transmit this information (bearing in mind that you will have no control of the email after you hit the 'send' button)?
- Have you indicated that the content of the email is confidential or restricted?
- Have you taken any other steps to protect the information (e.g. by using password protection)?

We will look at protocols for controlling sensitive data in more detail in Topic 2.

Example

Identify and classify sensitive information

Charlie works in the sales department at PetWorld, an online retailer of pet food and accessories. Every order which is received contains the following information:

- customer name
- customer email address
- customer shipping address
- products ordered
- type of pet.

Charlie recognises that, with the exception of the 'type of pet' information, all of this data can be classified as 'linked' PII.

Charlie has been involved in finalising a large contract with a wholesale supplier – all communications regarding this important contract are labelled 'confidential'. Charlie is aware that this means he cannot share any information regarding the contract outside the organisation

Practice Task 2

Question 1

Draw a line to match each classification label to the relevant type of workplace document.

» Internal	» Documents that can be freely shared outside the business
» Restricted	» Documents that are potentially sensitive and should not be shared outside the business
» Public	» Documents that are sensitive and could negatively affect business operations if shared outside the business
» Confidential	» Documents that are extremely sensitive and could lead to financial or legal risk if compromised

Question 2

List three types of 'linked' personally identifiable information.

1C Apply privacy policies to data devices

Many businesses and organisations are required to have a privacy policy. You need to know how this policy relates to the devices you use to store sensitive data.

We introduced the concept of privacy policies earlier in this Topic. All businesses with an annual revenue higher than $3 million are required to have a privacy policy. A number of smaller businesses (with annual revenues lower than $3 million) are also required to have a privacy policy.

While the privacy policy is generally made publicly available to an organisation's customers, as an employee you also need to know what the requirements of this policy are. Specifically, you might recall that one of the key sections in a privacy policy relates to how a company stores its customers' data on its data devices.

Data devices

Depending on your workplace, you may be required to store data on one or more devices.

Data devices are any devices or infrastructure that can be used to store data. The following table outlines some common types of data devices.

Hard disk drive
Also known as a 'hard drive', 'HD' or 'HDD', these can be found in most desktop and laptop computers. They are also used for servers and mainframes. They can hold large amounts of data.
USB memory sticks
USB memory sticks, or flash drives, are small portable devices that can be plugged into the USB port of a computer and used to transfer data. They generally hold much less data than a hard disk drive.
Solid state drive (SSD)
Solid state drives are faster and smaller than traditional hard disk drives. This is why they are used in portable devices such as smart phones.

Cloud storage

While not a 'device' per se, cloud storage should be considered here as it is a common way in which client information may be stored. Cloud storage involves a network of remote (i.e. external to the organisation) servers that are used to house data.

Steps and strategies for applying privacy policies

Organisations required to have a privacy policy are also required to comply with the APPs. The APPs provide steps and strategies for ensuring security of personal information.

We introduced the APPs earlier in this Topic. All organisations that have responsibilities under the Commonwealth Privacy Act must also adhere to the 13 APPs. If you work at an organisation that is not legally required to comply with the APPs, they are still an excellent source of information about best practices in data security.

Specifically, APP 11 provides guidance about how to use data devices to ensure that they securely manage personal information. The OAIC has published a detailed guide on APP 11, including steps and strategies to take in order to protect personal information.

A summary of how these steps and strategies relate to data devices is provided in the table below, but you may like to check out the full guide here as it goes into a lot more detail: aspirelr.link/oaic-steps

Governance, culture and training

The importance of personal information security needs to be understood across an entire organisation, not just in the ICT part of the business. You also need to be aware of correct practices when handling PII using data devices, and this may require your receiving training.

Questions you should ask include the following:

- Have I and other staff received training in how to use data devices for managing PII?
- Does this training include areas such as:
  - not accessing PII unnecessarily
  - proper use of passwords
  - how to recognise and avoid attacks on sensitive data (e.g. phishing)
  - whether and how personal devices can be used for work?

Internal practices, procedures and systems

Your organisation should have practices, procedures and systems in place relating to the security of PII.

Questions you should ask include the following:

- Do I know where and how to access relevant practices, procedures and systems?
- How do these relate to the devices used for managing sensitive data?

ICT security

ICT security is required to protect data devices from misuse, interference, unauthorised access, loss and modification; for example:

- malicious software such as malware and devices
- human error
- hardware or software failure
- system failures caused by power outages (including failures caused by natural disasters).

ICT security also enables these devices to remain accessible and usable for authorised persons.

Questions you should ask include the following:

- What security software is being used to protect data devices? Does it need to be upgraded?
- Are external files scanned for issues before they are opened locally?
- What data-encryption methods are used on data devices? Are these reviewed regularly?
- What sorts of firewalls are used and how have they been configured?
- Are any systems in place to prevent email systems from attacks?
- Is whitelisting or blacklisting used to manage the types of users that can access data devices?
- How often is the system tested? And what does this involve?
- How often are data devices backed up?
- Are there policies in place to prevent PII being transmitted via unsecured email?

Access security

Access security enables the security of data devices to be limited to only those parties considered to be 'authorised persons'.

Questions you should ask include the following:

- Is access to personal information stored on data devices limited to only those staff who need to access it?
- Is access to data devices cancelled when it is no longer required?
- What methods are used to authenticate 'authorised persons' accessing data devices?
- Is password complexity enforced?
- How is unauthorised access of data devices monitored? And how are alerts given?

Data breaches

An organisation's requirements under the NDB scheme were discussed earlier in this Topic.

Questions you should ask include the following:

- Does your organisation's data breach response plan include breaches of data devices?
- Do you know where the plan is stored and how it will be used in the event of a breach?

Physical security

While the focus of security often relates to hacks occurring over the internet, the physical security of data devices must also be considered.

Questions you should ask include the following:

- What security measures are in place relating to the access of physical data devices?
- Are work areas that regularly require access to sensitive information physically separate from other parts of the business?
- Are computers positioned so that sensitive information cannot be easily seen by others in the area?

Data destruction

When an organisation holds personal information that it is not permitted to hold under the APPs, it must take steps to destroy (i.e. delete) or de-identify the information.

Questions you should ask include the following:

- Is there a procedure for destroying or de-identifying data?
- Has any hardware containing personal data been properly sanitised (e.g. have any copies of the file in 'trash' or 'recycle bins' been securely deleted)?
- If the data has been stored on third party hardware (such as cloud storage), have steps been taken to confirm the third party has destroyed or de-identified the data?
- Have any digital backups of the data been destroyed?
- Have any records or physical media containing the data (e.g. printouts, CDs and DVDs) been destroyed?

The questions identified in the above table can be used as the starting point for a checklist you can create to confirm that your organisation is adhering to its privacy policy requirements. Refer back to the guide on the OAIC website to ensure that your checklist covers all the requirements.

If any aspects of the organisation's data devices do not comply with its privacy policy, you should discuss these with your manager. Use open- and closed-ended questions to confirm the actions required to achieve compliance.

Example

Apply privacy policies to data devices

Andia has recently started working in the IT department of Gremlin Games, a software company that sells games direct to consumers. Andia confirms that customer data is currently stored on a hard drive server in the Gremlin Games head office. Although the company has a privacy policy, nobody has checked that it is actually being applied. Andia develops a checklist based on the steps and strategies for APP 11. By using the checklist, she identifies a number of security issues that she raises with her manager.

