Learner Guide

302508602 / Den Rise / shutterstock.com

ICTICT532

Apply IP, ethics and privacy in ICT environments

tafe.qld.edu.au

MAKE GREAT HAPPEN

tafe Queensland

Unit version	Document version	Release date	Comments/actions
ICTICT532	v1	May 2022	Initial release

Copyright

© TAFE Queensland 2022

Copyright protects this material. Except as permitted by the Copyright Act 1968 (Cth), reproduction by any means (photocopying, electronic, mechanical, recording or otherwise), making available online, electronic transmission or other publication of this material is prohibited without the prior written permission of TAFE Queensland.

Inquiries must be addressed to the TAFE Queensland Copyright Officer, Office of the Chief Academic Officer, TAFE Queensland, PO Box 16100, CITY EAST QLD, 4002, or Email TAFEQLDIP@tafe.qld.gov.au.

Disclaimer

Every effort has been made to provide accurate and complete information. However, TAFE Queensland assumes no responsibility for any direct, indirect, incidental, or consequential damages arising from the use of information in this document. Data and case study examples are intended to be fictional. Any resemblance to real persons or organisations is coincidental.

If you believe that information of any kind in this publication is an infringement of copyright, in material in which you either own copyright or are authorised to exercise the rights of a copyright owner, and then please advise us by contacting the TAFE Queensland Copyright Officer, Office of the Chief Academic Officer, TAFE Queensland, PO Box 16100, CITY EAST QLD, 4002, or Email TAFEQLDIP@tafe.qld.gov.au.

Introduction

This Learner Guide has been developed to support you as a resource for your study program. It contains key information relating to your studies including all the skills and knowledge required to achieve competence.

What will I learn?

This unit describes the skills and knowledge required to maintain professional and ethical conduct, as well as to ensure that personal information of stakeholders is handled in a confidential and professional manner when dealing with stakeholders in an Information and Communications Technology (ICT) environment.

It applies to ICT personnel who are required to gather information to determine the organisation's code of ethics and protect and maintain privacy policies and system security.

Where can I get more information?

For further information on your qualification, accredited course or Unit/s of Competency, please go to:

https://training.gov.au/Training/Details/ICTICT532

© TAFE Queensland 2020

TAFE Queensland student rules

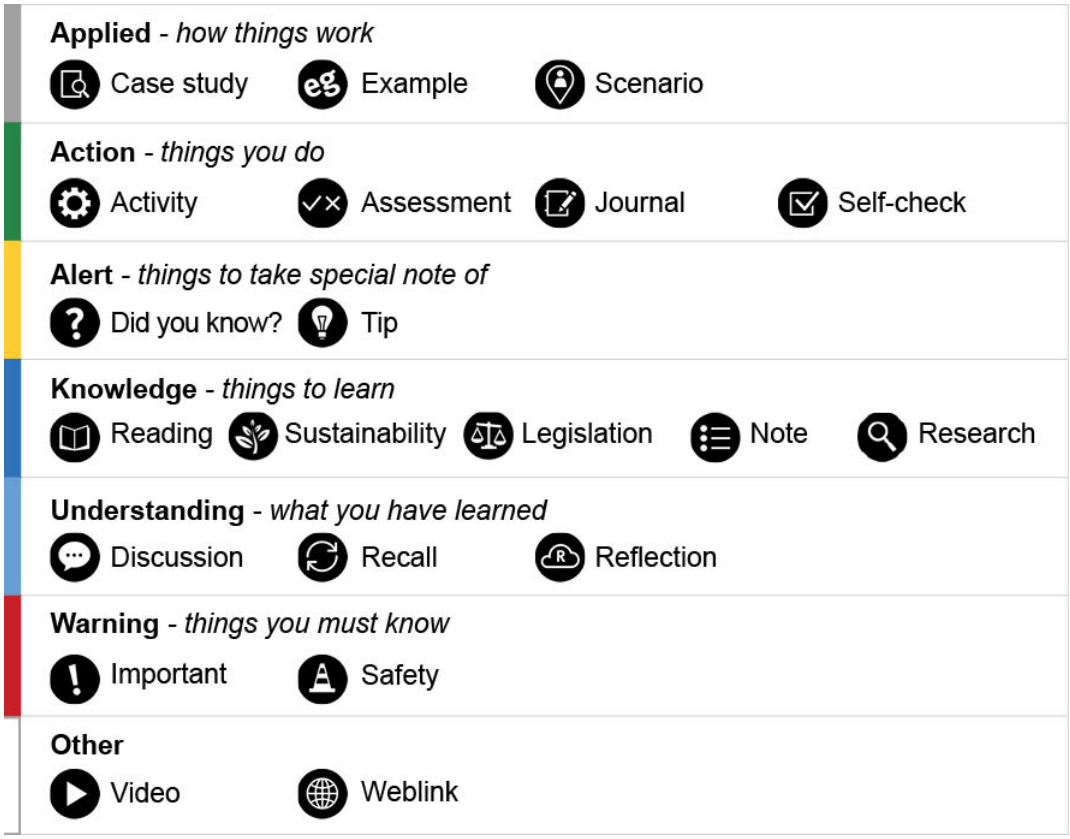
TAFE Queensland student rules are designed to ensure that learners are aware of their rights as well as their responsibilities. All learners are encouraged to familiarise themselves with the TAFE Queensland student rules, specifically as they relate to progress of study and assessment guidelines. A full guide to student rules can be found at Student rules[1].

Information to support your learning and assessment

There's always someone to help you. Undertaking further study can bring both excitement and challenges. Our Student Services, Learning Support and Library staff can help you make the most of your time at TAFE.

Callout panels

A number of panels have been designed to help guide you to important information and actions throughout this Learner Guide. The full choice of panels you are likely to encounter to support you in your studies are included below. NB: not all the panels will be used in every learner guide.



[1] http://tafeqld.edu.au/current-students/student-rules/

 © TAFE Queensland 2020

Contents

Introduction 3
What will I learn? 3
Where can I get more information? 3
TAFE Queensland student rules 4
Information to support your learning and assessment 4
Callout panels 4
Contents 5
Welcome 9
Policies and Procedures 10
Introduction 10
What is a workplace policy? 11
What are policy and procedure documents? 13
Business processes, procedures, and standards 15
Updating policies 18
Distributing policies 19
Topic summary and review 20
Legislation standards and policies 21
Introduction 21
Privacy Act 1988 22
Rights and responsibilities 23
Australian privacy principals 26
Notifiable breaches 28
Information Privacy Act 2009 (QLD) 30
ISO 27001 31
NIST 33
International legislation 36
Topic summary and review 38
Company privacy policies 39
Introduction 39
Privacy policy 40
Collection of personal information 42

 © TAFE Queensland 2020

Use and disclosure of personal information 44
Control and rights of a customer's personal information 46
For websites – cookies and third-party sites consent clauses 48
Topic summary and review 51
Copyright 52
Introduction 52
What is copyright? 53
The Copyright Act 1968 55
What does copyright protect? 57
How to get permission 58
Information on the web site for permission 61
Media files 63
Copyright – particular problems 65
Copyright clearance 67
Topic summary and review 70
Intellectual property 71
Introduction 71
What is Intellectual Property (IP)? 72
Patents 74
Trademarks 75
Design rights 76
PBR 78
Topic summary and review 79
Data 80
Introduction 80
What is data? 81
Sensitive data 82
Personally identifiable information 84
Identifying sensitive data 85
Classifying data 86
Topic summary and review 88
Sending and receiving sensitive data 89

Introduction....89
The Information life cycle....90
Sending and receiving unsecured data....91
Transmitting and receiving unsecured data....92
Sending and receiving secure data....94
Email and network security....95
Topic summary and review....98
File location....99
Introduction....99
Types of file location....100
The traditional storage devices....102
The cloud....103
Cloud computing deployment models....105
Cloud computing solutions....107
Microsoft Azure....108
Topic summary and review....111
Data integrity and authorised access....112
Introduction....112
Attacks on data integrity....113
What is a data integrity attack?....114
Mitigating data integrity attacks....116
Authorised personnel....117
Access permissions - passwords....118
Access permissions - two-factor authentication....120
Encrypting files....122
Hashing....125
Hashing files and messages....127
Topic summary and review....129
Destroying data....130
Introduction....130
Retention of data or records....131
Destruction of data – Queensland government agencies....132

 © TAFE Queensland 2020

Destruction of data – non-government organisations 134
Topic summary and review 135
Privacy Impact Assessment 136
Introduction 136
Undertaking a Privacy Impact Assessment 137
Topic summary and review 138
Ethics in the workplace 139
Introduction 139
What defines ethics in the workplace? 140
Codes of conduct 142
Implementing the code of conduct in the workplace 144
Topic summary and review 145
Self-check answers 146
References 158

 © TAFE Queensland 2020

Welcome

Welcome to the *ICTICT532 Apply IP, ethics and privacy in ICT environments*. By completing this unit you will be able to:

- establish organisational IP requirements
- review and determine organisational IP, ethics and privacy policies
- contribute to privacy policy
- maintain ethics code.

 © TAFE Queensland 2020

Policies and Procedures

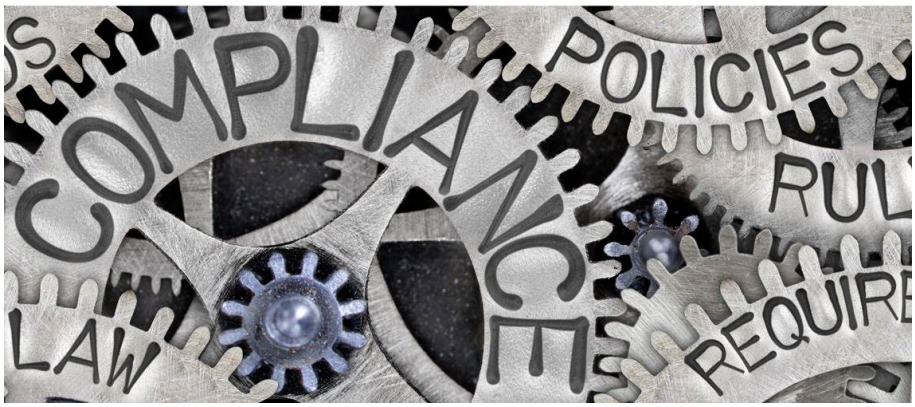
Introduction

No good business can operate successfully if the organisation does not have a set of policies and procedures in place. These policies and procedures are there to help the organisation keep on track with where they are going, how they treat employees and clients and how they react to situations that they will confront.

Objectives

By completing this topic, you will be able to:

- understand what a workplace policy is
- know the benefits of having workplace policies
- understand what policy and procedure documents are
- identify business processes, procedures, and standards
- standardise key business activities
- create effective processes, procedures, and standards
- update policies
- understand policy distribution.



309211911 / EtiAmmos / stock.adobe.com

 © TAFE Queensland 2020

What is a workplace policy?

A policy is a statement which underpins how human resource management issues will be dealt with in an organisation. It communicates an organisation's values and the organisation's expectations of employee behaviours and performance.

Workplace policies are important and have many functions.

- **Clarification** – Workplace policies often reinforce and clarify standard operating procedures in a workplace. Well written policies help employers manage staff more effectively by clearly defining acceptable and unacceptable behaviour in the workplace and set out the implications of not complying with those policies.
- **Purpose** – A workplace policy consists of a statement of purpose and one or more broad guidelines on action to be taken to achieve that purpose. The statement of purpose should be written in simple terms and free of jargon. The length of the policy may vary depending on the issue it addresses.
- **Discretion** – A policy may allow discretion in its implementation and the basis of that discretion should be stated as part of the policy. A policy may also be required where there is a diversity of interests and preferences, which could result in vague and conflicting objectives among those who are directly involved.

Not all workplace issues require a policy. Many routine matters can be dealt with through simple workplace procedures and processes being put in place. Read the following page to discover the benefits of workplace policies and examples of different types.

1788911858 / ra2 studio / shutterstock.com

 © TAFE Queensland 2020

Benefits of workplace policies

Well-written workplace policies:

- are consistent with the values of the organisation
- comply with employment and other associated legislation
- demonstrate that the organisation is being operated in an efficient and businesslike manner
- ensure uniformity and consistency in decision-making and operational procedures
- add strength to the position of staff when possible legal actions arise
- save time when a new problem can be handled quickly and effectively through an existing policy
- foster stability and continuity
- maintain the direction of the organisation even during periods of change
- provide the framework for business planning
- assist in assessing performance and establishing accountability
- clarify functions and responsibilities.

Types of policy

Here are some examples of common workplace policies that could assist your workplace:

- code of conduct
- recruitment policy
- internet and email policy
- mobile phone policy
- non-smoking policy
- drug and alcohol policy
- health and safety policy
- anti-discrimination and harassment policy
- grievance handling policy
- discipline and termination policy
- using social media.

Other policies are:

- privacy policy
- ethics policy
- copyright and intellectual property policy.

Copied Under s113P https://www.industrialrelations.nsw.gov.au/employers/nsw-employer-best-practice/workplace-policies-and-procedures-checklist/#types-of-workplace-policies, 29/07/2021

What are policy and procedure documents?

Policies and procedure documents are two different categories of the functions of an organisation. Policies are the guidelines that govern the organisation's behaviour and processes. Procedures are the processes used to implement policies within the organisation.

A policy dictates what the standard or benchmark is, whereas, procedures guide policy changes, taking into account internal and external influences such as technology, workplace environment, and even state and federal legislation.

By having policies and procedures in place, you create standards and values for the organisation. They can also improve the way the customers and staff deal with your organisation. See below for more detail.

- Identify key processes and tasks in the organisation and develop standard operating procedures (SOPs) for each.
- Allow staff to contribute to the SOPs and regularly review the organisation's procedures.
- Ensure the organisation's policies are documented and accessible.
- Make important procedures such as first-aid and emergency procedures clearly visible.
- Communicate the organisation's policies to staff. Help them to understand them and why they are important.
- Educate staff on procedures that are specific to a certain role.

242514907 / vinnstock / shutterstock.com

 © TAFE Queensland 2020

Example

There are no standardised templates used to create a policy or a procedure document. Here is an example of a Privacy policy template.

Privacy policy template[2]

Activity

As a student in the classroom, list the location where you would find the conduct and behaviour document.

Answer: Student rules and policies

[2] https://business.vic.gov.au/tools-and-templates/privacy-policy-template

© TAFE Queensland 2020

Business processes, procedures, and standards

Processes, procedures, and standards explain how you want an organisation to operate.

For example, a retail or hospitality business may want to:

- put a process in place to achieve sales
- create mandatory procedures for staff that are opening and closing the business daily
- set a standard (policy) for staff clothing and quality of customer service.

Benefits of processes, procedures, and standards

Developing processes, procedures and standards is particularly important if you are in the early stages of establishing a business, or when you are trying to rebuild or grow a business that has been underperforming.

Business processes, procedures and standards are vital for training staff and induction programs, as well as formal processes like staff performance reviews.

1319975300 / Trueffelpix / shutterstock.com

 © TAFE Queensland 2020

Processes and procedures

Having formalised processes and procedures for an organisation can save you time and money by increasing efficiency. Staff can get more done in less time by following set processes and procedures, and you can spend less time overseeing the day-to-day running of the organisation.

Processes and procedures can also improve the consistency of product and service delivery by the organisation's staff.

Standards and policies

By creating standards and policies for an organisation, you set benchmarks that the staff must meet.

For example, you may have a standard for serving customers that involves being courteous, completing transactions within a certain time, and doing everything in your power to accommodate customer requests. This can improve the experience of the organisation's customers, suppliers and/or distributors in their dealings with you.

Customers who have a positive experience are more likely to become repeat customers and are less likely to complain about the organisation.

Standardising key business activities

It's important to create processes, procedures, and standards for key business activities. Depending on the organisation's business, these may include:

- customer service (including a customer service program and after-sales service)
- sales practices and sales policies (e.g. guarantees, warranties and refunds)
- marketing and promotion (including online marketing and social media)
- staff training and performance reviews
- energy efficiency and environmental considerations (e.g. water restrictions)
- management responsibilities
- record keeping, privacy laws, reporting and money management
- use of technology (e.g. rules around staff internet usage) and mobile phones.

 © TAFE Queensland 2020

Creating effective processes, procedures, and standards

In order for all of your organisation's processes, procedures, and standards to be effective, they must be:

- documented (e.g., it's a good idea to create a 'standard operating procedures' manual)
- grounded in the vision and strategy of your business and aligned to your values
- clear about general organisations business procedures as well as role-specific procedures
- part of your staff training program, and made available in a user-friendly format afterwards (e.g., on paper or electronically as a PDF)
- practiced by management, so other staff will follow their lead
- discussed regularly in meetings (including positive and negative feedback)
- open to improvement
- designed to empower and inform, rather than constrain staff
- regularly reviewed and updated (especially due to legislative or compliance changes that affect your business).