Practice Task 3

Question 1

What are three questions you should ask when checking if a data device adheres to your organisation's privacy policy? Tick all that apply.

- ◯ What firewalls are in place to protect customer data?
- ◯ Is customer data being stored as cheaply as possible?
- ◯ How can I enable all staff to have access to customer data?
- ◯ What security is in place to protect physical data devices?
- ◯ What methods are used to authenticate the users who access customer data?

Question 2

Identify two types of data device for storing sensitive data in the workplace.

Question 3

What data must an organisation take steps to destroy or de-identify? Write your response in one sentence.

Summary

- You will generally need to comply with requirements at state/territory, national and international levels when handling sensitive information.
- The *Privacy Act 1988* (Cth) is the most important piece of federal legislation relating to the management of personal information.
- The Notifiable Data Breach (NDB) scheme means that organisations must report data breaches to both the individuals whose data is affected by the breach and the Office of the Australian Information Commissioner (OAIC).
- The main international requirement you need to be aware of is the General Data Protection Regulation (GDPR).
- Privacy policies and confidentiality agreements are the main forms of documentation relating to the management of sensitive information used by organisations.
- Sensitive information can be classified as either personally identifiable information (PII) or workplace information.
- PII is any information that can be used to identify a specific person.
- Workplace information can be classified as public, internal, confidential or restricted.
- Different data devices used for managing sensitive information include hard disk drives, USB memory sticks, solid state drives and cloud storage.
- The Australian Privacy Principles (APPs) can be used as a guide when applying a privacy policy to data devices in an organisation.

Learning Checkpoint 1

Handle sensitive information responsibly

Part A

1. What are two Commonwealth Government requirements relating to personally identifiable information that organisations with annual revenue above $3 million must be aware of?

2. If company's customer data is breached, who does the company need to notify under the Notifiable Data Breach scheme? Tick all that apply.

   - ◯ All the company's customers
   - ◯ Customers whose data was breached
   - ◯ Company shareholders
   - ◯ The police force in the company's state
   - ◯ Office of the Australian Information Commissioner (OAIC)

3. What is the main form of international legislation that Australian organisations should be aware of when operating online?

Part B

Read the case study and answer the questions that follow.

Case study

Cassie works at a firm called TaxSmart that helps customers to create and lodge their tax returns online. One morning, Cassie receives a link to a spreadsheet in a network folder available to all staff. The spreadsheet contains a large amount of data under columns with the following headings:

- FullName
- Username
- Password
- EmailAddress
- CreditCardNumber
- CreditCardExpiry

1. What would be the most appropriate classification for this data? Tick all that apply.

   - ◯ Unlinked PII
   - ◯ Linked PII
   - ◯ Intellectual property
   - ◯ Linkable PII
   - ◯ Public workplace information

2. What are three questions Cassie could ask to check whether this data has been stored according to TaxSmart's privacy policy? Tick all that apply.

   - ◯ What systems are in place to limit unauthorised access to this data?
   - ◯ Has the data been protected by a password?
   - ◯ How can the data be made available to all customers?
   - ◯ How can the data be accessed on staff members' personal devices?
   - ◯ Is there a procedure for destroying or de-identifying data that can no longer be held?

3. Go to the following website to find out whether any of your own PII been compromised. Summarise what you find out: aspirelr.link/have-i-been-pwned

4. Look up the privacy policies for two different Australian organisations. What types of details do they contain?

Topic 2 | Store and share sensitive information

2A Organise and confirm accuracy of data

2B Implement access protocols

2C Identify and report infrastructure malfunctions and attacks

2A Organise and confirm accuracy of data

In order to be useful to an organisation, data must be both well-organised and accurate.

Organisations are required to be very careful in handling data. But if data is poorly organised and inaccurate, even the best security won't make it useful to the organisation. Without careful management, data can quickly become disorganised and inaccurate. So it's important to take action to make sure data is easy to find and high quality.

Organising data

Organising files correctly will help you and your colleagues access the files you need, when you need them.

Have you ever forgotten where you saved a file? What about not being able to find what you want in a folder filled with hundreds of files? This might not be a big problem if it relates to your personal study assignments, but it becomes a huge issue when dealing with sensitive information in a workplace. Naming your files correctly and organising them using a logical folder structure will ensure they can be accessed when required.

Naming files

The first step in organising your information is to ensure you follow good file-naming conventions. If your organisation has its own file-naming convention, you should follow it. Otherwise, the following table includes some good practices for naming files.

File-naming conventions:

- Be consistent in your file naming. For example, if previous spreadsheets containing monthly sales data start with the term 'SalesData', don't save new spreadsheets using the term 'MonthlySales'.
- Use file names that are meaningful to both you and your co-workers. A document named 'Draft Document 1' has less meaning than 'SalesData_March2020_Draft'.
- Use names that will enable you to find your files quickly. This could include using the date as the first part of the file name, in the format 'YYYY-MM-DD'. This will make it easy to organise your files in date order.
- Agree on what vocabulary is to be used in file names. For example, it may be agreed that the term 'sales' is used in file names instead of 'goods sold', 'income' or 'revenue'.
- Agree on conventions for what punctuation can be used (if any). This includes the use of capital letters, spaces, underscores and hyphens. Some punctuation such as slashes (/) and full stops (.) should be avoided in all file names as they can cause errors.
- Include versioning information in the file name, using the organisation's versioning rules; for example, 'MonthlySalesReport_V01'.
- Avoid long names (longer than 25 characters).

Creating a logical folder structure

Using a logical folder structure will make it easier to find the files you need. Your organisation may already have an established folder structure, in which case you should follow that. Every organisation is different, so there isn't a single correct structure that will be used by every organisation.

However, if it seems like files are difficult to find in your organisation, consider whether the following conventions are being followed.

Group files into folders	If all your files are in a single folder, then finding an individual file is going to be difficult. Consider how files can be grouped, and create multiple folders to enable this. For example, if you have a folder containing a lot of files relating to different business areas (e.g. Sales, HR, Marketing, etc.), consider creating a folder for each business area.
Use sub-folders	Sub-folders enable you to create a structure or hierarchy for your files, and group them in even more detail. If you have a single folder called 'Sales', you might create sub-folders for different activities relating to sales (e.g. 'Wholesale' and 'Retail', or according to different product categories). There will be many different ways you can organise your folder structure. Drawing your planned folder structure on a piece of paper before you begin might help you identify the best approach to use.

Name folders appropriately and consistently	The conventions identified for naming files (see above) are also relevant to how you name your folders. The names you use for each folder should: ▪ be consistent ▪ be meaningful ▪ use agreed vocabulary ▪ avoid long names.
Use separate folders for work in progress and completed work	When you're looking for a file you're working on, you don't want to have to navigate through every document you've ever worked on. Creating a separate folder (or folders) for work you've completed will make your life easier, while also ensuring you can access completed work when required.
Use separate folders for previous versions	When you develop complex documents (especially in collaboration with others), you're likely to create multiple versions. While version names should be included in the document file name, it is also good practice to keep old versions in a separate folder. This will help to avoid people mistakenly reading or working on superseded versions of a document.

When creating or using a folder structure, ask the question: 'Who should have access to each of these folders?' If you're using a folder to store sensitive data, you need to use appropriate access protocols to prevent the information from being accessed by unauthorised persons. Access protocols will be covered shortly.

Confirming data quality

Quality data is accurate, up-to-date and comprehensive.

Data collected by an organisation often forms one of the starting points from which strategic decisions are made. The sales data collected by a company might indicate:

- the popularity of particular products or product categories, which can help predict where manufacturing efforts should occur
- the location or gender of customers, which can help indicate which marketing strategies used by the organisation are successful.

However, for data to be used in this way, it needs to be high quality. Poor-quality data is likely to result in poor quality decision-making – you may have heard this referred to as 'garbage in – garbage out'.

High-quality data is accurate, up-to-date and comprehensive. The following table identifies some strategies you can use to confirm the quality of your data.

Checking the data is accurate

Data inaccuracies are often the result of human error. Methods to check the accuracy of data include the following:

- Use the 'Check for duplicates' feature in the spreadsheet software you use to find repeated data.
- Use data-validation tools in your spreadsheet software to highlight data that is unlikely to be correct. For example, you could validate a column containing data on the age of customers to highlight any entries higher than 100. If a column is meant to contain a digit, you could also perform a validation to confirm that no entries contain text.
- Cross-check your data against other data sources. This may include spot checks of individual data entries against the original data source.
- Check that any data totals (e.g. yearly sales) are the sum of the individual entries (e.g. monthly sales for that year).
- If the data you're looking at doesn't make sense but you can't figure out why, check with an authorised colleague to make sure you haven't overlooked anything. Two sets of eyes are usually better than one.

Checking the data is up-to-date

You generally want to make sure you're working with up-to-date data (although in some situations, you may need to access historic data). To check if your data is up-to-date, consider the following:

- Data files exported from a database will often include the date and time of export in the file name and within the file itself. Check these dates are current.
- Data records will often include time or date information that can be used to help identify if the data is up-to-date. For example, web traffic data for the month of June should include logs with dates in June.
- As with data accuracy, cross-checking your data against other data sources can help to confirm if you're looking at data that's up-to-date.

Checking the data is comprehensive

Data that is 'comprehensive' contains all the required information (e.g. customers' names and date of birth may be required fields). Datasets will sometimes contain 'optional' fields (e.g. customers' personal interests) that do not need to be completed.

Required information may be missing from your data due to human error or a technical glitch. To check for comprehensiveness:

- use data validation tools in your spreadsheet software to check for blank fields
- if blank fields do exist, cross-check against other data sources (e.g. a source database), as these may contain the missing data.

Example

Organise and confirm accuracy of data

Ricki works in the IT department of Sweetwater, a financial services company with 180 employees. Ricki has been asked to assist the HR team due to concerns around the security of the company's personnel records. Ricki soon learns that:

- all staff records are stored in a single folder named 'STAFF' with no sub-folders or structure/hierarchy
- the folder contains multiple outdated personnel files for each staff member, which do not follow a consistent naming pattern (some files are named according to the employee's name; others according to the employee's staff ID number).

Ricki works with the HR team to create a logical folder structure that is arranged according to the different departments in the organisation. He also helps the team establish naming conventions for files, which will be based on the staff ID number.

Ricki also checks a spreadsheet file that is meant to contain the details of all current employees at Sweetwater, including their birthdays and annual leave entitlements. He discovers:

- some required fields (such as 'Surname') are empty
- the spreadsheet contains 210 rows, significantly more than the 180 current members of staff; this is due to some rows being duplicated
- the spreadsheet contains the names of some old employees and is missing the names of some new employees.

Practice Task 4

Question 1

Which of the following are good practices when naming files? Tick all that apply.

- ◯ Use file names longer than 25 characters.
- ◯ Avoid using slashes and full stops.
- ◯ Include versioning information.
- ◯ Use naming consistent with similar types of files.
- ◯ Include the author's name.

Question 2

List two ways you could check if the data you're looking at is accurate.

2B Implement access protocols

Access protocols protect sensitive data from falling into the wrong hands.

'Access protocols' are the rules used to control how data is accessed. Without access protocols in place, all data in an organisation could be accessed by anyone inside or outside the workplace. Such protocols therefore limit the ability of people to access sensitive data if they don't have permission to do so.

Strategies for implementing access protocols

Protecting sensitive data requires a number of access protocols to be implemented.

When it comes to controlling and protecting access to sensitive data, there are numerous strategies that can be used. A combination of these strategies is required in order to be successful. Consider each of the following strategies as a wall surrounding sensitive information – if a hacker manages to breach one wall, your data will still be protected if you've successfully implemented additional strategies.

Follow a data storage policy

All organisations should have a data storage policy. This policy sets out how the organisation's information is to be stored, managed and shared. Senior management are responsible for developing and managing this policy, but you need to understand and follow it.

The following table outlines the different aspects of a data storage policy.

Scope of the policy	A data storage policy may cover digital information stored on computers, servers and networks. It may also include non-digital information (such as printouts, faxes and even spoken conversations) in the workplace.
Security classification	In Topic 1, we looked at the different classifications that can be applied to information in the workplace (e.g. public, internal, confidential and restricted). The data storage policy may define the different classifications used in an organisation, and give examples of each.

Rules for accessing information	This section of the policy specifies how different types of information can be accessed in the organisation; for example: ▪ public and internal information is available to all staff on a need-to-know basis ▪ confidential and restricted information is only available to authorised persons who have written permission from the owner of that information asset. The section may also specify: ▪ that information covered in the policy must be accessed only in order to perform required work tasks ▪ what must occur when a person with permission to access sensitive data loses this permission or leaves the company (e.g. close access and update passwords).
Rules for storing information	This section of the policy provides information about steps that must be followed in order to protect the information held by the organisation. These rules may vary between organisations, but some examples are provided below: ▪ Physical access to sensitive information must be protected by physical barriers (e.g. stored within locked areas, not visible on public monitors). ▪ Information devices must be protected from physical threats (such as heat, fire, floods, etc.). ▪ There must be restrictions on where sensitive information can be stored (e.g. some organisations do not allow sensitive information to be stored on the cloud or on portable devices that can be taken out of the workplace) ▪ Transfer of sensitive data must be encrypted (we'll look at encryption and encryption policies in more detail shortly).

Use encryption

'Encryption' involves converting data into a code (called 'ciphertext') that can only be read by authorised persons who have the secret key to read it. Encryption is used on both:

- data being stored on a device, and
- data being shared on the internet or across networks.

Encryption means that even if sensitive data is accessed by hackers, it cannot be used unless the hacker also has the secret key. A secret key is similar to a highly complex password.

There are two main forms of encryption, outlined in the following table.

Symmetric cryptography
In symmetric cryptography, the same key is used to encrypt and decrypt the data. This means that both the person sending the data and the person receiving it need to have access to the same secret key.

Asymmetric cryptography
Asymmetric cryptography is also called 'public key' cryptography, and uses two keys instead of one. The person sending the data uses a 'public key' to transmit their data, which is then locked. Only the receiver (who has a 'private key') can decrypt the data. This method of cryptography enables the security of data without the sender needing to have a private key.