© The State of Queensland 2021, 'Business processes, procedures and standards', https://www.business.qld.gov.au/starting-business/planning/business-planning/processes-procedures-standards?cv=1, 07/05/2021, CC BY 4.0

Example

As with policy templates there are no standardised templates used to create a procedure document. Here is a link to a web site that covers numerous simple templates for a variety of situations:

Policies-procedures and templates[3]

Weblink

The following web link contains a broad discussion about policy – what it is and how we use it.

Writing policy and organisational manuals[4]

[3] https://business.vic.gov.au/tools-and-templates/privacy-policy-template

[4] http://www.mapl.com.au/policy/tp1.htm

Updating policies

A policy document clearly states an organisation's intentions. In the case of code of ethics policy, this is a set of statements about appropriate and expected behaviour of members of a company or a professional group, and as such, reflects the values of the company.

Copyright, intellectual property, privacy, and a code of ethics policy should be written and updated to incorporate any relevant legislation and industry standards.

Note

As mentioned previously, copyright and intellectual property must have alignment with the laws and legislations. In business, the word **alignment** is used to describe the process of developing systems to specifically support the needs of the company.

Example

We design a new website to address the clearly defined business needs of the company. By doing this, the organisation can make sure that the resources that go into deploying technology will be effective in helping the company meet its goals.

Below are examples of alignment between policy and legislation.

- **Policy statements** – These restate legislation in plain English.
- **Policy directives** – Clarify how the laws apply in the company's environment.
- **Policies** – Explicitly express legislative mandates as preferred behaviour for staff members.

544464544 / designtools / shutterstock.com

 © TAFE Queensland 2020

Distributing policies

Policies and procedures should be made available to all employees of the organisation and other stakeholders.

Policy and procedure documents are usually a matter of public record and signify that the company understands the importance of privacy, copyright, intellectual property, and ethical behaviour in their industry and the relevance of legislation and industry standards to the development of these policies.

Activity

Consider some of the ways that you could make a code of ethics available to the employees in a medium size organisation:

- What technologies could be used?
- How would you inform employees of the existence of the code of ethics?
- How would you make sure that they have read it?

1460101262 / William Potter / shutterstock.com

© TAFE Queensland 2020

Topic summary and review

This topic covered the knowledge and skills needed to understand policy and procedure documents for an organisation.

Self-check – Policies and procedures

Identify two benefits of having workplace policies.

- ☐ Clarify functions and responsibilities
- ☐ Identifies correct wage levels
- ☐ Fosters stability
- ☐ Discount codes for online purchases

In business, the word alignment is used to describe the process of developing systems to support needs of the company.

- ☐ True
- ☐ False

SOP is an acronym for?

- ☐ Systems Officer Programming
- ☐ Standard Operating Procedures
- ☐ Simply Off Putting
- ☐ Standard Offset Policy

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

Legislation standards and policies

Introduction

In all civilised democracies laws and regulations are developed for the good of its citizens. These laws include the way that an individual's sensitive information is handled by organisations. This topic looks at the Privacy Act in regard to the responsibilities of organisations and the rights of individuals. The topic also covers the areas of the ISO 27001 standards, NIST aims and where to access international legislation.

Objectives

By completing this topic, you will be able to:

- understand the principles of the Privacy Act 1988
- understand the rights and responsibilities of organisations
- recognise the Australian Privacy Principals
- identify notifiable breaches in regard to privacy
- summarise the Information Privacy Act 2009 (QLD)
- know what the ISO 27001 is
- demonstrate an awareness of the National Institute of Standards and Technology
- understand the importance of international legislation.

338053589 / Zerbor / shutterstock.com

 © TAFE Queensland 2020

Privacy Act 1988

The Privacy Act 1988 (Privacy Act) is a way to protect the privacy of individuals and to control how Australian Government agencies and organisations, and some other organisations, handle personal information.

The Australian Government agencies and organisations that are governed by the act will have an annual turnover of more than $3 million.

Weblink

For the full text of the Privacy Act 1988, below is the link to the Australian Government, Federal Register of Legislation web site:

Privacy Act 1988 (legislation.gov.au)[5]

Video

To learn more about the privacy act view the video by Go To Court Lawyers.

Privacy Law in Australia[6]

730538191 / Vitalii Vodolazskyi / shutterstock.com

[5] https://www.legislation.gov.au/Details/C2021C00139

[6] http://www.youtube.com/embed/MQc-UjE560A?rel=0

 © TAFE Queensland 2020

Rights and responsibilities

Who has rights under the Privacy Act?

The Privacy Act regulates the way individuals' personal information is handled. As an individual, the Privacy Act gives you greater control over the way that your personal information is handled. The Privacy Act allows you the rights shown below.

- Understand why your personal information is being accumulated, how it will be used and who it will be revealed to.
- Have the option of not identifying yourself, or of using an alias in certain situations.
- Request for access to your personal information (including your health data).
- Stop getting unsolicited direct marketing.
- Ask for your personal information that is inaccurate to be rectified.
- Make a complaint about an organisation or agency the Privacy Act covers, if you believe they have mismanaged your personal information.

Who has responsibilities under the Privacy Act?

Australian Government agencies (and the Norfolk Island administration) and organisations with an annual turnover more than $3 million have responsibilities under the Privacy Act, with certain exceptions.

Office of the Australian Information Commissioner, 'Rights and Responsibilities', https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities, 08/02/2022, CC BY 3.0

364995272 / Gustavo Frazao / shutterstock.com

Read below to learn the definition of an organisation and to understand which small businesses are covered by the act.

What is an organisation?

The Privacy Act defines an ‘organisation’ as:

- an individual, including a sole trader (though generally, the Privacy Act does not apply to an individual acting in a personal capacity)
- a body corporate
- a partnership
- any other unincorporated association, or a trust.

Small businesses covered.

The Privacy Act covers some small business operators (organisations with an annual turnover of $3 million or less), including:

A private sector health service provider — an organisation that provides a health service includes:

- a traditional health service provider, such as a private hospital, a day surgery, a medical practitioner, a pharmacist, and an allied health professional
- a complementary therapist, such as a naturopath and a chiropractor
- a gym or weight loss clinic.

The act also covers:

- a childcare centre, a private school, and a private tertiary educational institution
- a business that sells or purchases personal information
- a credit reporting body
- a contracted service provider for an Australian Government contract
- an employee association registered or recognised under the Fair Work (Registered Organisations) Act 2009
- a business that holds accreditation under the Consumer Data Right System
- a business that has opted-in to the Privacy Act
- a business that is related to a business that is covered by the Privacy Act
- a business prescribed by the Privacy Regulation 2013.

 © TAFE Queensland 2020

Reading

Go to the website of the Office of the Australian Information Commissioner using this link. Please read or listen from the top of the page to the bottom (Privacy laws applying to ACT public sector agencies).

Rights and Responsibilities[7]

[7] https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities

© TAFE Queensland 2020

Australian privacy principals

Australian privacy principles guidelines

The Australian Privacy Principles (APP) guidelines outline the mandatory requirements of the APPs, how we will interpret the APPs, and matters we may consider when exercising our functions and powers under the Privacy Act 1988 (Privacy Act).

Both the APPs and the APP guidelines apply to any organisation or agency the Privacy Act covers. The Privacy Act covers Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations.

Reading

Download the complete Australian Privacy Principles guidelines

Australian Privacy Principles guidelines-pdf download[8]

Weblink

View the online version of the Australian Privacy Principles guidelines by accessing following webpage.

Privacy Principles guidelines[9]

369815300 / Jirsak / shutterstock.com

[8] https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf

[9] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/

© TAFE Queensland 2020

The Australian Privacy Principles guidelines cover the following areas:

- Key concepts.
- Permitted general situations.
- Permitted health situations.
- Open and transparent management of personal information.
- Anonymity and pseudonymity.
- Collection of solicited personal information.
- Dealing with unsolicited personal information.
- Notification of the collection of personal information.
- Use or disclosure of personal information.
- Direct marketing.
- Cross-border disclosure of personal information.
- Adoption, use or disclosure of government related identifiers.
- Quality of personal information.
- Security of personal information.
- Access to personal information.
- Correction of personal information.

Office of the Australian Information Commissioner, 'Privacy Principles',
https://www.oaic.gov.au/privacy/australian-privacy-principles, 22/04/2021, CC BY 3.0

Notifiable breaches

Data breaches

A data breach happens when personal information is accessed, disclosed without authorisation, or is lost. Under the notifiable data breaches scheme, you must be told if a data breach is likely to cause you serious harm.

In the reading panel below there are three links to the Office of the Australian Information Commissioner (OAIC) website. The links contain the following content.

- What is a data breach?
- What is a notifiable data breach?
- How you will be told of a data breach.
- If you think you have not been told about a data breach.
- How to spot a phishing scam.
- Civil penalties for data breaches.

405302020 / Rawpixel.com / shutterstock.com

 © TAFE Queensland 2020

Reading

Access these 3 sections of the Office of the Australian Information Commissioner website.

Read each individual page.

What is a data breach?[10]

What is a notifiable data breach?[11]

For the link below, read footnote 1 to see the value of a penalty unit.

Civil Penalties[12]

[10] https://www.oaic.gov.au/privacy/data-breaches/what-is-a-data-breach

[11] https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach

[12] https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties#ftn1

© TAFE Queensland 2020

Information Privacy Act 2009 (QLD)

In Queensland, the state government implement the privacy legislation called the "Information Privacy Act 2009". The Act is designed to cover public service organisations in the state of Queensland.

The objects of the IP Act are:

- the fair collection and handling of personal information in the public sector environment
- to provide a statutory right for individuals to access and amend their personal information held by entities in the public sector environment.

The meaning of personal information

"Personal information" is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

© The State of Queensland (Office of the Information Commissioner) 2012, 'What is personal information?', https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/introduction-to-the-acts/what-is-personal-information, 09/03/2022 CC BY 3.0

Weblink

Access this link for the complete Information Privacy ACT 2009 – As of 1 July 2019 – Act 14 of 2009

Queensland Consolidated Acts[13]

1853752201 / RDK03 / shutterstock.com

[13] http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/qld/consol_act/ipa2009231/

ISO 27001

ISO 27001, also known as ISO/IEC 27001, presents the requirements for an information security management system (ISMS).

1190236807 / Trueffelpix / shutterstock.com

The ISO/IEC 27000 family

In the ISO/IEC 27000 family there are over a dozen standards. Applying these standards will facilitate organisations of any kind to manage the security of resources such as intellectual property, financial information, employee details or information entrusted by third parties.

What is Iso 27001?

The ISO/IEC 27001:2013 standard stipulates the requirements for establishing, implementing, maintaining, and continually developing an information security management system within the framework of the organisation.

Risk management

The ISO/IEC 27001:2013 standard additionally includes requirements for the appraisal and management of information security risks customised to the needs of the organisation. The requirements set out in the ISO/IEC 27001:2013 standard are universal and are intended to be applicable to all organisations, irrespective of type, size, or type.

1794926494 / Song_about_summer, 1428961169 / Photo Veterok, 1908323875 / Titima Ongkantong / shutterstock.com

© TAFE Queensland 2020

Weblink

Review of the ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27001-2013[14]

[14] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

© TAFE Queensland 2020

NIST

What is the NIST?

Founded in 1901, the National Institute of Standards and Technology (NIST) is now part of the United States Department of Commerce; they are one of the USA's oldest physical science laboratories. The United States Congress created the agency to remove a serious challenge to U.S. industrial effectiveness at the time, which was a mediocre measurement infrastructure that trailed behind the abilities of Germany, the United Kingdom, and other economic competitors.

Nowadays, NIST measurements provide for the smallest of technologies to the largest and most complicated of human-made innovations. From nanoscale mechanisms so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant buildings and worldwide communication networks.

Video

To learn more about the history of the NIST view the video.

NIST Illustrated[15]

1909114186 / grandbrothers / shutterstock.com

[15] http://www.youtube.com/embed/2j9BGVKbzS4?rel=0

© TAFE Queensland 2020

The Privacy Framework

The NIST Privacy Framework is a voluntary tool developed in cooperation with stakeholders intended to help organisations to develop privacy guidance, tools, and international standards.

Video

The link below gives a detailed overview of the Privacy Framework

The NIST Privacy Framework[16]

NIST has released their version 1 of the Privacy Framework, known as “NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management”. As the title suggests it is a tool to help enhance positive uses of data while protecting individual privacy. The following two links are the NIST web page that gives an overview of the document, and a link to the document itself.

Weblink

Access the link below to see a document overview.

NIST Releases Version 1.0 of Privacy Framework[17]

Access the link below to see the entire document.

NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0[18]

[16] http://www.youtube.com/embed/izdDPlEmhJc?rel=0

[17] https://www.nist.gov/news-events/news/2020/01/nist-releases-version-10-privacy-framework

[18] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

 © TAFE Queensland 2020

Guides

NIST has also developed a number of guides, such as the 'Quick-Start' Guide for Its Security and Privacy Safeguards Catalogue, full title being: "Control Baselines for Information Systems and Organizations".

Weblink

Access the weblink below for more detail.

NIST Offers 'Quick-Start' Guide for Its Security and Privacy Safeguards Catalogue[19]

Developments

NIST has a wide range of developments occurring in a broad range of fields, including Information Technology. Some areas, such as privacy, are helping in others, such as helping to slow down future pandemics. To read about news of this development, follow this web link.

Weblink

To read news of this development, access this web link.

NIST Develops Privacy-Preserving 'Encounter Metrics' That Could Help Slow Down Future Pandemics[20]

[19] https://www.nist.gov/news-events/news/2020/10/nist-offers-quick-start-guide-its-security-and-privacy-safeguards-catalog

[20] https://www.nist.gov/news-events/news/2021/03/nist-develops-privacy-preserving-encounter-metrics-could-help-slow-down

© TAFE Queensland 2020

International legislation

There are numerous countries that have privacy laws, however, there are also numerous countries that do not. Those countries that have weak or no privacy laws at all are normally based in despotic or totalitarian government systems.

The United Nations Conference on Trade and Development (UNCTAD) has a tool called Global Cyberlaw Tracker that offers global mapping of cyberlaws. At the time of writing, 66% of countries had legislation for data protection and privacy, while 19% had none. The other percentages were 10% in draft, and 5% with no data.

Although 66% of countries have a form of privacy legislation, the strength of the legislation will vary depending on the freedom of democracy they enjoy.

Weblink

Visit the link below to explore a global picture of data protection and legislation.

UNCTAD – Data Protection and Privacy Legislation Worldwide[21]

1091235845 / Alexandros Michailidis / shutterstock.com

[21] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

 © TAFE Queensland 2020

Another great web site to visit that not only is dedicated to protecting the privacy rights of Australians, but also provides information and links to the privacy laws of approximately 30 countries, is the Australian Privacy Foundation.

Weblink

For a full list and details of privacy laws by country visit the website below. Select a country to learn more.

Australian Privacy Foundation – Privacy Laws of the World[22]

[22] https://privacy.org.au/resources/privacy-law/plawsworld/

© TAFE Queensland 2020

Topic summary and review

This topic covered the knowledge and skills needed to understand the Privacy Act and the Act's components. The topic also covered the rights and responsibilities of organisations and the different legislation apart from the Privacy Act.

Self-check – Legislation standards and policies

In which year was the Privacy Act enacted?

- ☐ 1984
- ☐ 1988
- ☐ 1996

The Queensland Information Privacy Act 2009 covers all businesses in Queensland.

- ☐ True
- ☐ False

Which ISO 27001 standard includes the appraisal and management of information security risks?

- ☐ ISO/IEC 27001:2013
- ☐ ISO/IEC 27001:2015
- ☐ ISO/IEC 27002:2013

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

Company privacy policies

Introduction

All good organisations will have some form of company privacy policy. This makes sure that everyone involved with the organisation has the same ideas and principles. This topic looks at what a privacy policy is, and the way personal information is handled within the organisation. The topic will also look at areas such as storage of personal information and how privacy affects the organisation's website.

Objectives

By completing this topic, you will be able to:

- understand what a privacy policy is
- understand the collection of personal information
- know the parameters of the use and disclosure of personal information
- understand the control and rights of a customer's personal information
- understand the security and storage of personal information
- understand websites –cookies and third-party sites consent clauses.

1778936321 / TierneyMJ / shutterstock.com

 © TAFE Queensland 2020

Privacy policy

The purpose of a company policy is to provide guidance on how the organisation classifies, labels, and restricts access to, sensitive data. If your organisation, business, or company collects personal information data online or directly from your customers, you must use a privacy policy. By law you are required to have a privacy policy if your business falls within one of the conditions set out in the Privacy Act 1988.

Select the buttons below to see other names you will see used for privacy policies and the items a privacy policy should cover.

Names

A privacy policy may come under other names.

- Use of private and confidential information policy.
- Responsible Use of Data Policy.
- Privacy policy agreement.
- Website privacy policy.

Cover

A privacy policy should cover the topics listed below.

- Collection of personal information.
- Disclosure of personal information.
- How personal information is used.
- Control and rights of a customer's personal information.
- Security and storage of personal information.
- For websites – cookies and third-party sites consent clauses.

489852166 / Rawpixel.com/ shutterstock.com

 © TAFE Queensland 2020

Weblink

For more information on creating a privacy policy visit the links below.

Lawpath, Privacy Policy[23]

Legal123, How to Write a Privacy Policy for Your Website[24]

[23] https://lawpath.com.au/legal-documents/privacy-policy

[24] https://legal123.com.au/how-to-guide/privacy-policy-australia/

 © TAFE Queensland 2020

Collection of personal information

Organisations and agencies sometimes need personal information about you to carry out their work. Australian privacy law sets out what personal information they can collect and what they need to tell you.

An organisation may only collect your personal information that is reasonably necessary for their work. An agency may only collect your personal information that is related to their work. They do not need your consent unless the information is sensitive.

Office of the Australian Information Commissioner, 'Collection of personal information', https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/collection-of-personal-information, 26/04/2021, CC BY 3.0

Reading

For more about this important topic, read the resources from the Office of the Australian Information Commissioner, particularly **How can an organisation or agency collect personal information?**

'Collection of personal information'[25]

Also, read the following chapters from the OAIC **Australian Privacy Principles guidelines**

Chapter 3: APP 3 - Collection of personal information[26]

Chapter 4: APP 4 - Dealing with unsolicited personal information[27]

[25] https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/collection-of-personal-information#:~:text=An%20organisation%20may%20only%20collect,unless%20the%20information%20is%20sensitive

[26] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information

[27] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information

 © TAFE Queensland 2020

1751753813 / alexkich / shutterstock.com

Important

For more information, see the APP Guidelines, Chapter 5.

Notification of the collection of personal information[28]

[28] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information/

© TAFE Queensland 2020

Use and disclosure of personal information

Australian privacy law allows an organisation or agency to use or disclose your personal information for the reason they collected it (the primary purpose), including for direct marketing activities.

An organisation or agency cannot use or disclose your personal information for another reason (a secondary purpose) unless an exception applies. See below to learn more about exceptions.

- **Consent** – You have consented to an organisation or agency using or disclosing your personal information for a secondary purpose.
- **Necessity** – An organisation or agency uses or discloses your personal information because they think it is reasonably necessary for enforcement-related activities carried out by, or on behalf of, an enforcement body.
- **Secondary purpose** – A secondary purpose is required or authorised under an Australian law, or court or tribunal order.

1344677786 / HelloRF Zcool / shutterstock.com

 © TAFE Queensland 2020

Another point to be aware of is when an agency or organisation is ‘using’ or ‘disclosing’ your personal information. Read below for more detail on this important distinction.

Using

An organisation or agency is ‘using’ your personal information if they control how the information is handled. For example, if they:

- search their records for your personal information
- access and read the personal information they hold about you
- make a decision based on the personal information they hold about you
- pass your personal information from one part of the organisation or agency to another.

An organisation or agency is even using your personal information if an employee without authority accesses it while doing their work duties.

Disclosing

An organisation or agency discloses your personal information if they give access to it, or show it to another individual, organisation or agency. This includes situations where the individual, organisation or agency receiving your personal information already knows it.

Office of the Australian Information Commissioner, ‘Use and disclosure of personal information’, https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/use-and-disclosure-of-personal-information, 26/04/2021, CC BY 3.0

Control and rights of a customer's personal information

This information has already been covered previously under the section 'Legislation, Standards and Policies – Privacy Act 1988'.

Who has rights under the Privacy Act?

The Privacy Act regulates the way individuals' personal information is handled.

As an individual, the Privacy Act gives you greater control over the way that your personal information is handled. The following are the things you can do under the Privacy Act to manage your personal information.

- You can know why your personal information is being collected, how it will be used and who it will be disclosed to.
- Have the option of not identifying yourself, or of using a pseudonym in certain circumstances.
- Ask for access to your personal information (including your health information).
- Stop receiving unwanted direct marketing.
- Ask for your personal information that is incorrect to be corrected.
- Make a complaint about an organisation or agency the Privacy Act covers, if you think they have mishandled your personal information.

Office of the Australian Information Commissioner, 'Who has rights under the privacy act?', https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities, 26/04/2021, CC BY 3.0

203407133 / Olivier Le Moal / stock.adobe.com

 © TAFE Queensland 2020

Security and storage of personal information

Securing personal information is one of the most critical processes that needs to be implemented today in this world of numerous malicious players.

The Office of the Australian Information Commissioner has released a guide for securing personal information and the following is the introduction on the OAIC website.

Reading

Access the link below and read the 'Introduction' section from the Guide to securing personal information. You can also access a PDF version from the webpage.

Guide to securing personal information[29]

[29] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information

© TAFE Queensland 2020

For websites – cookies and third-party sites consent clauses

Should my privacy policy include ‘cookies’? – Yes

A business privacy policy should include a ‘cookie’ notification section if you are gathering information via a web site.

What is a ‘cookie’? A ‘cookie’ is a small file located in your web browser that gathers data about your web browsing behaviour. Even though ‘cookies’ do not access information stored on your computer or anything personal, they do allow collection of identifiable information. Use of ‘cookies’ allows a website to customise its structure to your needs and likings, as well as possibly serve ads to you while you are browsing the internet.

If you have a website that collects personal information, you need to state the way in which the information is collected.

97896980 / faithie / stock.adobe.com

 © TAFE Queensland 2020

Web analytics

Businesses will use a web analytics application to collect data about your interaction with their website. The sole purpose of collecting personal data in this way is to improve the users experience when visiting the site. The following are the type of information collected.

- Your device's IP address (collected and stored in an anonymised format).
- Device screen size.
- Device type, operating system, and browser information.
- Geographic location (city).
- Referring domain and out link if applicable.
- Search terms and pages visited on the website.
- Date when pages were accessed on the website.
- Time when pages were accessed on the website.

Note

If your web browser has Do Not Track enabled, the web analytics application will not track your visit. The web analytics application has to be hosted within Australia, if hosted overseas the third-party must guarantee the same privacy conditions that are met by Australian law.

Office of the Australian Information Commissioner, 'Privacy policy', https://www.oaic.gov.au/about-us/our-corporate-information/key-documents/privacy-policy, 26/04/2021, CC BY 3.0

© TAFE Queensland 2020

Email lists, registrations, and feedback

A business will collect information that is provided to them when a user signs up to mailing lists, registers for events, or when submitting feedback on their experience with the business's website. There are applications that manage mailing lists and event registrations. These application vendors will also have a privacy policy that should be linked.

When subscribing to a mailing list, you will be asked to give your express consent that the managing application may use your data for analytics purposes. Analytics are performed when you click on links in the email, or when you download the images in the email. This includes which emails you open, which links you click, your mail client (e.g., 'Outlook" or 'iPhone'), if the action occurred on 'mobile' or 'desktop', and the country geolocation of the IP address (the IP address itself is not stored).

When registering for an event, you may be required to give booking application personal information, including your name, address, telephone number and email address. You may also be required to provide financial information, including credit card number and expiration date if you make a payment for an event. The booking application may share some of your personal information, including information about whether a particular registered individual has made payment, but should not receive your financial information.

A feedback application is used to conduct anonymous stakeholder surveys to gather feedback to help the business improve their performance. Information about how the feedback application manages personal information should be available in the privacy and data collection policies on their website.

293673522 / Ivelin Radkov, 283750165 / Artur, 129754549 / STOATPHOTO / shutterstock.com

© TAFE Queensland 2020

Topic summary and review

This topic covered the knowledge and skills needed to understand the privacy policies within an organisation and the requirements for collection, use, and disclosure of personal information. Other areas in this topic were understanding the security and storage of personal information and websites.

Self-check – Company privacy policies

The Privacy Act allows an individual to? Select the correct option/s.

- ☐ Have the option of not identifying yourself, or of using a pseudonym in certain circumstances.
- ☐ Ask for access to their personal information (including health information).
- ☐ Stop receiving unwanted direct marketing.
- ☐ All the above.

A Privacy Policy could also be known as a Responsible Use of Data Policy?

- ☐ True
- ☐ False

The Office of the Australian Information Commissioner has released a guide for securing personal information called?

- ☐ Guide to securing personal information – Reasonable steps to protect personal information.
- ☐ Guide to securing personal information – The step-by-step to protect personal information.
- ☐ Guide to securing personal information – 'Nearly all steps' to protect personal information.

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

Copyright

Introduction

Copyright is an issue for any person or organisation that develops any original work. This can be from a person writing a poem, an organisation developing a new web site, or even this learning material.

Without the protection of copyright, the people and organisations that develop their original work would not do so because of the loss or prestige, recognition, and in lots of cases financial income.

Objectives

Key concepts for this topic:

- laws surrounding copyright
- what does copyright protect
- granting and getting copyright permission
- protecting copyright
- information on the web site for permission
- types of media file copyright
- particular problems obtaining copyright permissions
- copyright clearance.

In addition to the material provided you will also need to spend some time on further research of these concepts.

47334346 / Kheng Guan Toh / shutterstock.com

 © TAFE Queensland 2020

What is copyright?

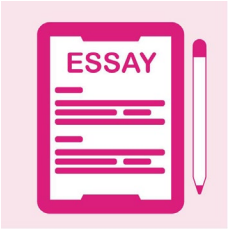
Copyright is defined as the exclusive rights of the creator of an original work to copy, adapt and distribute the created work. Copyright does not protect the idea only the expression of that idea.

> *"Copyright provides creators with an incentive to create new works and a legal framework for the control of their creations."* – Australian Copyright Council.

Copied Under s113P https://www.copyright.org.au/browse/book/ACC-An-Introduction-to-Copyright-in-Australia-INFO010, 29/07/2021

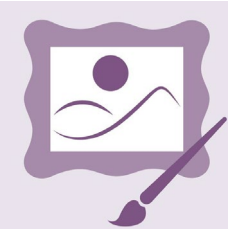
362281055 / FR Design / stock.adobe.com

Copyright works are created all the time. See the examples below. A copyright work is created any time any of these activities are undertaken.



An essay is written

A report is created



A painting is made

A picture is taken

An audio is recorded

A video recording is made

© TAFE Queensland

Copyright is usually owned by the person who created that work, however in the case of work that is produced for an employer that work is usually copyrighted to the employer.

> Australian Copyright Council "Our Mission"
>
> *The Australian Copyright Council is an independent, non-profit organisation. Founded in 1968, we represent the peak bodies for professional artists and content creators working in Australia's creative industries and Australia's major copyright collecting societies.*
>
> *We are advocates for the contribution of creators to Australia's culture and economy, the importance of copyright for the common good. We work to promote understanding of copyright law and its application, lobby for appropriate law reform and foster collaboration between content creators and consumers.*
>
> Copied Under s113P, https://www.copyright.org.au/about_us, 22/04/2021

Reading

The following web page from the Australian Copyright Council has links to the following documents. Alternatively, use the search function to find what you need. It is a great resource.

- An Introduction to Copyright in Australia
- Protecting Your Copyright
- Ownership of Copyright
- Infringement: What Can I Do?

Australian Copyright Council[30]

[30] https://www.copyright.org.au/search?page=1&keyword=an%20introduction%20to%20copyright

 © TAFE Queensland 2020

The Copyright Act 1968

In Australia, the Copyright Act 1968 is the law that governs copyright. In 2000 in Australia the Copyright Amendment (Digital Agenda) Act 2000 was also introduced to better serve the needs of the online environment. In 2006 the Copyright Amendment Bill 2006 was also passed with several aims including:

- providing stronger rights for copyright owners
- providing exceptions for consumers to enjoy some copyright material in certain circumstances
- providing some exceptions for the use of copyright material for socially useful purposes.

Since 2006 there has been an additional 3 amendments and a regulation attached to the Act. These include:

- Copyright Amendment (Disability Access and Other Measures) Act 2017.
- Copyright Amendment (Online Infringement) Act 2018.
- Copyright Amendment (Service Providers) Act 2018.
- Copyright Regulations 2017.

Reading

You can access all these Acts and regulations at the link below.

https://www.legislation.gov.au/Search/copyright[31]

431834837 / Yurii Kibalnik / stock.adobe.com

[31] https://www.legislation.gov.au/Search/copyright

© TAFE Queensland 2020

Duration of copyright

Copyright in Australia is automatic on creation of the work and in general the work is then protected by copyright for a period of 70 years after the end of the year of the creator's death, or 70 years from the end of the year the material was first made public.

Weblink

There are some exceptions to the above rule, for a full explanation refer to the fact sheet "Duration of Copyright" at the following link.

Australian Copyright Council-Duration of copyright[32]

[32] https://www.copyright.org.au/search?page=1&keyword=duration%20of%20copyright

 © TAFE Queensland 2020

What does copyright protect?

In general copyright protects such things as writing, music, dramatic works, both still and moving images, computer programs and recorded sounds. The following are examples reproduced from the Australian Copyright Council. This is a comprehensive list of what is covered, as well as examples of the type of work.

281542322 / robuart / shutterstock.com

Type of works	What is covered
Textual material	Literary works such as journal articles, novels, screenplays, poems, song lyrics and reports.
Computer programs	A sub-category of 'literary works'.
Compilations	Another sub-category of 'literary works', such as anthologies – the selection and arrangement of material may be protected separately from the individual items contained in the compilation.
Artistic works	Such as paintings, drawings, cartoons, sculpture, craft work, architectural plans, buildings, photographs, maps, and plans.
Dramatic works	Such as choreography, screenplays, plays and mime pieces.
Musical works	That is, the music itself, separately from any lyrics or recording.
Cinematograph films	The visual images and sounds in a film, video or DVD are protected separately from any copyright in works recorded on the film or video, such as scripts and music.
Sound recordings	The particular recording itself is protected by copyright, in addition to, for example, the music or story that is recorded.
Broadcasts	TV and radio broadcasters have a copyright in their broadcasts, which is separate from the copyright in the films, music, and other material which they broadcast.
Published editions	Publishers have copyright in their typographical arrangements, which is separate from the copyright in works reproduced in the edition (such as poems or illustrations or music).

Copied Under s113P https://www.copyright.org.au/search?page=1&keyword=an%20introduction%20to%20copyright, 22/04/2022

© TAFE Queensland 2020

How to get permission

Unlike the systems for trademarks, patents and designs, there is no Australian registration system for copyright, so there are no official records of ownership that you can search. For this reason, you may need to use a variety of resources when looking for copyright owners. In some cases, you may need to do some detective work.

The following are some important points about copyright ownership.

- **Ownership** – The owner of a physical item does not necessarily own copyright in that item. For example, a gallery or museum does not necessarily own copyright in items in its collection.
- **Permission** – The Copyright Act does not allow you to use material without permission if you cannot contact the copyright owner. If you use a substantial part of copyright material without permission, you will infringe copyright, unless an exception to infringement applies.
- **Creator** – The creator of copyright material is not always the copyright owner.
- **Death** – If copyright is owned by an individual who has died, ownership may have passed to someone else – usually the copyright owners spouse or children. If a company owned copyright and it has now gone out of business, its assets, which include copyrights, may have been distributed elsewhere.
- **Moral rights** – As well as clearing copyright, you need to ensure you do not infringe the creator's moral rights.

470247834 / Andrey Popov / stock.adobe.com

 © TAFE Queensland 2020

Where to start

It is a good idea to check whether there is a licence available from a copyright collecting society that covers your intended use. If no licence is available, the appropriate collecting society may nevertheless be able to assist (sometimes for a fee) in finding the copyright owner.

Often you can get information about how to contact the copyright owner from the material you want to use. Copyright notices that appear on CDs and on the imprint page of books usually name the owner of copyright and sometimes give contact details.

If you know that the material has been used by someone else (for example, it has been reproduced in a book) it may be worth contacting that person or organisation for information about where they obtained permission.

Copied Under s113P, Australian Copyright Council, 2019, Information Sheet G051v15 – Permission: How To Get It, Australian copyright council, pgs 1-2.