The Australian Government encourages the use of secret key lengths of at least 128 bits up to 256 bits (using symmetric cryptography). The longer the key length, the more difficult it is for hackers to attempt to guess the key and thereby decrypt the data (this 'guessing' process is also called a 'brute-force attack').

Organisations should have policies and procedures relating to data encryption. The main components of an encryption policy are outlined in the following table.

Purpose of the policy	The purpose of an encryption policy will generally relate to protecting an organisation's data and information.
Scope of the policy	This section identifies what parts of an organisation are covered by the policy. This could include the assets to be covered (e.g. systems, hardware, data, etc.), as well as the people to whom the policy relates (e.g. employees, contractors, partners, etc.).
Details about how encryption is to be used	This section may include details about: ▪ what types of data must be protected (e.g. 'protected' or 'restricted' data, such as personally identifiable information) ▪ how encryption keys are to be managed ▪ how networks and hard disks are to be encrypted.
Roles and responsibilities for encryption	This section should specify: ▪ who is responsible for enforcing the policy
Compliance requirements	This section may include details about who is required to comply with the policy, and what the penalty is for non-compliance.

An encryption policy template is available from the National Cyber Security Society: aspirelr.link/ncss-encryption-policy

Use good password practices

A 2018 report conducted by Verizon found that 81 per cent of data breaches related to hacking were a result of either stolen or weak passwords. One of the most common passwords used is '123456' – how would you feel if this was the password being used to protect your personal information?

Good practices relating to passwords (also referred to as 'passphrases') are essential when maintaining the security of sensitive data and systems. A selection of the most important password practices is provided in the following table.

Use strong and long passwords	Passwords that are strong and long are much harder for hackers to guess. A 'strong' password uses a combination of: ▪ uppercase letters ▪ lowercase letters ▪ numbers ▪ symbols. In addition to being strong, passwords should be at least eight characters in length. However, longer passwords (up to 64 characters) provide even more security. Avoid using dictionary words or passwords that can be easily guessed (e.g. '123456', 'abcde', 'qwerty', etc.)
Use different passwords for every account	If you use the same password for all your personal and work accounts, you create the risk of having all your accounts compromised if one service is hacked. The best practice is to maintain completely different passwords for each account you use.
Change passwords when staff leave the organisation	Avoid the risk of ex-employees accessing sensitive data or sharing passwords to others by changing passwords as soon as a staff member leaves your organisation.
Use two-factor authentication	In two-factor authentication, a user is required to confirm their identity using an additional method to their password; for example, by entering a unique code sent to their personal device. This provides an additional barrier to hackers gaining access to your account using a password alone.
Use a password manager	Avoid keeping a list of all your passwords in a notepad or file on your phone. These methods are highly prone to being compromised. A password manager stores the passwords you use for all your accounts in one highly secure place. A good password manager can also help you to generate highly secure, unique passwords. You'll just need to remember the one password to access the password manager.

Share data securely

In a workplace, there will be times when you need to share or collaborate on documents containing sensitive data with colleagues. Data needs to be shared securely so that it does not fall into the wrong hands. When planning to share sensitive data with a colleague, consider the following steps.

Steps for sharing sensitive data:

- Confirm the data is being stored according to the organisation's data storage policy.
- Confirm the colleague has permission to access the sensitive data – this may require them to seek approval to gain access.
- Provide the colleague with information about where the sensitive data is stored in the organisation's network. Accessing data within a secure/encrypted network location provides greater transparency about when the data is accessed and by whom.
- If the sensitive data is protected by password, provide the password in person or over the phone. Never include password information in the same email as information regarding the location of the data.
- Mark any email communications relating to sensitive data as 'Private and Confidential' – any email communications must be conducted via secure/encrypted email.
- Never use unsecured email or messaging services when sharing sensitive data (this will be looked at in more detail shortly).

If your organisation is planning to share data with another party on an ongoing basis, the Australian Government Office of the National Data Commissioner has developed a draft data sharing agreement template. Working through this template can enable both parties comply with data sharing principles. The template can be accessed and downloaded here: aspirelr.link/data-commissioner-sharing-agreement

Avoid sending sensitive information via non-secure methods

Communication methods such as unsecured email and text message are fast, convenient and easy-to-use. However, they are not appropriate for sending and sharing sensitive information such as personally identifiable information. This is because they are not secure and may result in sensitive information ending up in the wrong hands. Examples of how this could occur include:

- the person who you send the sensitive information to forwards it to other unapproved people (either intentionally or unintentionally)
- the devices of either you or the recipient are hacked and the sensitive information is accessed
- the email account used by you or your recipient is breached as the result of a phishing attempt (discussed below)

- the server where your email (or your recipient's email) is stored is hacked.

Next time you're about to hit 'send' on a text message or email, think about whether you're about to transmit sensitive information. If the answer is 'yes', identify and use a secure method instead.

Example

Implement access protocols

Nhan works in the IT department of BookSmart, a large online textbook retailer. The company maintains a database of its customers, including sensitive information such as customer names, email addresses, postal addresses and passwords for the BookSmart online store. Nhan reviews the company's data storage policy and confirms (among other details) that:

- customer data is classified as 'restricted'
- customer data must not be stored in the cloud
- the server containing the customer database must be secured in a locked area at all times, with physical barriers providing protection from threats such as fire and flood.

Nhan checks the encryption of the customer database against the requirements of BookSmart's encryption policy and confirms that the data is encrypted using 128-bit symmetric cryptography.

Nhan has recently been involved in implementing a project to improve the quality of passwords used by staff to access the database. Staff were previously able to use any passwords they wanted, but are now required to use a password that is:

- at least 10 characters long
- uses a combination of lowercase, uppercase, numbers and symbols.

Two-factor authentication has also been set up so that when staff access the database, they need to enter a security code sent to their work mobile device.

Nhan receives an email from BookSmart's Head of Sales, Tim, asking Nhan to send an Excel spreadsheet containing the data of all customers who live in Brisbane to Tim's personal Hotmail account so he can work on it at the weekend. Nhan checks that Tim has permission to access this data, and gives him a call to explain how to access the data required. Nhan also explains to Tim that the company's data storage policy does not allow for sensitive data to be taken outside of the workplace.

Practice Task 5

Question 1

Which of the following statements are correct? Select 'yes' or 'no' for each one.

a) Unencrypted emails and text messages are secure methods for sending sensitive information. » Yes » No

b) Secure passwords should be both strong and long. » Yes » No

c) When considering sharing sensitive data, you should check your organisation's data storage policy. » Yes » No

d) Two-factor authentication provides extra security if a password is compromised. » Yes » No

e) Encrypted data can usually be decrypted quickly without a secret key. » Yes » No

Question 2

Which of the following would be considered good passwords? Tick all that apply.

- ◯ 123456
- ◯ password123
- ◯ X!jsh@jwjs2322
- ◯ H&b@3
- ◯ Alice1984

2C Identify and report infrastructure malfunctions and attacks

The security of an organisation's data may be threatened by both technical glitches and hacking attempts.