Weblink

If you wish to use written material in which a state, territory or Commonwealth government owns copyright, find out more at this link

Government: Commonwealth, State and Territory[33]

For information on exceptions to infringement that may allow you to use written material without permission see the links below.

Quotes and Extracts[34]

Fair Dealing: What Can I Use Without Permission[35]

---

33 https://www.copyright.org.au/ACC_Prod/ACC/Information_Sheets/Government__Commonwealth__State___Territory.aspx?WebsiteKey=8a471e74-3f78-4994-9023-316f0ecef4ef

34 https://www.copyright.org.au/search?page=1&keyword=quotes%20and%20extracts

35 https://www.copyright.org.au/ACC_Prod/ACC/Information_Sheets/Fair_Dealing__What_Can_I_Use_Without_Permission.aspx?WebsiteKey=8a471e74-3f78-4994-9023-316f0ecef4ef

 © TAFE Queensland 2020

When acquiring resources for a website or social media there are a few categories of what these resources are:

- images
- video
- music
- text

Obtaining permission for any of these can sometimes be a nightmare, with resources showing no references to the author, nor any contact details on the web site where the resource appears.

Weblink

For more information on getting permission, visit the link below.

Permission: How to get it[36]

[36] https://www.copyright.org.au/browse/book/ACC-Permission:-How-To-Get-It-INFO051

 © TAFE Queensland 2020

Information on the web site for permission

When searching for use of resources from a web site it is best to check either the 'Copyright' or 'Terms and Conditions' links normally located on the bottom of the page. With most Australian Government web sites, being state or federal, copying of text and most images are free for use but do contain caveats.

Government and non-government websites usually take different approaches to copyright.

26982999 / Orlando Florin Rosu / stock.adobe.com

Government

Normally a government web site will carry the following information.

The Commonwealth owns the copyright in all material produced by this department.

All material presented on this website is provided under a Creative Commons Attribution 4.0 International[37] – external site licence, with the exception of:

- the Commonwealth Coat of Arms
- this department's logo
- content supplied by third parties.

The details of the relevant licence conditions are available on the Creative Commons - external site[38] website, as is the full legal code for the CC BY 4.0 license. See the links in the panel.

Weblink

Creative Commons - external site[39]

Attribution 4.0 International[40]

[37] https://creativecommons.org/licenses/by/4.0/

[38] https://creativecommons.org/licenses/by/4.0/

[39] https://creativecommons.org/licenses/by/4.0/

[40] https://creativecommons.org/licenses/by/4.0/legalcode

© TAFE Queensland 2020

Non-government

Non-government website

If the website has a copyright link it will take you to a page where the copyright will be explained. An example is:

Example

Copyright of all original material generated by contributors to the “organisation’s name” websites (with the exception of images) on this website is held by “organisation’s name”.

Copyright on all images on the website remain with the contributor.

You may download, display, print and reproduce written material in unaltered form for your personal, non-commercial use.

If our written material is used on a similar non-commercial website or social media page, then the “organisation’s name” websites must be acknowledged as the source

Use of information and/or images for commercial use must be obtained in writing from the “organisation’s name” before use, and the website acknowledged as the source.

All other rights reserved.

There will be numerous times where there is no copyright link on the page, however, a **terms and conditions** link may help with copyright. Most of the time the information will state that all copyright, trademarks, and content are the property of the said organisation.

Normally in the terms and conditions it will state limited use for private no-commercial use, and also to contact them for any clarification.

Important

If a web site has resources that you would like to use and there is no copyright information anyway, nor is there a way to contact the owner or website administrator, just do not use any of the resources.

Just because there is no way to verify the copyright does not mean you have permission to use the resources, because you do not.

 © TAFE Queensland 2020

Media files

Anytime that a person puts pen to paper, or takes a photo or a video, it automatically has copyright attached to it in Australia, as this is what is stated by the Copyright Act. This also applies to any text or media files you want to copy from any overseas source.

So, unless the source states that the owner of the text or media file gives you permission to use the resource, either by a statement on the web site or verification by email, then no permission is granted until a yes is confirmed.

Steps to take for permission

After you have noted the text or media files you would like to source, follow the simple steps below to seek permission if possible:

1. Locate if there is a Copyright link on the page. If so, this will state the type of rights for copying information. If not, move to the next step.
2. Locate if there is a Terms and Conditions link on the page. If so, read through the content and locate any statements in regard to the use or copying of resources on the web site. If nothing exists, or there is no Terms and Conditions link, move to the next step.
3. Locate if there in a Contact page link available. If so, contact the web page owner or administrator to enquire about the usage of their resources. If no Contact page is available, move to the next step.
4. See if there is a link available to either an administrator, or what we used to call the webmaster, or a link to the company that owns the site. You may be able to contact someone who can advise you on who next to contact in regard to gaining permission. If not, move to the next step.
5. Check to see if there is any embedded information in the digital material, such as metadata. Any information would help when you move to the next step.
6. At this point you may need to go outside of any web page link to the relevant authorities for some help. See below for more detail.
7. If you have got to this step without being able to obtain permission to use the resource, it may be best to cut your losses and seek other resources or build your own.

 © TAFE Queensland 2020

If you are having trouble finding the information you need, the following organisations may be able to help you.

Photos or visual art

You may be able to obtain a licence from Copyright Agency (with which Viscopy merged in 2017) for the reproduction of works of art from Australia or overseas from copyright.com.au.

Music and sound recordings

There may be separate copyrights in a sound recording – in the recording itself and in the music and lyrics on the recording. There are several organisations you may need to contact, depending on how you want to use music.

- The Australasian Mechanical Copyright Owners Society (AMCOS) and the Australasian Performing Right Association (APRA) may be able to help you find the owner of copyright in music, as they have extensive databases of rights holders.
- The Phonographic Performance Company of Australia (PPCA) and the Australian Record Industry Association (ARIA) may be able to help you find the record company that owns copyright in a sound recording you want to use.

Copied Under s113P, Australian Copyright Council, 2019, Information Sheet G051v15 – Permission: How To Get It, Australian Copyright Council, p1-2.

Important

Get your permission agreement in writing, or a screenshot of the agreement from the web page.

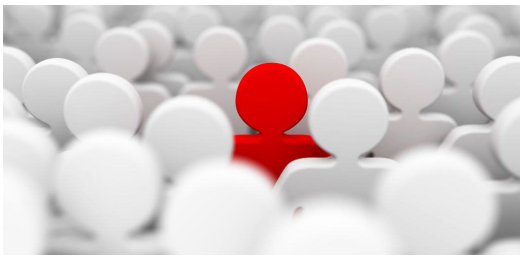
91096202 / CreativeAngela / shutterstock.com

Copyright – particular problems

Orphan works

The fact that you cannot identify or locate the copyright owner does not provide you with a legal defence to a claim of infringement.

We recommend that your organisation adopts an internal policy as to the circumstances in which it will use an orphan work where a clearance is needed. The policy should include the steps your organisation will take to mitigate the risks in using orphaned material.



77656587 / Leigh Prather / stock.adobe.com

Non-responsive copyright owners

If you need permission, the fact that a copyright owner does not respond does not mean that you can go ahead and use the material. You may decide to make a commercial decision to go ahead with your intended use, but in doing this you run the risk of being held liable for copyright infringement if the copyright owner brings an action against you.

490361127 / iQoncept / stock.adobe.com

Expensive or onerous licences

Copyright owners are generally free to set whatever licence terms and conditions they want. It then becomes a matter of trying to negotiate terms you are comfortable with. If the licence for the material you want to use is set by a collecting society, you may be able to challenge the licence conditions by applying to the Copyright Tribunal.

15816348 / Ashwin / stock.adobe.com

'Free' licences

Many copyright owners offer "free" licences to use their material, particularly where they make that material available on the internet. The most well-known example of such licences are the licences offered under Creative Commons.

Note, however, that many of these are still subject to conditions and to limits. Always read the terms and conditions carefully and ensure use will be within the scope of the licence. If you need a broader licence, contact the copyright owner.

161755849 / Brad Pict / stock.adobe.com

Copied Under s113P, Australian Copyright Council, 2019, Information Sheet G051v15 – Permission: How To Get It, Australian Copyright Council, p 5-7.

© TAFE Queensland 2020

Weblink

For more information visit these weblinks

Orphan works[41]

Creative Commons Licences[42]

[41] https://www.copyright.org.au/browse/book/ACC-Orphan-Works-INFO101

[42] https://www.copyright.org.au/ACC_Prod/ACC/Information_Sheets/Creative_Commons_Licences.aspx?WebsiteKey=8a471e74-3f78-4994-9023-316f0ecef4ef

 © TAFE Queensland 2020

Copyright clearance

Before using copyrighted resources, you will need to obtain copyright clearance for their intended use. Unfortunately, for these materials to be available copyright clearance must be obtained. Copyright clearance means that you have permission, ideally written, from the copyright holder to use the resource.

For commercially published resources, such as textbooks or magazines, it is unlikely that you will be able to obtain copyright clearance, because of the publishers' desire to be exclusive copyright holders and receive income generated from royalties.

When requesting copyright clearance, you need to be specific about which materials and how they will be used. You should also indicate that you are contacting them because you believe they are the copyright holder. See the following page to learn more about copyright clearance letters and client copyright clearance documents.

1803348466 / Blan-k / shutterstock.com

 © TAFE Queensland 2020

Clearance letters

Access the link below to see an example of a copyright clearance letter for an online course.

If this is a physical letter, include the date and a return address.

Weblink

Copyright clearance letter

Copyright clearance[43]

After sending out the copyright clearance letters, be prepared to wait. Organisations that are copyright holders will sometimes take a long time to respond to copyright clearance requests. Individuals, with the exception of very prominent ones, will usually respond within a few days (sometimes it can be as short as few minutes by e-mail). Some copyright holders will, unfortunately, not respond. In those situations, it is best to find alternate resources. Do not take a lack of response as copyright clearance.

WikiEducator 'Copyright clearance',
https://wikieducator.org/OER_Handbook/educator_version_one/License/Copyright_clearance?cv=1,
accessed 08/03/2022. CC BY 4.0

[43] https://wikieducator.org/OER_Handbook/educator_version_one/License/Copyright_clearance?cv=1

 © TAFE Queensland 2020

Clearance documents

It is best practice in a business to document that copyright clearance has been obtained and that it is signed off by an appropriate person. This appropriate person in most ways will be the client, as it will be their resources once a web site has been developed and commissioned.

Prior to having the client sign the copyright clearance you will need to explain the process you have gone through and the copyright licence that applies to each and every asset. This would best be done in a document that can be saved as a template for future client use and sections removed that are not applicable.

The copyright clearance information can be easily presented using a table where the information would be as follows. Example based on the image at the top of this section.

Content to Source Asset filename	**Description** Basic description of the asset	**Copyright Status** Type of copyright licence, holders and licence location.
1803348466.jpg	Set of 24 – vector format - assorted copyright protection icons (greyscale).	

To complete the document, you should also include a statement verifying that approval has been obtained from the client. The following information should be included:

- client organisation
- client name
- signature
- date.

WikiEducator 'Copyright clearance', https://wikieducator.org/OER_Handbook/educator_version_one/License/Copyright_clearance?cv=1, accessed 08/03/2022. CC BY 4.0

 © TAFE Queensland 2020

Topic summary and review

In this topic we have discussed the laws surrounding copyright and what does copyright protect. We also covered granting and getting copyright permission and protecting copyright.

Other topics covered were identifying information on the web site for permission and particular problems obtaining copyright permissions. The last part was understanding copyright clearance.

Self-check – Copyright

In Australia, the Copyright Act 1968 is the law that governs copyright.

- ☐ True
- ☐ False

The Copyright Act does allow you to use material without permission if you cannot contact the copyright owner.

- ☐ True
- ☐ False

Of the two (2) statements below, which one is correct?

- ☐ Unless the source states that the owner of the text or media file gives you permission to use the resource, either by a statement on the web site or verification by email, then no permission is granted until a yes is confirmed.
- ☐ After exhausting all avenues to identify and obtain permission from the copyright owner without success, you can contact and fill out the appropriate form to use the resource.

Before using copyrighted resources, you will need to obtain copyright clearance for their intended use.

- ☐ True
- ☐ False

Check your answers at the end of this Learner Guide

 © TAFE Queensland 2020

Intellectual property

Introduction

Intellectual property (IP) is the property of your mind or proprietary knowledge. It is a productive new idea you create. This can be an invention, trademark, design, brand or even the application of your idea.

Objectives

By completing this topic, you will be able to:

- understand what intellectual property is
- know the difference between IP rights and copyright
- understand the difference between patents, trademarks, design rights, and PBR.

418956310 / putilov_denis / stock.adobe.com

© TAFE Queensland 2020

What is Intellectual Property (IP)?

Intellectual property (IP) is the property of your mind or proprietary knowledge. It is a productive new idea you create. This can be an invention, trademark, design, brand or even the application of your idea.

Your idea must be something new or original, but determining whether your idea is new or not is not always easy. Applying for an IP right to protect your idea can be critical if you want to build a business and establish your presence in a market. As stated by Craig Venter, a geneticist and one of the first scientists to sequence the human genome, ‘intellectual property is a key aspect for economic development.’

599533328 / ibreakstock / shutterstock.com

 © TAFE Queensland 2020

Different IP rights and copyright

Some forms of IP require formal application and examination before you can claim a right to ownership. Others do not.

- Copyright is a separate form of intellectual property which does not require registration.
- Copyright and circuit layout rights are administered by the Department of Infrastructure, Transport, Regional Development and Communications and they assist the government in developing and managing copyright policy in the Copyright Act 1968 and Circuits Layouts Act 1989.
- Business names, company names and domain names are not a type of IP.
- IP Australia administer patents, trademarks, designs, and plant breeder's rights in Australia.

Before you apply for any IP rights, it is important to understand the differences between the four main rights and which one suits your idea.

© Commonwealth of Australia 2017. 'IP Explained', https://www.ipaustralia.gov.au/understanding-ip/getting-started-ip/ip-explained, 22/04/21 CC BY 4.0

Weblink

Access the links below for more about IP.

IP Australia – Understanding IP

Australian Government - IP Australia[44]

Department of Infrastructure, Transport, Regional Development and Communications[45]

Types of intellectual property

Queensland Government – Business Queensland[46]

[44] https://www.ipaustralia.gov.au/understanding-ip

[45] https://www.communications.gov.au/what-we-do/copyright

[46] https://www.business.qld.gov.au/running-business/ip/types

Patents

A patent is a legally enforceable right for a device, substance, method, or process. For your application to be successful, your invention must be new, useful, and inventive or innovative. When granted, a patent will give you exclusive commercial rights to your invention (a monopoly).

The type of patent you hold will determine the duration of your protection.

- A standard patent lasts for up to 20 years.
- An innovation patent only lasts for up to 8 years. (The innovation patent is being phased out, learn more).
- Pharmaceutical patents can last up to 25 years.

All Australian patent applications must be filed with IP Australia. IP Australia will assess your application to make sure it meets legislative requirements.

Visit the link below for more detail.

Weblink

Visit the link below for more information about patents.

Australian Government IP Australia – Patents[47]

181007266 / Olivier Le Moal / stock.adobe.com

[47] https://www.ipaustralia.gov.au/patents

© TAFE Queensland 2020

Trademarks

271621477 / Olivier Le Moal / stock.adobe.com

Your trademark, often called a brand, is your identity. It is the way you show your customers who you are.

It might be your corporate logo, a jingle you use in an advertisement, your business name painted on the side of your truck or your signage or packaging.

A trademark can also be any of the following things.

- word (in a plain font or a 'fancy' font)
- phrase
- letter
- number
- logo
- picture
- aspect of packaging
- or combination of the above.

A common misconception is that a trademark is the same thing as a business name, company name or domain name. It is not.

- **Business names** – Business names and company names are registered with the Australian Securities and Investments Commission (ASIC). While they are required to run a business in Australia, they do not stop others from using the same or similar name.
- **Trademarks** – IP Australia register trademarks to give you the exclusive rights to that mark, which makes it easier for you to take legal action to prevent others from using it. Registered trademark is different to business, company, and domain names.
- **Domain names** – Domain names are issued by private internet companies and registered by the.au Domain Administration. The purpose of a domain name is to secure the web URL only.

Weblink

More information can be found at the website below.

IP Australia – Trademarks[48]

[48] https://www.ipaustralia.gov.au/trade-marks

© TAFE Queensland 2020

Design rights

A design right protects the overall visual appearance of new and distinctive products. The overall visual appearance can be a combination of visual features including:

- shape
- colour
- configuration
- pattern
- ornamentation.

A design right aims to protect the visual appearance of a whole product that:

- has physical and tangible form
- is manufactured or handmade
- is produced on a commercial scale.

481499200 / adike / shutterstock.com

 © TAFE Queensland 2020

Design rights do not protect everything. The following are not protected by design rights.

- How your product works.
- The materials used in your product.
- The size of your product.
- The brand name or logo you have developed for your product.
- Partial design features of a product.
- The visual appearance of your product changing over time.

Weblink

More information can be found at this website.

IP Australia – Designs[49]

[49] https://www.ipaustralia.gov.au/designs

© TAFE Queensland 2020

PBR

Plant breeder's rights (PBR) are exclusive commercial rights for a registered variety of plant. The rights are a form of intellectual property (IP), like patents, trademarks, and designs. If you develop a new plant variety, you may want to protect your IP with plant breeder's rights.

The plant breeder's rights (PBR) scheme protects plant breeders and gives them a commercial monopoly for a period of time. This encourages plant breeding and innovation and means that a large and growing pool of new plant varieties is freely available to anybody when the protection periods lapse.

308786104 / Golden Sikorka / stock.adobe.com

 © TAFE Queensland 2020

Topic summary and review

In this topic we covered intellectual property and how it applies to, and is different from, copyright. We also introduced the different types of intellectual property including patents, trademarks, design rights and the plant breeders' rights scheme (PBR).

Self-check – Intellectual property

Domain names for websites are classed as intellectual property.

- ☐ True
- ☐ False

All concepts and processes have design rights protection.

- ☐ True
- ☐ False

A standard patent lasts for up to how many years?

- ☐ 15
- ☐ 30
- ☐ 20
- ☐ 50

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

Data

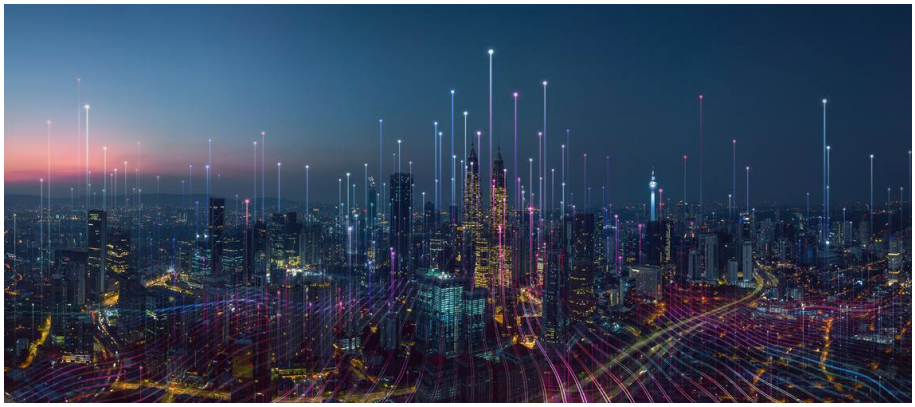
Introduction

Every transaction you do, any information you read, and any program or app you run is made up of data. Some of this data is just raw information that runs a program, and some is highly sensitive personal information. This topic takes a look at understanding what type of data relates to person personal information and how it is classified.

Objectives

By completing this topic, you will be able to:

- understand what data is
- determine sensitive data
- understand personally, identifiable information
- identify sensitive data
- classify data.



1499306735 / Creat jamesteohartor / shutterstock.com

 © TAFE Queensland 2020

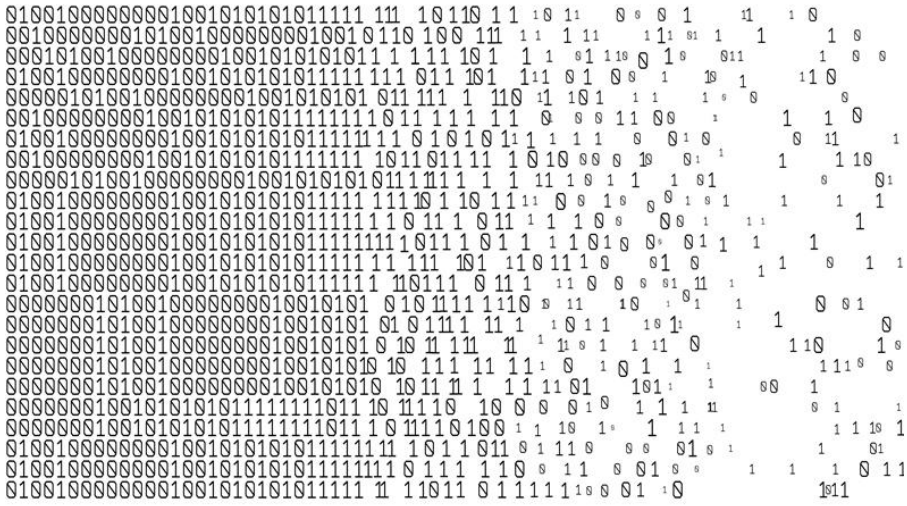
What is data?

Technically in Information Technology data is the bits and bytes stored in memory or a storage device, and what is being transmitted encapsulated in what is termed ‘packets’. However, the way we will look at data in the terms of this unit is information that is stored, collected, or shared. Information as data on a computer will take form in the shape of files, such as the common Microsoft Word.docx file.

Let us have a look at a small business that is in the engineering section and produces design and CAD drawings for structural steel. The following are some of the data files that the company may have.

Common business	• Word processing • Spreadsheets • Bookkeeping • Wages
Industry specific	• Design concepts • Detailed drawings • Specifications
Customer relations	• Client contact information and company details • Personal information from web site contacts

Data has different importance attached to it, the differences could be personal, intellectual property, copyrights, trademarks, financial, etc. Each of these types of data brings with it a risk in privacy that can affect individuals and businesses.



785530237 / Yuri Hoyda / shutterstock.com

Sensitive data

Sensitive data is information that must be always protected against unauthorised access from malicious parties. To prevent unauthorised access to sensitive data there should always be sufficient data security, and information security policies and procedures in place to prevent any data disclosure or data breaches.

An organisation may have to guard against unauthorised access to sensitive data for legal or ethical requirements, also regulatory reasons, trade secrets, personal privacy, and critical business data.

Any breaches to access of sensitive data can cause irreparable damage to the organisation in regard to client trust and industry representation. This could also lead to not just financial loss to the business but also breaches to Australian law where the organisation and directors or owners, could be exposed to penalties in regard to fines or imprisonment.

See the following page to learn how the Australian government defines sensitive information.

201706189 / jirsak / stock.adobe.com

 © TAFE Queensland 2020

Section 6.89

‘Sensitive information’ is defined in the Privacy Act to mean information or an opinion about an individual’s:

- racial or ethnic origin.
- political opinions.
- membership of a political association.
- religious beliefs or affiliations.
- philosophical beliefs.
- membership of a professional or trade association.
- membership of a trade union.
- sexual preferences or practices; or
- criminal record.

Section 6.90

‘Sensitive information’ also includes health information and genetic information about an individual that is not otherwise health information.

Section 6.91

‘Sensitive information’ is subject to a higher level of privacy protection than other ‘personal information’ handled by organisations in the following ways:

- ‘Sensitive information’ may only be collected with consent, except in specified circumstances. Consent is generally not required to collect ‘personal information’ that is not ‘sensitive information’
- ‘Sensitive information’ must not be used or disclosed for a secondary purpose unless the secondary purpose is directly related to the primary purpose of collection and within the reasonable expectations of the individual
- ‘Sensitive information’ cannot be used for the secondary purpose of direct marketing
- ‘Sensitive information’ cannot be shared by ‘related bodies corporate’ in the same way that they may share other ‘personal information’.

Australian Law Reform Commission, ‘Sensitive information’, https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/6-the-privacy-act-some-important-definitions/sensitive-information, 29/04/2021 CC BY-NC-ND 3.0

Activity

As a student of TAFE Queensland, create a list of the sensitive information that the organisation holds. Compare your list with your colleagues and discuss any differences.

Personally identifiable information

The Privacy Act defines 'personal information' as, "Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not
- whether the information or opinion is recorded in a material form or not."

The definition is technologically neutral to ensure sufficient flexibility to encompass changes in information-handling practices over time. It is also consistent with international standards and precedents.

Office of the Australian Information Commissioner, 'What is personal information', https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information, 26/04/2021, CC BY 3.0

Types of personal information

The term 'personal information' encompasses a broad range of information. For a full description visit the link below.

Reading

Please read the 'What is personal information' section to 'Common types of information".

What is personal information?[50]

1826382596 / Piscine26 / shutterstock.com

[50] https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information#:~:text=The%20Privacy%20Act%20defines%20%27personal,a%20material%20form%20or%20not

© TAFE Queensland 2020

Identifying sensitive data

Australian Law Reform Commission's view

The ALRC recognises that personal information can become more or less sensitive because of the context in which it is considered and notes that this can apply to almost any personal information. The definition of 'sensitive information'; however, should not be amended to include information made sensitive by context. On balance, the existing approach of listing categories of information as sensitive provides greater certainty. This is important because the Privacy Act imposes stringent requirements for handling sensitive information (6.102).

In particular, the Privacy Act and the model UPPs provide that sensitive information should generally be collected with consent and should be used only for the purpose for which the information was collected or a directly related secondary purpose. This regime is significantly different to the regime regulating the handling of other personal information, which can be collected without consent and used and disclosed for a broader range of purposes. It is important to be clear about what information is covered by the more stringent requirements (6.103).

Australian Law Reform Commission website, 'Sensitive information', https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/6-the-privacy-act-some-important-definitions/sensitive-information/, 29/04/2021 CC BY-NC-ND 3.0

402951798 / JustSuper / stock.adobe.com

Classifying data

When you get information from various sources including staff and clients, you need to classify the type of data it is. If you are getting information just for a simple project like a phone book that has publicly available information, this information would not be classified as sensitive and therefore available for public use.

However, if the information you are collecting is attached to financial or health information, then the information you are collecting would be classified as sensitive. The reason for this is because financial information could contain tax records such as tax file numbers and health information could contain data relating to a person's mental or physical problems. Both these types of information are protected under Australian Privacy law.

As mentioned previously in the 'Personally, Identifiable Information' section, personal information would be classified as sensitive information and should be treated accordingly.

Provided the information or opinion otherwise meets the definition of personal information.

'Sensitive information' includes the information listed below.

- Racial or ethnic origin
- Political opinion
- Religious beliefs
- Sexual orientation
- Criminal record
- 'Health information' (which is also 'sensitive information')
- 'Credit information'
- 'Employee record' information (including tax file number)

169077710 / Fredio / stock.adobe.com

 © TAFE Queensland 2020

Apart from the above being classified as sensitive, intellectual property (IP) can also be classified a sensitive. Intellectual property is property knowledge, or also known as the property of your mind. This can be design, trademark, an invention, a brand, or even the application of your idea.

Although the privacy act does not include intellectual property you should always consider if the data you are handling is sensitive or not.

Weblink

Visit this government website for a comprehensive overview of IP.

IP explained[51]

[51] https://www.ipaustralia.gov.au/understanding-ip/getting-started-ip/ip-explained

 © TAFE Queensland 2020

Topic summary and review

This topic covered the knowledge and skills needed to understand what data is, especially sensitive data. Other areas in this topic were understanding what personally identifiable information is, and how to identify and classify data.

Self-check – Data

The Privacy Act allows an individual to:

- ☐ have the option of not identifying yourself, or of using a pseudonym in certain circumstances
- ☐ ask for access to your personal information (including your health information)
- ☐ stop receiving unwanted direct marketing
- ☐ All the above

Types of personal information can include ‘health information’, ‘credit information’, and ‘tax file number information’.

- ☐ True
- ☐ False

Which one of the following is defined in the Privacy Act as sensitive information?

- ☐ Sports club membership
- ☐ Racial or ethnic origin
- ☐ Opinion of the best NRL team

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

Sending and receiving sensitive data

Introduction

Every microsecond of the day information is back and forth from a point A to a point B. This normally does not matter until the information becomes personal and sensitive. This topic looks at understanding how we collect sensitive information, and the risks involved. The topic also looks at the way we send information in regard to being unsecured and secured.

Objectives

By completing this topic, you will be able to:

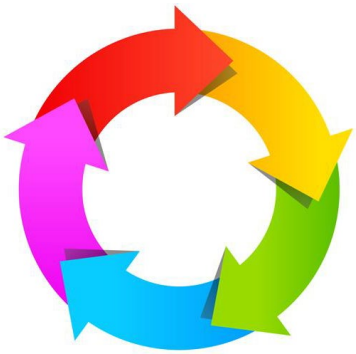
- understand the information life cycle
- understand the basics of sending and receiving unsecured data
- understand the basics of sending and receiving secured data.

206169546 / ArtemSam / stock.adobe.com

© TAFE Queensland 2020

The Information life cycle

Personal information security throughout the life cycle involves:



287018294 / Arcady / shutterstock.com

- considering whether it is actually necessary to collect and hold personal information in order to carry out your functions or activities
- planning how personal information will be handled by embedding privacy protections into the design of information handling practices
- assessing the risks associated with the collection of the personal information due to a new act, practice, change to an existing project or as part of business as usual
- taking appropriate steps and putting into place strategies to protect personal information that you hold
- destruction or de-identification of the personal information when it is no longer needed. If you handle personal information, you should consider how you will protect personal information during the stages of its life cycle.

To effectively protect personal information throughout its life cycle, you will need to be aware of when and how you are collecting it and when and how you hold it. As noted above, your personal information holdings can be dynamic and change without any necessarily conscious or deliberate action.

Additionally, the life cycle may include the passing of personal information to a third party for storage, processing, or destruction.

Office of the Australian Information Commissioner, 'Guide to securing personal information', https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information, 26/04/2021, CC BY 3.0

Reading

Please read the guide below for a detailed look at the information lifecycle. Please look at sections 1-5.

Office of the Australian Information Commissioner.

'Guide to securing personal information'[52]

[52] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information

© TAFE Queensland 2020

Sending and receiving unsecured data

What is unsecured data

There are many definitions of unsecured data, the first one that comes to mind is where data is available to the public and contains sensitive information.

Another definition of unsecured data is where data becomes available due to a breach in the system, being either a network infrastructure or storage system. These breaches are normally caused by mismanagement or hacking by a malicious party.

There are many areas where information could become public:

- emails
- public file sharing services (such as a drop box)
- organisations own computer networks (especially when Wi-Fi or WAN is part of the IT infrastructure)
- if any part of the computer network is not properly configured for security, it will then pose a risk for hacking and sensitive information could become public.

194382434 / tadamichi / shutterstock.com

 © TAFE Queensland 2020

Transmitting and receiving unsecured data

As mentioned earlier, emails and public file sharing services can provide access to the public and therefore the data is unsecured. We've the transmission of data attached to emails, these can be easily hacked during transmission of data packets from the host to the destination.

Many commonly used methods of transmitting data are unsecured.

- **Email services** – Even some of the big-name email services like Gmail and Yahoo do not provide end to end encryption for your emails. When you send an email, it passes through several insecure servers that are vulnerable to hacking and other dangerous things.
- **Public file sharing** – Public file sharing services are not designed to cater for sensitive data as a default setting. Businesses need to be aware that when using public file sharing services, they are exactly what the name implies; therefore, businesses should not use these types of file sharing services where sensitive information could be transmitted to by accident.
- **Storage devices** – Another way of transmitting unsecured data is with external storage devices such as USB memory sticks or USB hard drives. Often, staff members use a USB memory stick to transport data and are not aware that the memory stick could be unsecured. Oblivious that USB storage devices have the capability of being either encrypted or have a data lock activated.
- **USB devices** – Any type of USB storage device should be discouraged for use of transmitting data from one location to another, as these devices can be either easily lost or stolen. And if sensitive information were on these USB storage devices, the data could easily become public.

653397169 / Olena Yakobchuk / shutterstock.com

 © TAFE Queensland 2020

Receiving unsecure data

There are a number of ways of receiving unsecured data.

- It can be through emails.
- Transferring of information from one source to yourself.

Unsecure data can come in many forms, it can be sensitive information that you receive where the sender has not secured the data by encryption or other secure means. This can be by accident, by negligence in the form of not caring, or where the sender is doing it for malicious purposes.

Important

If you receive unsecured data with sensitive information you have to report it to the Office of the Australian Information Commissioner as a breach. Breaches of the Privacy Act can have consequences for both the sender and the receiver.

To battle against unsecured data being received by the organisation, you require not only good IT management, but also an industry strength security suite, plus well-trained staff in regard to handling emails, attachments, and data handling.

 © TAFE Queensland 2020

Sending and receiving secure data

Sending and receiving secure data is not just a process of pressing a button and assuming that the process is done. There are many background policies and procedures that need to be in place for an organisation to be able to securely send and receive data that has sensitive information.