An organisation's IT infrastructure comprises many different parts, including physical computers, servers, data centres, routers, firewalls, hardware, software, operating systems and more. Infrastructure may experience malfunctions arising from technical issues, as well as attacks from hackers. In both cases, the personal information held by an organisation may be at risk. It's important to identify and report malfunctions and attacks as efficiently as possible to minimise their potential damage.

Infrastructure malfunctions

Breakdowns in IT infrastructure may not always be immediately obvious.

Like all technology (toasters, lawnmowers, cars, etc.), IT infrastructure will eventually malfunction and break down. On average, server hardware can be expected to last around three to five years; however, there are many reasons why technology may break down and these malfunctions may not always be obvious. A system might immediately shut down, or it might get slower and slower over time. In either case, malfunctions may prevent data from being protected.

The following table identifies some key ways to identify malfunctioning infrastructure.

Physical signs
The main physical symptoms of hardware malfunction are: ▪ overheating devices (such as servers) ▪ increased noise from devices. These signs may indicate a number of problems, ranging from broken power supplies and overloaded memory to broken fans. Outdated infrastructure is especially likely to experience issues such as these. These signs may also be accompanied by performance issues (see below), and should be reported immediately for investigation and maintenance.

Performance issues

Common performance issues include:

- system crashes
- system slowness
- system freezing.

Performance issues may occur due to:

- physical breakdowns in hardware
- compatibility issues with hardware/software
- viruses or attacks
- disk errors.

Checks that can be conducted in response to performance issues include:

- checking event logs
- physically checking infrastructure
- running a memory test
- checking server disks for errors
- running antivirus software
- using network monitoring software to check if the system is being put under stress.

Infrastructure malfunctions should be reported as quickly as possible, to prevent them from getting worse. Many organisations have processes in place for logging technical issues to an IT helpdesk. Using a formal logging process (instead of informally telling colleagues) will help to ensure the issue is properly escalated (if needed) and resolved.

Infrastructure attacks

Cyber attacks are deliberate attempts to exploit a computer system. Their impacts can be devastating.

The purpose of many cyber attacks is to steal sensitive data that can then be used to commit crimes. All parts of your organisation's digital infrastructure may be targeted by hackers, who will use a variety of techniques to gain access to your systems. By implementing the access protocols discussed earlier, the hacker's job is made more difficult. However, it is important that you can identify the signs of potential attacks and know how to report them.

Identifying potential attacks

The following table outlines some of the common signs that your IT infrastructure has been attacked.

Suspicious emails	'Phishing' is a term used for attempts by hackers to obtain sensitive information via email. Hackers can be very clever at disguising their email addresses so that they look like staff members or other trusted figures. Phishing emails typically include one of the following: ▪ requests for login credentials ▪ online links that compromise security ▪ attachments that compromise security. Staff education and training in identifying phishing attempts is necessary to prevent hackers from gaining access to your system. In the case of 'ransomware' attacks (where hackers demand a 'ransom' in order to unlock systems they have taken control of), hackers may make contact to demand money. You should not engage with blackmailers.
Suspicious password activity	If you find yourself locked out of your account and have not changed your password, it may be a sign that a hacker has gained access to the account and changed the password. Similarly, if you receive an email asking you to confirm a change of password request, this should be treated very suspiciously. As above, educating staff to be alert to these types of attacks is an important step in preventing their effectiveness.
Suspicious pop-ups	Hacking attempts may result in you being presented with unexpected pop-up windows when using the internet. These should not be clicked (even to close them) as they may result in further damage or access being provided to the hacker.
Unexpected computer/ network performance	Hacking attempts may result in computers on your network: ▪ running very slowly ▪ unexpectedly shutting down and restarting ▪ being operated without a local user entering commands ▪ using high amounts of data ▪ installing unknown software ▪ deactivating anti-virus software. Hacking attempts may also involve you being locked out of your devices and data being removed.

Reporting incidents

Any incidents that could compromise the security of sensitive information must be documented.

In the event of anything compromising your organisation's IT infrastructure, you need to follow organisational policies for reporting incidents. In the first instance, especially if the incident or threat is still active, this may involve making senior management aware of the issue so that they can identify the best course of action.

Many organisations use a cyber security incident register to report and manage incidents. The Australian Government's Australian Signals Directorate recommends that an incident register should include the following details.

Cyber security incident register details:

- The date the incident occurred
- The date the incident was discovered
- A description of the incident
- A description of the actions taken in response to the incident
- Details of the person/parties to whom the incident was reported

As discussed in Topic 1, any incidents that involve a breach of personal information must be reported under the Notifiable Data Breach (NDB) scheme to:

- the people whose data was compromised
- the Office of the Australian Information Commissioner (OAIC).

Example

Identify and report infrastructure malfunctions and attacks

Suzette works in the IT department of StockTips, a stock trading company. Recently, the computers used by StockTips staff have begun to run very slowly. Suzette conducts a number of checks to confirm that the issue is not due to an infrastructure malfunction. These checks include:

- physically checking the company's servers for excess noise or heat
- running memory tests
- checking event logs.

As she is conducting these tests, Suzette receives a call from a colleague who says he has been locked out of his work email account. When questioned, the colleague mentions he did recently open an attachment on an email that he thought 'looked a bit funny'. Suzette suspects the performance issues may be a result of a phishing attempt. She alerts her manager to the issue and also records it in the company's cyber security incident register.

Practice Task 6

Question 1

Which of the following are signs of malfunctioning infrastructure? Tick all that apply.

- ◯ A server generating a lot of heat
- ◯ Business systems running very slowly
- ◯ Demands for ransom being received
- ◯ Computing equipment making loud noises
- ◯ Staff receiving unexpected pop-ups when using the internet

Question 2

List two common signs that IT infrastructure has been hacked.

Summary

- Data needs to be well-organised and accurate in order to be useful.
- Organising data involves following file-naming conventions and using a logical folder structure.
- Data should be checked to confirm it is accurate, up-to-date and timely.
- Protocols should be implemented on sensitive data to limit who can access it.
- All organisations should have a data storage policy, which outlines how information is to be stored, managed and shared.
- Sensitive data should be encrypted to prevent it from being read by unauthorised persons.
- Good password practices (such as using strong and long passwords) are one of the best ways of protecting sensitive information.
- Data should be shared using secure methods – non-secure emails and text messages must never be used for sharing sensitive information.
- Infrastructure malfunctions and cyber attacks can both hurt the protection of data.
- Incidents must be reported as soon as possible using organisational policies and procedures.

Learning Checkpoint 2

Store and share sensitive information

Part A

1. Which of the following statements are correct? Select 'yes' or 'no' for each one.

   a) When naming files, you should consider how similar files have been named in the past. » Yes » No

   b) File names should be at least 25 characters in length. » Yes » No

   c) It is best to delete previous versions of files to keep things organised. » Yes » No

   d) The 'Check for duplicates' feature in spreadsheet software can help you check data for accuracy. » Yes » No

   e) Datasets may include information to help identify if the data is up-to-date. » Yes » No

2. Which of the following statements are correct? Select yes or no for each one.

   a) Cyber attacks should be reported using an organisation's cyber security incident register. » Yes » No

   b) Performance issues may be a result of either infrastructure malfunctions or cyber attacks. » Yes » No

   c) A data encryption policy should include information about the types of data to be encrypted. » Yes » No

   d) A data storage policy only covers digital information held by the company. » Yes » No

   e) A data storage policy identifies digital barriers to information, but not physical barriers. » Yes » No

Part B

Read the case study and answer the questions that follow.

Case study

Toni is working in the IT department of CoffeeKick, a large coffee bean retailer. The company gathers sensitive data from customers who purchase coffee beans from the company's online store. Toni is aware that staff members regularly send spreadsheets containing customer data to one another using unsecured email accounts.

1. Which of the following are potential risks of using unsecured email accounts to send sensitive information? Tick all that apply.

   - ◯ Emails containing sensitive information might be forwarded to unapproved people.
   - ◯ Emails containing sensitive information might take longer to reach recipients.
   - ◯ Devices containing unsecured email accounts might be hacked.
   - ◯ Unsecured email accounts are less convenient to use.
   - ◯ Servers where email data is stored might be hacked.

2. What are two steps Toni should follow when considering sharing sensitive data with a colleague?

3. When protecting files with a password, what are three strategies Toni should use? Tick all that apply.

   - ◯ Use dictionary words.
   - ◯ Use at least eight characters.
   - ◯ Use a mix of uppercase letters, lowercase letters, numbers and symbols.
   - ◯ Use the same password she uses for other online services.
   - ◯ Use multi-factor authentication, if possible.

Topic 3 | Apply information protection protocols

3A Conduct data back-ups

3B Conduct privacy impact assessments

3C Confirm adherence to data protection standards

3A Conduct data back-ups

Back-ups are a critical step in ensuring data security.

For many organisations, data is a very precious asset. The cost of losing this data can be enormous. This is why back-ups are so important. A 'back-up' is simply a copy of data that is created and stored in another (physical and/or digital) location. If data is lost or corrupted due to an attack or other failure, the back-up can be used to recover some or all of the lost data.

Organisational back-up plans

Data back-ups must be conducted according to the organisation's back-up plan.

When backing up data, you need to follow the relevant policies and procedures used in your organisation. The key information you need to know is usually contained in the organisation's back-up plan.

The following table provides an overview of the key information you should be able to access in the back-up plan.

What data is being backed up?	Your organisation is likely to be holding a lot of data. However, not all of this data will always need to be backed up. For example, computer operating system and program files may not need to be included in a back-up plan, as they can be easily re-downloaded from the software publisher if required. The types of data specified in a back-up plan may include: ▪ customer information ▪ financial information ▪ HR information ▪ company emails.
What type of back-up is being performed?	There are three types of back-up. Full back-up: This involves a complete back-up of all data. This approach takes a longer time and uses more space than other options. Incremental back-up: This involves backing up only the data that has been changed or created since the last incremental back-up was performed. This approach is faster and needs less space than a full back-up, but requires all incremental back-up files to be available in order to completely restore data in the event of a loss. Differential back-up: This is similar to an incremental back-up, but it backs up the data that has been changed or newly created since the last full back-up.

Where is the data being backed up?	The main question here is whether the data is being backed up on-site or off-site. We'll look more at this shortly.
How often do data back-ups occur?	Regular back-ups are required to minimise the amount of data that can be lost. For important files, back-ups should generally occur at least every 24 hours.
Who is responsible for performing and monitoring back-ups?	Data back-ups may be set to be performed automatically at regular intervals, but they may also be conducted manually by a specified person or position. You need to identify the person or role whose responsibility it is to monitor the success of the back-up process. This involves testing back-ups to ensure they can be recovered if required. Ensuring back-ups are monitored reduces the risk of back-up data not being able to be restored after a disaster.

Back-up methods

Back-ups can be conducted on-site or off-site.

The two main methods for backing up data are performing on-site back-ups or off-site back-ups (also referred to as 'remote' back-ups). Each method has benefits and risks.

On-site back-ups

An on-site back-up involves back-up data being stored on a local storage device such as:

- an on-site back-up server
- an external hard drive
- magnetic tape
- optical media such as a DVD or CD.

The benefits and risks of on-site back-ups are outlined in the following table.

Benefits of on-site back-up	Risks of on-site back-up
▪ The internet is not required to restore backed-up data. ▪ Back-ups are easily accessible. ▪ Back-ups are generally low-cost.	▪ Back-ups are open to physical threats such as natural disasters and burglary. ▪ The back-up process may be manual and time-consuming.

Back-up devices must be stored securely to protect them from physical threats. This generally involves the use of locks and passcodes in the areas where back-ups are stored.

Off-site back-ups

An off-site (or remote) back-up involves saving a copy of your data to the cloud. Cloud storage is a network of servers located in multiple locations and managed by a hosting provider. Organisations rent space from the hosting provider to store data. The hosting provider is responsible for keeping the data both safe and accessible to authorised users. The term 'distributed storage' is used when data is stored across multiple physical servers and data centres.

Benefits of off-site back-up	Risks of off-site back-up
▪ Back-up data can be accessed from anywhere. ▪ Back-ups are protected from physical threats to the on-site location . ▪ Back-ups can be stored by vendors who specialise in data storage security. ▪ The back-up process can be automated.	▪ The internet is required to access the backed-up data. ▪ Full data recovery may take some time depending on how the cloud storage is configured. ▪ It involves a third party having access to your data. ▪ It involves data being distributed across multiple sites – this increases the risk of being compromised, in comparison to keeping the data in one location.

The National Archives of Australia provides comprehensive information about the potential risks and benefits of cloud storage: aspirelr.link/naa-digital-storage

Using a combination

As on-site and off-site methods of backing up data each have advantages and disadvantages, to minimise risk, organisations can use a blend of both methods. For example, an organisation might automatically back up its data to the cloud, but also create an on-site back-up to a local hard drive.

You should also refer back to your organisation's data storage policy (covered in Topic 2) – this policy may specify what types of data can and cannot be stored in the cloud.

Consequences of storage location

When considering the use of off-site back-ups and cloud storage, identify the locations where your data will be stored. The physical locations of the servers where your data is stored are governed by local laws and regulations. International governments may have the power to view all your information, including sensitive data. Storing sensitive data in countries where it may be accessed by international governments may breach Australian privacy legislation.

To minimise the above risks when using cloud-based storage, check:

- the location of the servers where your data is being stored
- whether the hosting provider provides any access to third parties
- whether Australian data can be stored legally in the jurisdiction that covers the servers.

Example

Conduct data back-ups

Aradhya recently joined the IT team at Perfekt, an online cosmetics retailer. Part of Aradhya's role is being responsible for the company's data back-ups. Aradhya refers to Perfekt's back-up plan and confirms:

- what the data is to be backed up (including financial, customer and HR data among others)
- that incremental back-ups are to be conducted
- that back-ups are to be performed at least every 24 hours.

Automatic back-ups to the cloud are run every 24 hours, but it is Aradhya's role to check that these back-ups have been run and the data can be restored. To minimise risk, the back-up plan also specifies that a weekly manual on-site back-up is to be conducted (requiring a back-up to an external drive). Aradhya sets a calendar reminder to perform this manual back-up every Friday.

Practice Task 7

Question 1

What are the three types of data back-up? Tick all that apply.

- ◯ Full back-up
- ◯ Incomplete back-up
- ◯ Predictive back-up
- ◯ Incremental back-up
- ◯ Differential back-up

Question 2

What are two benefits of using cloud storage or distributed storage for data back-ups?