'Information security' involves all measures used to protect any information generated by an entity or individual, that is not intended to be made publicly available, from compromise, loss of integrity or unavailability. This can include personal information, security classified information and commercially confidential information.

Why is personal information security important?

Personal information security is about more than just ensuring compliance with the requirements of the Privacy Act.

See below to learn more about the consequences and benefits of how PI is handled.

- **Reputational loss** – If you mishandle the personal information of your customers, it can cause a financial or reputational loss to the customer.
- **Loss of trust** – Mishandling information can also lead to a loss of trust and considerable harm to your reputation.
- **Loss of revenue** – A significant breach may result in a loss of customers or business partners and revenue.
- **Reporting** – Under the NDB scheme, you must, subject to some exceptions, notify individuals who are likely to suffer serious harm as a result of an eligible data breach. You must also notify the Commissioner.
- **Business function** – If personal information that is essential to your functions or activities is lost or altered, it can have a serious impact on your ability to undertake business as usual.
- **Benefits** – The benefits of applying personal information security to your business practices can include more efficient processes. It also reduces the risk of privacy breaches and the time and resources involved in addressing any breaches that do occur.

1838253076 / Aozora21 / shutterstock.com

 © TAFE Queensland 2020

Email and network security

Email security

Email is not a secure form of communication and you should develop procedures to manage the transmission of personal information via email.

- Avoid sending certain types of personal information via unsecured email (for example sensitive information) and use secure methods for communicating information, such as a secure website or to a secure online mailbox.
- Use secure end-to-end encryption messaging where appropriate and available.
- Obtain a recipient's consent to send their own personal information to them via email.
- Validate the email address with the recipient before sending the unencrypted email to reduce the chance of unauthorised disclosure to a party, who is not the intended recipient.
- Ensure that accurate records are kept regarding when external emails are sent and received.
- Only send sensitive information or large amounts of non-sensitive personal information by email as an encrypted or password protected attachment.

Office of the Australian Information Commissioner, 'Guide to securing personal information', https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information 26/04/2021, CC BY 3.0

175846607 / Production Perig / stock.adobe.com

© TAFE Queensland 2020

Network security

Data security is not just about having encryption on the data during transmission, but also restricting the access to the location of the data. There are a number of areas where security to a system can be improved:

Passwords. This is the simplest form of security for any system, it is also the easiest area for a hacker to break through due to weak strength of some password policies. Password strength not only applies to when you login to a device or network, but also into applications that access personal information for clients and yourself.

Strength', denotes the general length of the password as well as the combination of potential character combinations you select, such as symbols, numbers, and lower or upper-case letters.

- **Weak** – A weak password may only consist of 6 characters, mainly lower-case and maybe some numbers, with an example being John63. Dates, names, teams, anniversaries, vehicle registrations, pets and places are frequently used by people for passwords, and so they are also the options attempted first by attackers. 'Password' is still unfortunately the most commonly used password.
- **Strong** – A strong password is a longer and more haphazard mixture of characters. With the strongest passwords considered as passphrases. Comparable to a password, but instead of creating a string of letters, numbers, and symbols, use words that make up a silly statement. For example: aCorgimake5agreaTh@mburg3r! This is an extremely strong password as who would have thought a corgi can make a great hamburger.

Depending on whose resource on the internet you visit, they will give you differing results on how long the password would take to be cracked with a brute force attack.

Example

The following websites can estimate how long it would take to crack a password.

How secure is my password?[53]

- John63 – 1 second
- aCorgimake5agreaTh@mburg3r! – 25 Undecillion years

The Time it Takes to crack a Password[54]

- John63 – 1 second
- aCorgimake5agreaTh@mburg3r! – 7+ Undecillion years

[53] https://howsecureismypassword.net/

[54] https://community.spiceworks.com/topic/2286767-the-time-it-takes-to-crack-a-password-visualized

 © TAFE Queensland 2020

Other security that needs to be implemented on a network:

- A properly administered firewall
- Security suite that is industry recognised and gives end-point protection
- Two-factor authentication for accessing sensitive information or applications
- Good staff training in email protocol, especially in recognising phishing.

 © TAFE Queensland 2020

Topic summary and review

This topic covered the knowledge and skills needed to understand the information life cycle for information and understand the basics of sending and receiving unsecured data and secured data.

Self-check – Sending and receiving sensitive data

Under APP 11.2, APP entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed.

- ☐ True
- ☐ False

Under APP 3, you should only collect personal information that is reasonably necessary to carry out your functions or activities.

- ☐ True
- ☐ False

Which one of the following is true in regard to emailing sensitive information?

- ☐ Use non-encryption messaging for speed and accuracy.
- ☐ Obtain a recipient's consent to send their own personal information to them via email.
- ☐ Send the email addressed to the recipient and resend the unencrypted email if unsuccessful.

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

File location

Introduction

We now know what data is, but where is it kept? This topic looks at understanding the different types of file location where we keep our data. We will also explore the types of storage device that exist, including the cloud. The topic will also glimpse the cloud solutions that are available for storing data.

Objectives

By completing this topic, you will be able to:

- understand the different types of file locations
- understand tradition storage devices
- know what the cloud is
- understand the different cloud computing solutions.

1181228215 / Alexander Supertramp / shutterstock.com

 © TAFE Queensland 2020

Types of file location

In a small business, the location of sensitive files would be within the business data files. Although both file types would be in would be in the same location, folder structures would differ, with sensitive data being properly secured.

Let us have a look at a few scenarios where small businesses store their data, keeping in mind that all business models will normally have 3 options – onsite storage, cloud storage, or a mixture of both.

Micro business with standalone computer

This type of business might be a home-based business that does consultancy work, or a business that has a number of service staff but having a single computer that managers and plans all the business activities.

Data capacity 10GB to 250GB

The structure of the business could be:

- book keeping application running straight from the vendor's cloud
- client contacts running through cloud-based application such as Microsoft Outlook
- file storage can be located on the computer or cloud, or synchronised with the cloud.

Small network business up to 10 users

This type of business could have a small 5 to 10 user peer-to-peer or server-client network. These types of businesses can range from a small motel complex, retail outlet, small medical clinics, to small engineering firms.

Data capacity 250GB to 1TB

The structure of the business could be:

- book keeping application running straight from the vendor's cloud
- client contacts running through cloud-based application such as Microsoft outlook
- file storage can be located on a network attached storage (NAS) device, or server, or cloud, or synchronised with the cloud.

 © TAFE Queensland 2020

Small network business up to 50 users

This type of business would have a server-client network. These types of businesses can range from a small business with multiple departments to design centres or application development hubs.

Data capacity 1TB and above

The structure of the business could be:

- accounting application running straight from the vendor's cloud, or server-based
- client contacts running through a cloud-based or server-based application such as a customer relationship management system
- file storage managed through the server via NAS, synchronised with the cloud.

As you can see from the above scenarios the way that files can be stored can easily vary. This also means that the way that businesses secure sensitive information will also vary depending on where the information is stored.

 © TAFE Queensland 2020

The traditional storage devices

Less than 10 years ago the traditional storage location for any files in a business would have been on a hard disk drive somewhere.

On a standalone system this would be an internal Hard Disk Drive (HDD), with backups performed to an external USB device being memory sticks or portable HDD depending on the amount of data.

See below to learn more about different types of storage.

- **Small network** – A small network with 5 computers in a peer-to-peer configuration would have either one of the computers designated as the main storage device for the files with all the other computers having mapped folders linked to them. Or a network attached storage (NAS) device attached to the network and all computers mapped to it. Backups would again normally be performed to an external USB storage device.
- **NAS** – A NAS would have preferably 2 or more HDD installed and running Redundant Array of Individual Drives (RAID) that gave the device a failover capability. If a single drive fails the information would be still available on the other drives.
- **Server/client network** – On a server/client network, normally referred to as a domain, the server would have 2 or more HDD installed for the main storage. These drives would be attached to a RAID controller for redundancy and backups would be performed to a tape cartridge drive normally embedded in the server. Depending on the size of the organisation, or the data size, instead of backups the whole server may be mirrored to another location via fibre optics and synchronisation maintained.

Step forward to today, and with businesses having access to the NBN in most places, cloud storage is now becoming more and more the norm.

Activity

List the different types of storage devices you use for your own data and compare your list with your fellow colleagues.

744358555 / H_Ko / shutterstock.com

 © TAFE Queensland 2020

The cloud

A simple cloud solution for a micro or small business that has less than 1TB of data could be the use of services such as OneDrive. The files would be located on a drive at the business premises and simply synchronised with the cloud service. However, for a more secure option it would be preferrable to look at cloud services offered by the numerous vendors, currently in the marketplace.

Cloud computing helps organisations to ease the burden of managing IT infrastructure and saves money on capital expenditure spent on infrastructure. Today's organisations can implement their complete IT network and run their applications on the cloud. There are excellent features available in cloud services, such as high availability and scalability, which companies can do in a few clicks, rather than spending hours configuring and managing them.

In this section we will be only looking at cloud as a storage service, although the basics will still be covered.

611605280 / Blackboard / shutterstock.com

 © TAFE Queensland 2020

Cloud computing models

Software as a Service (SaaS)

Software as a service enables consumers to use software programs in the cloud without installing them in local computers. SaaS already includes IaaS and PaaS, but consumers only use and pay for SaaS built on IaaS and PaaS.

Best example for SaaS is Microsoft Office 365. Consumers can use complete Microsoft Office package online by subscribing to MS Office 365 and pay for monthly subscription.

Platform as a Service (PaaS)

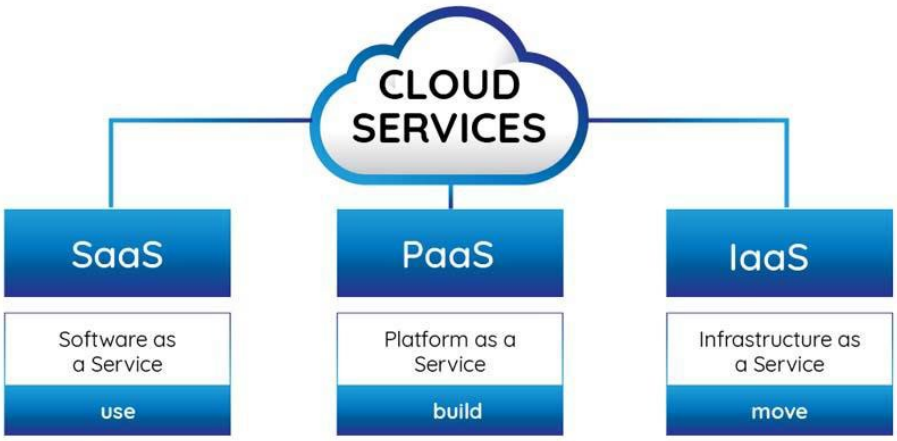
Platform as a service includes the preconfigured environment of IaaS. Cloud consumers only use the service as a platform to run their development tools, use operating systems, and for business analytics.

In this model, the burden of infrastructure management is taken away from the consumers and consumers only pay for the platform services they use.

Infrastructure as a Service (IaaS)

Hardware based IT resources in a network can be categorised as infrastructure. This may include computers (servers), storage, and networking resources such as routers and switches (a device that connects routers together). Cloud can host these resources in a virtual environment where consumers can implement their complete network in the cloud which is called Infrastructure as a Service.

IaaS offered in the cloud is not a pre-configured service; consumers have full control over how they want the network and infrastructure deployed, therefore the responsibility of managing the cloud is placed directly upon cloud consumers.



1415429273 / Luna2631 / shutterstock.com, Modified by TAFE Queensland

 © TAFE Queensland 2020

Cloud computing deployment models

There are three main cloud computing models, distinguished by ownership, size and access.

Private cloud

Private cloud is owned and hosted by a private organisation (on-premises), with the purpose of centralising access to different departments or sections of the organisation. The access to private cloud is only for people who have permission to do so. Actual administration of the private cloud could be under internal staff or an outsourced company. Private cloud may physically be in the same location but the cloud services should be available to access remotely to cloud consumers.

Hybrid cloud

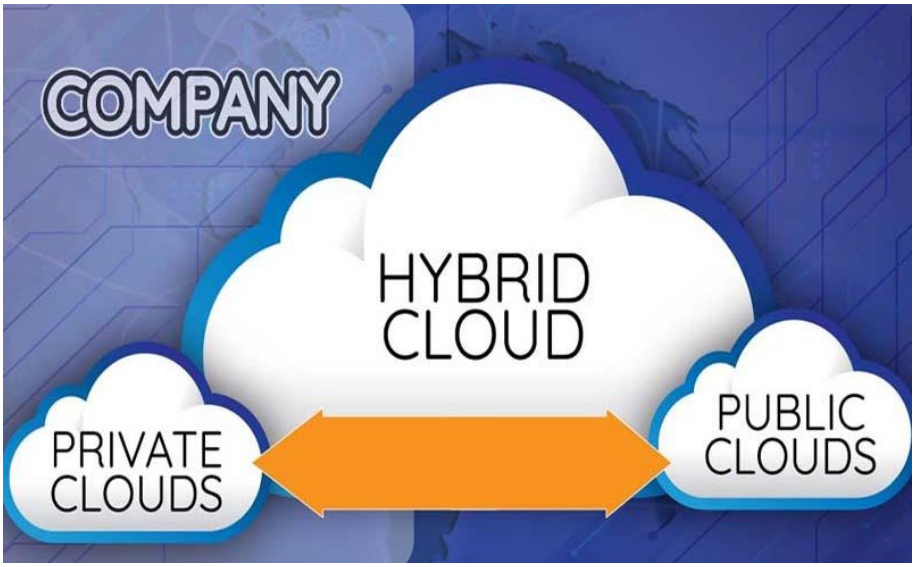
Hybrid cloud consists of aspects of both the private cloud and the public cloud. For example, an organisation may have their server running on the premises but wanted to install a database in a cloud that is connected to a local server. For another example, an organisation may prefer to store their sensitive data on-premises while running other services on the cloud.

The most important configuration concern for hybrid cloud would be the integration between public and private cloud.

Public cloud

Public cloud is hosted by a provider, available to all and connected via an internet connection. Public cloud services are offered to consumers at a cost. The cloud provider is responsible for the physical infrastructure and maintenance of their resources. Consumers need the least technical expertise to use public cloud compared to other cloud computing models.

Examples are Microsoft Azure, Amazon Web Services and Google Cloud. These are the leading public cloud solutions in the industry.



699701578 / Bakhtiar Zein / shutterstock.com. Modified by TAFE Queensland

 © TAFE Queensland 2020

Each type of cloud offers pros and cons for their type. The public cloud is the cheapest to run as it is an operational expense for a business, lacks security, but also requires the least amount of IT expertise. Whereas, the private cloud can have the highest security, but also requires the highest IT expertise as everything is managed by the business.

Compare the three deployment models

A simple comparison is given below.

Expenditure type:	OpEx
Security:	Lowest
Flexibility:	Lowest
Technical expertise:	Least

Expenditure type:	CapEx
Security:	Highest
Flexibility:	Medium
Technical expertise:	Most

Expenditure type:	CapEx
Security:	Highest
Flexibility:	Medium
Technical expertise:	Most

167048390 / Equipoise, 151713311 / Blablo101 / shutterstock.com. Modified by TAFE Queensland.

Weblink

To compare and contrast cloud computing models, visit this webpage.

"What are the different types of cloud computing services?"[55]

[55] https://azure.microsoft.com/en-au/overview/types-of-cloud-computing/

 © TAFE Queensland 2020

Cloud computing solutions

Cloud computing service providers

The following are the top 5 cloud solutions that Australian businesses are increasingly using. All these solutions offer cloud services.

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- Alibaba Cloud
- IBM Cloud Satellite

Activity

Out of the above cloud service providers, AWS and Azure cloud service providers hold the biggest share of the market.

We will take AWS and Azure as an example when we discuss cloud solutions in this document.

215968639 / Buffaloboy / stock.adobe.com

© TAFE Queensland 2020

Microsoft Azure

MS Azure is the cloud computing solution offered by Microsoft. Azure provides cloud infrastructure with more than 200 products that customers can use in their businesses. As other cloud services, Azure offers infrastructure, software, and platform as services. Azure is a service covering 140 countries with 55 geographical locations.

346398611 / tadamichi / stock.adobe.com

 © TAFE Queensland 2020

Azure architecture

Azure architecture consists of regions, availability zones and sets, resource groups and Azure resource manager.

Azure regions

Azure regions are locations which contain data centres that store your data, regions are located around the world. Each Azure region is paired with another region for fault tolerance.

Customers can choose the region where their data is to be saved. There could be government regulations on which region you can save data in. The cost of your Azure service will vary from region to region.

Weblink

Access this link to find more information about Azure regions.

Azure geographies[56]

Availability zones and sets

Availability zone is a physical location with one or more data centres. Each region has at least three availability zones. The purpose of availability zones is to achieve high availability. If one data centre is not working, the other two data centres can keep the region working.

Availability sets help to achieve availability and provide application redundancy across multiple virtual machines. You can either use availability zones or availability sets but not both.

Resource groups

Allow customers to organise and manage resources for a particular application, you can add virtual machines, SQL databases, network interfaces and other resources related to a particular application under one resource group.

[56] https://azure.microsoft.com/en-au/global-infrastructure/geographies/#overview

 © TAFE Queensland 2020

Azure also offers a choice of storage options. See below to learn more about Blob and File storage.

Blob Storage

Used to store huge amounts of unstructured data. Customers can store any type of data and access them as and when they want. Blob storage can meet any capacity requirements for a lower price.

Azure blob storage is durable, scalable, and secure. It uses role based access control with active directory to make sure your data is secure. Azure can create Data Lakes using blob storage for analytical purposes.

Weblink

Read more about Blob storage here.

Azure Blob Storage[57]

File Storage

File Storage offers fully managed file share that is accessible via SBM and NFS protocols. A highlight of Azure file share is that it is serverless and can be used in a hybrid environment as well. This offers multiple protocol support for optimised cost.

Weblink

Read more about Azure file storage here

Azure Files[58]

[57] https://azure.microsoft.com/en-us/services/storage/blobs/

[58] https://azure.microsoft.com/en-us/services/storage/files/

 © TAFE Queensland 2020

Topic summary and review

This topic covered the knowledge and skills needed to understand the different types of file locations. These locations included the traditional storage devices and the emergence of cloud storage solutions which are becoming an everyday norm.

Self-check – File location

Three (3) options for file storage are onsite storage, cloud storage, or a mixture of both.

- ☐ True
- ☐ False

Which of the following is not a file storage area?

- ☐ HDD
- ☐ NAS
- ☐ NVMe
- ☐ Cloud

Which one of the following is not a cloud service?

- ☐ Amazon Web Service
- ☐ Cumulus cloud
- ☐ Azure Cloud

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

Data integrity and authorised access

Introduction

So is your data safe, or reliable? This topic looks at understanding your data integrity and how reliable it is, especially when sending the data to someone. The topic will also look at keeping your data safe and secure from malicious players.

Objectives

By completing this topic, you will be able to:

- understand attacks on data integrity
- understand how to mitigate data integrity attacks
- allow permission to access data
- understand the difference between data encryption and hashing.

1740417467 / Profit_Image / shutterstock.com

 © TAFE Queensland 2020

Attacks on data integrity

What is data integrity?

Data integrity is normally refers to the overall accuracy, completeness, and consistency of data. Integrity of personal information in the Privacy Act is the Australian Privacy Principle 10, which reads as follows.

Australian Privacy Principle 10 — quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date, and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete, and relevant. (15*)

Therefore, data integrity is a guarantee that the personal information can only be accessed or modified by those who are authorised to do so.

Office of the Australian Information Commissioner, Australian Privacy Principle 10, https://www.oaic.gov.au/__data/assets/pdf_file/0013/1282/app-guidelines-chapter-10-v1.1.pdf, 26/04/2021, CC BY 3.0

Video

Watch the video by 365ComputerSecurity for a short overview of Information Security.

Confidentiality, Integrity, and Availability of Computer Security[59]

1977780443 / Bankrx / shutterstock.com

[59] http://www.youtube.com/embed/j8FT9WqmuDY?rel=0

© TAFE Queensland 2020

What is a data integrity attack?

Data integrity is an assurance that the information can only be accessed, or modified, by persons authorised to do so. Therefore, data integrity attack objectives are to compromise this assurance with the intention of gaining unauthorised access, to modify data accuracy and reliability.

Example

An example of a data integrity attack occurred in 2016 – Both the World Anti-Doping Agency and Democratic National Committee were breached with hackers manipulating their data to embarrass the organisations. These types of attacks are the worst modes of cyber-attacks.

Types of attacks

Over time, data has been evolving in the way it is seen in the domain of cyber security.

- **Data availability** – When data first became easily available, it went through the first type of attacks by malware and distributed denial of service (DDOS). Malware has a history of preventing access to data, while DDOS attacks the bandwidth or resources of a targeted system.
- **Data confidentiality** – Cyber threats to data confidentiality are characterised as data theft.
- **Data integrity** –This form of data attack does not deny access or steal data like malware. It compromises the integrity of the data's reliability and accuracy.

 © TAFE Queensland 2020

How are data integrity attacks carried out?

Data integrity attacks involve a number of combined attacks on different layers in the system with a purpose of exploiting the vulnerabilities. Attackers will achieve a level of access based on the level of vulnerabilities. Attackers use a number of tools and techniques to breach and monitor a system over time. Attackers will sometimes embed their bugs into the infrastructure and wait for years until they think it is the perfect time to attack.

Scenario

Consider a scenario in which the attacker plants a malware through phishing emails in the administrator's computer. The malware establishes a key logger program in the system to gain the credentials. In the meantime, he can also change the security settings and infiltrate more harmful programs. This is the way integrity attacks occur. These attacks are very dangerous and have the potential to conquer the whole system.

Video

Watch this video from Lepide about cyber-attacks and mitigation strategies.

Popular Cyber Attack Methods and How to Mitigate Them[60]

[60] http://www.youtube.com/embed/N68pGHbnJWc?rel=0

© TAFE Queensland 2020

Mitigating data integrity attacks

How can these attacks be prevented?

Implementing certain security measures can help prevent data integrity attacks. Most attacks target the networks and then they climb up the ladder as each level of vulnerability is breached.

- **Separate networks** – On larger networks, constructing separate networks in the system will help stop spreading attacks. Using security suites in all devices will act as a shield from integrity attacks. In order to detect and prevent data integrity attacks, we must also consider developing network security tools with artificial intelligence, which can block suspicious moves.
- **Strong password policies** – The implementation of strong password policies and using 2 points of verification for access to secured personal information is necessary in any situation where privacy of information is concerned. All this is useless if training of staff is not provided to a level where the staff can recognise possible threats and social engineering traits.
- **Cloud-based storage** – The majority of breaches actually occur internally via devices and emails. With the availability of decent internet connections for the majority of the country, staff need to use cloud-based storage and move away from devices such as USB memory sticks. USB memory sticks are a popular way to transfer malicious software from the staff member's home computer to the office network.
- **Good staff training** – Emails are a popular way of getting staff members to click on or open up emails that have attachments or links to websites that promise prizes or other incentive enticements. This process is known as phishing and is best prevented by good staff training to identify this threat.

Video

Watch this video by Mindset about common cyber-threats and safeguards.

Cyber Threats & Safeguards to Protect you against Attacks (English)[61]

1942305685 / Chor muang / shutterstock.com

[61] http://www.youtube.com/embed/Z-0ZphHmQDE?rel=0

 © TAFE Queensland 2020

Authorised personnel

The Collins Dictionary defines “Authorised” as officially permitted or empowered.

People who are authorised to access sensitive personal information should be properly trained in privacy rights, and how to identify common threats.

Authorised personnel should have a good understanding of the Privacy Act. Prior to accessing personal information, they should sign a form indicating they understand the policy and procedures set out in the Privacy Act 1988, and the organisation’s policies.

An authorised person with access to personal information should have knowledge of the following topics.

- Principles of the Privacy Act 1988.
- Data protection and encryption.
- How to recognise and action phishing emails.
- Malicious intrusion of the system and programs.

The above should be part of induction for new employees, with signed employment agreement.

Video

The following video by ‘How to engage in cyber policy’, is a discussion on privacy and data protection:

Privacy and data protection[62]

1404797651 / Lakmal Ditmax / shutterstock.com

[62] http://www.youtube.com/embed/ZNEPaGFApX4?rel=0

© TAFE Queensland 2020

Access permissions - passwords

There are a number of ways to enforce access permissions, no matter if the computer system is standalone or a domain-based client-server network.

Enforce password access

On any system, the most basic access permission is to enforce passwords for all users. This means that when a person starts a computer on whatever system they use, the first thing that occurs is the user requires a username and password to logon. Review the following information, which we have already covered.

Passwords. This is the simplest form of security for any system, it is also the easiest area for a hacker to break through due to the weak strength of some password policies. Password strength not only applies to when you login to a device or network, but also into applications that access personal information for clients and yourself.

Strength denotes the general length of the password as well as the combination of potential character combinations you select, such as symbols, numbers, and lower or upper-case letters.

- **Weak** – A weak password may only consist of 6 characters, mainly lower-case and maybe some numbers, with an example being John63. Dates, names, teams, anniversaries, vehicle registrations, pets and places are frequently used by people for passwords, and so they are also the options attempted first by attackers. 'Password' is still unfortunately the most commonly used password.
- **Strong** – A strong password is a longer and more haphazard mixture of characters. With the strongest passwords considered as passphrases. Comparable to a password, but instead of creating a string of letters, numbers, and symbols, use words that make up a silly statement. For example: aCorgimake5agreaTh@mburg3r! This is an extremely strong password, as who would have thought a corgi can make a great hamburger.

1350947612 / Andrew Rybalko / shutterstock.com

 © TAFE Queensland 2020

Depending on whose resource on the internet you visit, they will give you differing results on how long it will take the password to be cracked with a brute force attack.

Weblink

The following websites provide estimates on the strength of passwords.

How Secure Is My Password?[63]

- John63 – 1 second
- aCorgimake5agreaTh@mburg3r! – 25 Undecillion years

The Time it Takes to crack a Password Visualized[64]

- John63 – 1 second
- aCorgimake5agreaTh@mburg3r! – 7+ Undecillion years

[63] https://howsecureismypassword.net/

[64] https://community.spiceworks.com/topic/2286767-the-time-it-takes-to-crack-a-password-visualized

© TAFE Queensland 2020

Access permissions - two-factor authentication

Two-factor authentication (2FA) is where you will logon to a system or gain access to an application using two forms of verification. This is done using something you know, such as your password, and something you have, such as a mobile phone.

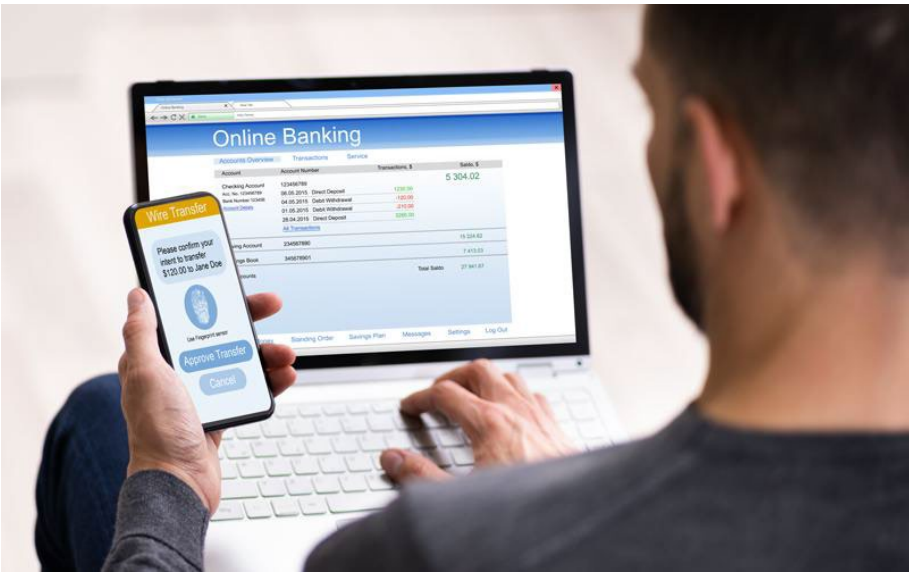
Two-factor authentication acts as a second line of defence, because if your password is guessed by a hacker, sensitive personal information is now vulnerable to malicious intent. Two-factor authentication attempts to tackle that flaw by requiring a secondary code, called a one-time password (OTP). OTPs are usually six characters in length and produced by a smartphone app before you can gain access to your account. So, if a hacker has your password, they will still need to break a secondary code, which makes getting into the system much more difficult.

There are numerous apps that are now available to setup two-factor authentication, depending on the systems you are using. Two of the largest companies in the IT space, Google and Microsoft, both have apps available, as do many other companies in the marketplace. Check out this video for more information.

Video

Check out this video from Duo Security for more information about 2FA.

What is Two-Factor Authentication? (2FA)[65]



1769700296 / Andrey_Popov / shutterstock.com

[65] http://www.youtube.com/embed/0mvCeNsTa1g?rel=0

 © TAFE Queensland 2020

Two-factor authentication as a software application is not the only way two-factor authentication can be done, it also can be achieved by hardware. The following are the advantages and disadvantages of physical security.

Advantages

The safest way to lock down your accounts with two-factor authentication is to employ a physical security key. It has been found in studies that security keys blocked 100 percent of bulk phishing and targeted attacks.

Disadvantages

Where the is a positive there is normally a negative. The negative of using a security key, is that if you ever break or lose the key you could be locked out of your system, and you will have to change your second-factor authentication method to a new key.

Video

Watch the video from SMBSECURE for an in-depth comparison of 2FA methods.

Two Factor Authentication Methods - Pros and Cons of Each[66]

[66] https://www.youtube.com/embed/ea5oYHxbflY

 © TAFE Queensland 2020

Encrypting files

All modern-day operating systems will have some support for encrypting files. You can also use utilities, such as WinZip to encrypt your files.

Windows

In Microsoft Windows.

1. A right click on a file or folder and select Properties.
2. Select the Advanced button and select the Encrypt contents to secure data check box.
3. Select OK to close the Advanced Attributes window, select Apply, and then select OK.

To encrypt a folder.

1. Create a folder you would like to encrypt.
2. Go to Disk Utility.
3. Click File > New Image > Image from Folder.
4. Find and click on the folder you created.
5. Select an encryption method, create a password, and save your encrypted folder.

Linux

To encrypt in a Linux-based operating system, such as Ubuntu.

1. Right-click on a file or folder and select Encrypt.
2. Select to use a shared passphrase or create or import a key.
3. Once you have gone through the process of a passphrase or key, and if you are encrypting a folder, you will be asked if you want to encrypt each file contained within or pack them together in a compressed file.

Video

The videos below give detailed guides to encryption for the main operating systems from TechJunkie, Techmyoldtechchannel and TechJuMax Dalton.

ICTICT532 - Encryption files[67]

[67] https://www.youtube.com/embed/videoseries?list=PLr24-CFnxcCyDFwQnWiiqVKGn1SmLpgcC

 © TAFE Queensland 2020

Encrypting hard drives

Windows device encryption

Turn on device encryption

1. Sign into Windows with an administrator account (you may have to sign out and back in to switch accounts). For more info, see Create a local or administrator account in Windows 10.
2. Select the **Start** button, then select **Settings,** then select **Update & Security** , select **Device encryption**.

If **Device encryption** does not appear, it is not available. You may be able to use standard BitLocker encryption instead.

Open Device encryption setting.

1. If device encryption is turned off, select **Turn on**.

Windows BitLocker encryption

Turn on standard BitLocker encryption

1. Sign into your Windows device with an administrator account (you may have to sign out and back in to switch accounts). For more info, see Create a local or administrator account in Windows 10.
2. In the search box on the taskbar, type **Manage BitLocker** and then select it from the list of results. Or, you can select the **Start** button, and then under **Windows System** , select **Control Panel**. In **Control Panel** , select **System and Security** , and then under **BitLocker Drive Encryption** , select **Manage BitLocker**.
3. Note: You will only see this option if BitLocker is available for your device. It is not available on Windows 10 Home edition.
4. Select **Turn on BitLocker** and then follow the instructions.

Mac OS X Lion or later

When FileVault is turned on, your Mac always requires that you log in with your account password.

1. Choose **Apple menu** and select **System Preferences** , then select **Security & Privacy**.
2. Click the **FileVault** tab.
3. Click **Locked** , then enter an administrator name and password.
4. Click **Turn On FileVault**.

 © TAFE Queensland 2020

Linux OS

Most Linux operating systems do not allow for an easy encryption of a hard drive after the initial installation process is complete. The option to encrypt is selected during the steps of the operating system install.

There are optional workarounds; however, it is considered easier to back up your data and re-install the operating system from scratch.

Video

Watch the first video by Britec09 to learn how to encrypt a Windows 10 hard drive and the second, by Hands-On Mac on how to use Filevault for a Mac.

The videos will play one after the other, but if you want to watch them at separate times use the playlist menu in the top right corner of the video.