Question 3

Why do you need to know the physical location where cloud data is being stored?
Tick all that apply.

- ◯ Data storage is cheaper in some countries than others.
- ◯ Your data will be governed by local laws and regulations.
- ◯ Storing sensitive data in some countries may breach Australian privacy laws.
- ◯ Some foreign governments may be able to view your confidential data.
- ◯ All data must be hosted in Australia according to the *Privacy Act 1988* (Cth).

3B Conduct privacy impact assessments

Conducting a privacy impact assessment helps to identify how your work might impact on people's privacy.

All Australian organisations with responsibilities under the *Privacy Act 1988* (Cth) should undertake privacy impact assessments (PIAs). PIAs help organisations meet the Australian Privacy Principles (APPs). Specifically, PIAs help to ensure that personal privacy considerations are built into a planned piece of work (such as a new project or changes to an existing work practice), instead of being an afterthought. Examples of when a PIA may be required include:

- an organisation plans to make changes to how it stores customer information
- an organisation plans to conduct a project to gather customer information for marketing purposes.

Steps involved in a PIA

Conducting a PIA involves following a systematic process.

Organisations may have their own PIA processes. However, if your organisation does not have its own PIA process in place, the Office of the Australian Information Commissioner (OAIC) provides a comprehensive process for conducting a PIA, which is a great starting point. This process comprises 10 steps.

An overview of the PIA process provided by the OAIC is provided below, but further detail is available from the OAIC website: aspirelr.link/oaic-privacy-impact-assessments

1. Conduct a threshold assessment

   A threshold assessment will help you identify if a PIA is required for the work you are planning to do.

   Questions to answer in a threshold assessment include:

   - Will any personal information be collected, stored, used or disclosed in this work?
   - What type of information will be collected, and how sensitive is it?

   If personal information is not being collected as part of the work, you may not need to proceed with the PIA.

2. Plan the PIA

If the threshold assessment indicates that a PIA will be required, the PIA process needs to be planned. Questions to answer when planning the PIA include:

- How detailed does the PIA need to be?
- Who will be involved in the PIA?
- When does the PIA need to be conducted?
- What budget and resources are available for conducting the PIA?
- What other stakeholders need to be involved in the process?
- What will happen after the PIA? For example, how will recommendations from the PIA be put into action?

3. Describe the work being planned

You need to be able to describe the work being planned in enough detail for external reviewers to understand it.

Questions you should be able to answer when describing planned work include:

- What are the overall aims of the planned work?
- How do these aims fit within the organisation's objectives?
- What is the scope of this work?
- What are the links between this work and other projects?
- Who is responsible for this work?
- What is the time frame for this work?
- What are the key privacy issues relating to this work?

4. Consult with stakeholders

Stakeholders include anyone who is interested in or may be affected by the work being planned. Stakeholders may include clients, service providers, industry experts, regulators and others.

The main reason for consulting with stakeholders is to identify:

- potential privacy risks and concerns that may not have been identified by you or the team conducting the PIA
- strategies to manage these risks.

5. Map the flow of personal information

This step involves identifying how personal information will flow through the work you are planning to do. To conduct this step, you need to be able to answer the following questions:

- What information will be collected as a result of the planned work?
- How will the information be securely held and protected?
- How will the information be used and disclosed?
- What processes will be used to ensure information quality?
- Who will have access to the information, and what security is in place for this?
- How will information be destroyed?
- How will people be able to access and correct their personal information?

6. Check how the planned work impacts on privacy

This step involves identifying whether the planned work has acceptable or unacceptable impacts on people's privacy.

Questions to answer include:

- What is the risk to people's privacy as a result of the planned work?
- Are any impacts on privacy unnecessary or avoidable?
- Do privacy impacts affect the aims of the planned work?
- Will privacy laws be complied with?
- Does the planned work meet the 13 APPs?
- Do the impacts on privacy meet community expectations?

7. Manage privacy risks

In the previous step, risks to people's privacy may have been identified. Examples of risks include:

- personal information is collected when it is not required
- information collection methods are unreasonably intrusive
- people are not able to easily access and correct their own information.
- Strategies to manage these types of risks need to be identified and documented. Examples of strategies you might consider include:
- technical controls, such as the use of data encryption or access protocols
- operational controls, such as policies or procedures and staff training
- communication strategies, such as privacy notices.

8. Develop recommendations

Based on what you have identified in the previous steps, you should develop recommendations. Questions to answer include:

- What changes would enable a balance between the aims of the planned work and people's privacy?
- What strategies can be used to manage privacy risks?
- Is any further consultation required?
- Are the potential privacy risks so great that the planned work should not go ahead?

Time frames for actioning each recommendation should also be identified.

9. Create a PIA report

A PIA report collects all the information you have gathered and created in the previous steps. Your organisation might have its own PIA template you can use. Otherwise, you can adapt the PIA report template provided on OAIC website: aspirelr.link/oaic-pia-tool

The standard inclusions for a PIA report are:

- executive summary
- details of the approach used for conducting the PIA
- description of the planned work, including information flows
- analysis, including the privacy impacts of the planned work, and risks, strategies and recommendations relating to these impacts
- conclusion, containing the overall findings of the PIA
- appendices, including details of stakeholders consulted.

10. Respond to recommendations

Creating the PIA report is not the final step in the process. The PIA will be reviewed by relevant stakeholders, and decisions will be made about which recommendations will be implemented. Based on the review process, you may need to make further changes to the PIA report.

Example

Conduct privacy impact assessments

Antonio works at BizWizz, a large marketing intelligence company. The company is planning a project to move the storage of its marketing database (containing the personal information of clients on its mailing list) from an in-house server to a cloud-based solution. Antonio recognises that this work requires the completion of a PIA. BizWizz does not have its own PIA process or documentation, so Antonio adapts the process provided by the OAIC and uses its PIA report template. Through the process of conducting the PIA, Antonio identifies significant risks to the organisation's client data. He identifies strategies for managing these risks and documents them in a PIA report, which he distributes to the ICT management team for consideration.

Practice Task 8

Question 1

In what situations should a full privacy impact assessment be conducted? Tick all that apply.

- ◯ When an organisation has responsibilities under the Commonwealth Privacy Act
- ◯ When personal information was gathered as part of a project that has been completed
- ◯ When an organisation has experienced a data breach
- ◯ When planned work involves personal information being collected, stored, used or disclosed
- ◯ When an organisation has a contract with the OAIC

Question 2

What are three questions you would ask when mapping the flow of personal information as part of a PIA?

3C Confirm adherence to data protection standards

The APPs set out the main standards you need to meet when working with sensitive data.

Topic 1 introduced the APPs. Following the APPs enables organisations to comply with the Commonwealth Privacy Act and protect sensitive data. Each APP contains a lot of detail, so it's important that you're aware of ways to check your workplace is compliant.

The 13 APPs

To comply with the 13 APPs, you first need to understand them.

All organisations with responsibilities under the Privacy Act must adhere to the 13 APPs. Even if your organisation does not have responsibilities under the Privacy Act, following the APPs will ensure you are meeting best practices in protecting sensitive data.

The following table provides a summary of the 13 APPs and the purpose of each.

APP 1: Open and transparent management of personal information	An organisation must manage personal information openly and transparently. This include maintaining a privacy policy.
APP 2: Anonymity and pseudonymity	With some exceptions, an organisation must give people the option to not identify themselves, or to use a pseudonym.
APP 3: Collection of solicited personal information	An organisation can only collect personal information in certain situations. Even higher standards apply when an organisation wishes to collect sensitive information.
APP 4: Dealing with unsolicited personal information	An organisation has obligations when people send it unsolicited personal information.
APP 5: Notification of the collection of personal information	An organisation is required to inform people when it is collecting personal information.
APP 6: Use or disclosure of personal information	An organisation may only use or disclose personal information in certain circumstances.
APP 7: Direct marketing	An organisation can only use personal information for the purposes of direct marketing under certain conditions.

APP 8: Cross-border disclosure of personal information	An organisation must take steps to protect personal information before it is disclosed outside Australia.
APP 9: Adoption, use or disclosure of government-related identifiers	In limited situations, an organisation may be able to use a government-related identifier of an individual as its own identifier.
APP 10: Quality of personal information	An organisation must take reasonable steps to ensure that the information it holds about people is accurate, up-to-date and comprehensive.
APP 11: Security of personal information	An organisation must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure. An organisation also has responsibilities around the destruction and de-identification of personal information in some situations.
APP 12: Access to personal information	An organisation has responsibilities when an individual requests access to any personal information held by the organisation.
APP 13: Correction of personal information	An organisation has responsibilities to correct the personal information it holds regarding individuals.

The OAIC website provides comprehensive information about each of the APPs: aspirelr.link/oaic-privacy-principles

Confirming adherence

Confirming adherence requires you to investigate and ask questions.

If you've looked at the detailed information for the APPs (available from the OAIC), you'll know that there are a lot of requirements for each one. This means that confirming adherence with each APP can be challenging.

In Topic 1C, we looked in some detail at APP 11 (Security of Personal Information) and identified a number of questions you can ask to confirm adherence. Using the detailed information for each APP, you can create a similar checklist for each of the additional APPs. You could also ask senior staff the questions in your checklists.

A sample checklist for APP 2 (Anonymity and Pseudonymity) is provided below.

Sample APP 2 checklist:

- Are the situations in which a person can deal anonymously or by pseudonym with our organisation outlined in our privacy policy?
- Does the privacy policy indicate if there will be any consequences if a person chooses to deal with our organisation anonymously or by pseudonym?
- Are people made aware that they can deal either anonymously or by pseudonym with our organisation?
- When information is gathered from people via website forms, are fields that cannot be anonymous made non-mandatory?
- Are there any situations where people are required by law to provide their personal information to our organisation (instead of anonymously or by pseudonym)? If yes, what situations are these?

Tips from the OAIC

In addition to this detailed approach to confirming adherence with the APPs, the OAIC suggests a number of broader actions you can take to help you and your organisation comply with all 13 APPs. These are summarised in the following table.

10 tips to support adherence with the APPs:

- Ensure that you're familiar with your organisation's internal privacy policies, processes and procedures,
- Ensure that you know who is responsible for privacy. While all staff must ensure privacy is protected, there should be a key privacy officer who leads the organisation's privacy efforts.
- Conduct PIAs when planning projects or changes to how work is done.
- Only collect the personal information your organisation actually needs. Don't collect information you think might be useful at some point in the future.
- Try to avoid disclosing personal information even in situations where a person has consented to disclosure.
- When disclosing personal information to overseas parties, make sure the overseas party also complies with the APPs.
- Take extra care when handling highly sensitive information such as linked data relating to a person's health, genetics, religious beliefs or sexual orientation.
- Ensure personal information is accessed on a need-to-know-basis, using appropriate access protocols.
- Keep personal information secure, following relevant policies relating to data storage, encryption, back-ups, etc.
- Be aware of your organisation's data breach response plan, and your responsibilities according to the plan.

Example

Confirm adherence with data protection standards

Ben works in the IT department of SoftPlay, an Adelaide-based video game publisher with annual revenues of $20 million per year. Ben has been asked to assist in a project to confirm the company's compliance with the APPs.

Ben first refers to the OAIC website to gain a better understanding of the APPs. As he reviews each APP, Ben writes a list of questions relating to SoftPlay's operations. He uses this checklist to look at how SoftPlay currently meets the APP requirements. Some of the questions require discussion with Ben's managers about how things are currently done. Ben also prints out a copy of the 10 tips provided by the OAIC as a quick reference to help maintain compliance with the APPs during his everyday work.

Practice Task 9

Question 1

What are two actions you can take to help confirm your organisation's adherence to the APPs?

Summary

- Data back-ups need to be conducted according to the organisation's back-up plan.
- Back-ups can be conducted on-site (on a server, hard drive or physical media), off-site or a combination of both.
- Off-site back-ups are conducted to the cloud – this has benefits, but also comes with a number of risks.
- The physical location of servers needs to be identified when considering off-site back-ups.
- Privacy impact assessments (PIAs) help organisations to identify how people's privacy might be affected by planned work.
- The PIA process involves following the 10 steps outlined by the OAIC.
- Organisations with responsibilities under the *Privacy Act 1988* (Cth) must adhere to the 13 Australian Privacy Principles (APPs).
- Methods to confirm adherence with the APPs include creating checklists and following the strategies provided by the OAIC.

Learning Checkpoint 3

Apply information protection protocols

Part A

1. Number each step from 1 to 6 in the order you would follow to conduct a PIA.

   ◯ Check how planned work impacts on privacy and manage the risks.

   ◯ Respond to recommendations.

   ◯ Conduct a threshold assessment and plan the PIA.

   ◯ Map the flow of information.

   ◯ Describe the work being planned and consult with stakeholders.

   ◯ Develop recommendations and create a PIA report.

2. Which of the following statements are correct? Select 'yes' or 'no' for each one.

   a) The APPs must be met by all organisations with responsibilities under the Commonwealth Privacy Act. » Yes » No

   b) Confirming compliance with the APPs may require you to ask senior managers questions. » Yes » No

   c) There are 10 APPs you need to understand and comply with. » Yes » No

   d) Developing a checklist is a good way to check compliance with the APPs. » Yes » No

Part B

Read the case study and answer the questions that follow.

Case study

Therese works in the ICT department of TurboGlitch, an app development company. Therese has recently been given the responsibility of managing back-ups of the company's data.

1. What are three pieces of information Therese should expect to find in the company's back-up plan?

2. What are the three main types of back-ups Therese might perform? Tick all that apply.

- ◯ Redundant back-up
- ◯ Encrypted back-up
- ◯ Full back-up
- ◯ Incremental back-up
- ◯ Differential back-up

3. What are three benefits of backing up data to the cloud or distributed storage? Tick all that apply.

- ◯ Backed-up data can be retrieved without access to the internet.
- ◯ Backed-up data can be retrieved from anywhere.
- ◯ Back-ups are protected from physical threats to the TurboGlitch office.
- ◯ The back-up process can be automated.
- ◯ The back-up process does not involve any third parties.

4. What are two questions Therese should ask relating to the location of cloud hosting provider used for remote back-ups?