ICTICT532 - Encrypting hard drives[68]

[68] https://www.youtube.com/embed/videoseries?list=PLr24-CFnxcCy39fyH-3HlmUSlvk661Fyf

 © TAFE Queensland 2020

Hashing

Hashing is used to verify data integrity; it is not encryption. Hashing is achieved by having an algorithm performed on data, such as a file or message, to create a number called a hash (also known as a checksum). The hash is then used to validate that the data has not been modified, tampered with, or corrupted. This is where you can verify the data has maintained integrity.

Integrity of the data is directly linked to the hashing algorithm, if the hash differs at any point, it means that the data has been modified or corrupted.

Example

An IT technician has to update the BIOS on a computer system. When running the actual update to the ROM (Read Only Memory) it applies the data in sections and compares the section that was just updated with the checksum, which is the hash. If the checksum differs, it then reapplies the section again just in case it was a packet of data that did not transfer over properly.

If the checksum fails again, the whole process is stopped, and the BIOS returned to its original condition.

Video

Watch the videos from Lisk and Programming with Professor Sluiter, for more information about hashing and encryption.

The videos will play one after the other, but if you want to watch them at separate times use the playlist menu in the top right corner of the video.

ICTICT532 - Hashing[69]

203379583 / Gustavo Frazao / shutterstock.com

[69] https://www.youtube.com/embed/videoseries?list=PLr24-CFnxcCzYWCJVYjGEbjbH2B10UtYk

 © TAFE Queensland 2020

Hashing algorithms

Some of the common hashing algorithms in use today are detailed below.

MD5

Message Digest 5 (MD5) is a common hashing algorithm that produces a 128-bithash. Hashes are commonly shown in hexadecimal format instead of a stream of 1s and 0s. For example, an MD5 hash is displayed as 32 hexadecimal characters instead of 128 bits. Hexadecimal characters are composed of 4 bits and use the numbers 0 through 9 and the characters a through f.

SHA

Secure Hash Algorithm (SHA) is another hashing algorithm. There are several variations of SHA grouped into four families—SHA-0, SHA-1, SHA-2, and SHA-3:

- SHA-0 is not used.
- SHA-1 is an updated version that creates 160-bit hashes. This is similar to the MD5 hash except that it creates 160-bit hashes instead of 128-bit hashes.
- SHA-2 improved SHA-1 to overcome potential weaknesses. It includes four versions. SHA-256 creates 256-bit hashes and SHA-512 creates 512-bit hashes. SHA-224 (224-bit hashes) and SHA-384 (384-bit hashes) create truncated versions of SHA-256 and SHA- 512, respectively.
- SHA-3 (previously known as Keccak) is an alternative to SHA-2. The U.S. National Security Agency (NSA) created SHA-1 and SHA-2. SHA-3 was created outside of the NSA and was selected in a non-NSA public competition. It can create hashes of the same size as SHA-2 (224 bits, 256 bits, 384 bits, and 512 bits).

HMAC

Another method used to provide integrity is with a Hash-based Message Authentication Code (HMAC). An HMAC is a fixed-length string of bits similar to other hashing algorithms such as MD5 and SHA-1 (known as HMAC-MD5 and HMAC-SHA1). However, HMAC also uses a shared secret key to add some randomness to the result and, only the sender and receiver know the secret key.

RIPEMD

RACE Integrity Primitives Evaluation Message Digest (RIPEMD) is another hash function used for integrity. It is not as widely used as MD5, SHA, and HMAC.

 © TAFE Queensland 2020

Hashing files and messages

Numerous applications calculate and compare hashes automatically, this normally occurs without any user involvement. An example is where a digital signature uses a hash within an email, and email applications automatically create and compare the hashes.

Additionally, there are a number of applications you can use to manually calculate hashes. As an example, the Microsoft Store has a tool developed by DigitalVolcano Software called **Hash Tool**, which is a free program anyone can use to create hashes of files.

Weblink

Visit the link below to see the Digital Volcano hash tool.

Hash Tool[70]

A Google search on “hash tool download” will show a list of applications that are available.

Note

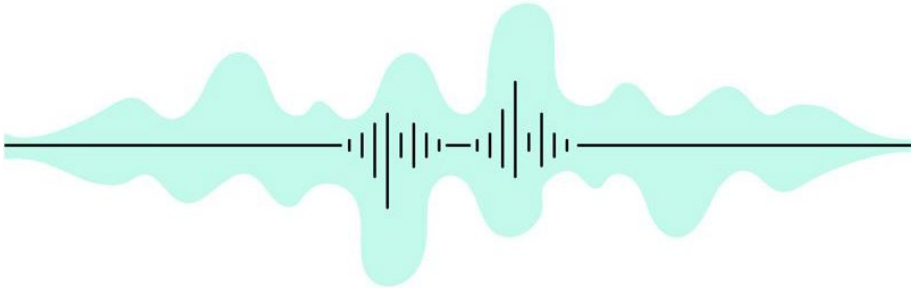
It is worth emphasising that hashes are one-way function. You can calculate a hash on a file or a message, but you cannot use the hash to reproduce the original information. Also, to note, the hash code will always be the same length, no matter how big the file is.

Research

Download a hashing algorithms application to your system.

Copy a number of files to a temporary folder and create a hash for the file.

Compare the hash and see if there is any correlation between each created hash.



1381983182 / Iriejah / shutterstock.com

[70] https://www.digitalvolcano.co.uk/hash.html

© TAFE Queensland 2020

Hashing messages

For integrity when sending for messages, hashing is a good option. Hashing will provide guarantee to a person receiving a message that the message has not been altered or modified.

Scenario

If we look at a scenario where Bill is sending a message to Ted. The message is “The song is almost complete.” As this message may not be secret, there is no need to encrypt it. Although, we do want to establish integrity, so the focus on this description is only on hashing.

In this scenario, something modified the message before it reaches Ted. When Ted receives the message and the original hash, the message is now “The song is nearly almost complete.”

It shows that the message has been modified in transit, but the hash has not changed. A program on Ted’s computer calculates the MD5 hash on the received message as 564294439E1617F5628A3E3EB75643FE. It then compares the received hash with the calculated hash.

- Hash created on Bill’s computer, and received by Ted’s computer: D9B93C99B62646ABD06C887039053F56
- Hash created on Ted’s computer: 564294439E1617F5628A3E3EB75643FE

The above shows that the hashes are different, so it indicates that the message has lost integrity. The program on Ted’s computer would report the discrepancy.

Note

This shows that there could have been a malicious attacker modifying the message, or it could have been a technical problem. However, Ted is now aware that the received message is not the same as the sent message and he should not trust it.

 © TAFE Queensland 2020

Topic summary and review

This topic covered the knowledge and skills needed to understand data integrity, the attacks on data integrity, and how to mitigate these attacks. The topic also covered permission to access data and understanding the difference between data encryption and hashing.

Self-check – Data integrity and authorised access

Which of the following is not a hashing algorithm?

- ☐ HMAC
- ☐ MD5
- ☐ PC-7
- ☐ SHA

If a laptop is stolen, or maybe lost, and the files or hard drive are not encrypted, anyone can access any sensitive information.

- ☐ True
- ☐ False

Two-factor authentication (2FA) is where you will logon to a system, or gain access to an application, using two forms of verification. The first factor is something you know, such as your password and the other is something you have, which is?

- ☐ An asset such as a car or house.
- ☐ A device such as a mobile phone.
- ☐ Knowledge, such as training or experience.

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

Destroying data

Introduction

So let us delete the data, clicking the delete button does not meet the requirements for sensitive personal data. This topic looks at how an organisation retains sensitive information and what steps are required to destroy data or records. At no point does an organisation want to be the next headline in the news because someone found other people's personal information sitting in a garbage bin.

Objectives

By completing this topic, you will be able to:

- understand the retention of data or records
- understand Queensland Government agencies destruction of data procedures
- know Queensland Government agencies documentation
- understand destruction of data for non-government organisations.

518466241 / Photobank.kiev.ua / shutterstock.com

 © TAFE Queensland 2020

Retention of data or records

Retention of records

There are many laws that come into effect with regard to the length of time the records are kept and the way the records are destroyed. In this section, when we use the wording 'records', it has to the same meaning as data, but can be in hard copy and stored or archived in a physical filing system.

To have a better understanding of the destruction of records in an organisation, it is also good to know how long an organisation must retain records, before destroying them.

There are many rules and regulations for different types of data.

- **Common Law** – The general position in common law is that organisational documents are the property of the organisation and they can deal with them anyway they want. The exceptions start to arise in regard to a number of federal and state legislations.
- **Income Tax** – The Income Tax Assessment Act (1936) (Cth) requires, that organisations carrying on a business keep hold of records relevant to the income of the income and expenditure of the organisation, for at least 5 years.
- **Fair Work** – The Fair Work Act 2009 (Cth) requires, that employee records be retained for a minimum of 7 years from the end of the financial year in which the document was created. The scope of employee records is broad, and includes information such as the employment, training, discipline, performance, behaviour, and termination of the employee, as well as the terms and conditions of employment, income, taxation elements and entitlements.
- **NPPs** – The National Privacy Principles (NPPs) also impact organisational record retention and destruction policies. Organisations subject to the NPPs must destroy or de-identify records containing personal and sensitive information if the organisation no longer needs information for the purpose for which it was collected, or for any purpose for which it may be used or disclosed.
- **Tax File Number** – The Privacy (Tax File Number) Rule 2015 [4] also requires organisations to take practical steps to securely destroy or permanently de-identify tax file number information, that is no longer required by law to be retained, or is no longer required for a purpose under taxation law, personal assistance law or superannuation law.
- **Corporations Act** – The Corporations Act 2001 (Cth) also contains various document retention requirements. Financial records must be kept for at least seven years, organisational records such as meeting minutes and registries for at least five years.

 © TAFE Queensland 2020

Destruction of data – Queensland government agencies

Queensland Government

The destruction and transfer of public records must have authorisation from the State Archivist. You can usually get this authorisation through a retention and disposal schedule. Sometimes authorisation may be provided through another legal authority. You also cannot sell, donate, abandon, damage, or amend a record without authorisation.

Before you destroy

Before you destroy records, you must have authorisation to dispose of records from the State Archivist and:

- Seek endorsement from your agency's CEO or authorised delegate.
- Ensure records are not required as evidence for any current or pending legal action (the destruction of evidence is an offence under the Criminal Code Act 1899).
- Check that the records are not required for any Right to Information (RTI) requests.
- Check that records are no longer needed for ongoing business (talk to the relevant business area).
- Consider any other potential reason to retain records–you may need to do a risk assessment if they relate to a high-profile issue (e.g. asbestos).
- Check that no disposal freezes have been issued for the records.

© The State of Queensland 2021, 'Retention, disposal and destruction of records', https://www.forgov.qld.gov.au/information-and-communication-technology/recordkeeping-and-information-management/recordkeeping/retention-disposal-and-destruction-of-records/how-to-destroy-records#-a-name-methods-a-methods-of-destruction, 07/05/2021 CC BY 4.0

1038942481 / Eugen Thome / shutterstock.com

The Queensland Government website has a detailed section on how to destroy records. See the reading link below.

Reading

Please visit this link and read from 'Methods of destruction through to 'Document the destruction of records', Reading time-max 3-4 mins.

'Retention, disposal and destruction of records'[71]

[71] https://www.forgov.qld.gov.au/information-and-communication-technology/recordkeeping-and-information-management/recordkeeping/retention-disposal-and-destruction-of-records/how-to-destroy-records#-a-name-methods-a-methods-of-destruction

© TAFE Queensland 2020

Destruction of data – non-government organisations

What does APP 11 say? – Privacy Act

Legislation

Visit the link below to discover the steps an APP entity needs to take to protect the data it holds and the requirements covering its destruction.

'APP 11–Security of Personal Information'[72]

ISO 27001

The objective of ISO 27001:2013 Annex A.8.1 is about responsibility of assets, including disposal of media.

Weblink

For a description of this Annex, visit the weblink below.

What is the objective of Annex A.8.1[73]

1925795873 / Evgeny Ostroushko / shutterstock.com

[72] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information#what-does-app-11-say

[73] https://www.isms.online/iso-27001/annex-a-8-asset-management/#what-is-annex-a-8-1

© TAFE Queensland 2020

Topic summary and review

This topic covered the knowledge and understanding for the retention of data or records, and how organisations destroy data or records.

Self-check – Destroying data

Which of the following two (2) devices must be physically destroyed if they hold sensitive data?

- ☐ HDD
- ☐ SATA cable
- ☐ DVD
- ☐ Projector

All Queensland Government agencies must obtain authorisation from the State Archivist when destroying data.

- ☐ True
- ☐ False

The ‘reasonable steps’ an organisation should take to destroy sensitive data depend upon circumstances that include? Select the correct option.

- ☐ The amount and sensitivity of the personal information
- ☐ The time available to destroy the sensitive data
- ☐ Authorisation from shareholders

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

Privacy Impact Assessment

Introduction

In this topic for the unit we will be looking at the impact of an organisation's project on the privacy of an individual's personal information, and the steps required.

Objectives

By completing this topic, you will be able to undertake a privacy impact assessment.

1887308413 / Yuriy K / shutterstock.com

 © TAFE Queensland 2020

Undertaking a Privacy Impact Assessment

A privacy impact assessment (PIA) is a scalable tool an agency can use to:

- identify the impact that a project might have on the privacy of an individual's personal information
- make recommendations on how to manage any negative impacts.

This guideline sets out the key steps involved in a PIA and what each of those steps involves. A PIA report template is also available for agencies and health agencies to tailor as necessary, to meet the needs of the project and the agency.

© The State of Queensland (Office of the Information Commissioner) 2012, 'Undertaking a Privacy Impact Assessment', https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment, 07/05/2021 CC BY 3.0

Weblink

Access the link below and read the Queensland Information Commissioner's guide to undertaking a PIA.

'Undertaking a Privacy Impact Assessment'[74]

1290531400 / chainarong06 / shutterstock.com

[74] https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment

Topic summary and review

This topic covered the knowledge and understanding of what a Privacy Impact Assessment (PIA) is, and how to undertake a PIA for an organisation.

Self-check – Privacy impact assessment

PIA stands for Privacy Intervention Assessment.

- ☐ True
- ☐ False

Which of these is not a reason to do a PIA? Select the correct option.

- ☐ Support good governance and informed decision-making.
- ☐ Identify problems early when it is easier and cheaper to address them.
- ☐ Address community concerns and build trust in the agency's information handling practices.
- ☐ Because it is mandatory.

How many steps are in a PIA normally?

- ☐ 7
- ☐ 8
- ☐ 12
- ☐ 9

Check your answers at the end of this Learner Guide

 © TAFE Queensland 2020

Ethics in the workplace

Introduction

In this last topic for the unit will be looking at what ethics and the code of practice is. The topic discusses the importance to an organisation of ethical behaviour, and how this affects the perceived appearance to clients and the performance of staff.

Objectives

By completing this topic, you will be able to:

- understand and define ethics in the workplace
- have knowledge of what ethics is
- understand the components and importance of a code of conduct policy.

292917414 / Web Buttons Inc / stock.adobe.com

 © TAFE Queensland 2020

What defines ethics in the workplace?

What is the definition of ethics in the workplace?

Ethics in the workplace is described as the principal code that guides the conduct of employees in respect to what is right and wrong in regard to conduct and decision making.

Workplace ethical decision making takes into account the individual employee's best interest and also takes into account the best interest of those impacted. Ethical behaviour does not only apply to individual employees, but the organisation also should demonstrate standards of ethical conduct.

Why is ethical behaviour in the workplace important?

The presence of an ethical workplace can have many advantages and the absence of ethics can have a negative impact on the workplace.

- **Positive influence** – Ethical behaviour in the workplace can have a positive influence on staff that can produce growth in many areas for an organisation. The opposite can also happen if unethical behaviour is allowed to fester in the workplace.
- **Mutual expectation** – Organisational stakeholders (individuals, internal and external groups and organisations) enter into a partnership with a business organisation with a mutual expectation that stakeholders and business organisations behave in an ethical manner, and in each other's best interest.
- **Reputational damage** – A decision to act unethically, by the organisation or a stakeholder, can strain the relationship and damage the reputation of the organisation. Today with social media now playing a major role in not only an organisation's reputation but also an individual's, that reputation can be easily tarnished by unethical behaviour that is against community expectations.

An organisation that is understood to act ethically by staff can achieve positive benefits and increased business results. The awareness of ethical behaviour can have many benefits.

- Increased employee performance
- Job satisfaction
- Organisational commitment
- Trust

 © TAFE Queensland 2020

What are ethics?

In an organisation, management may supply a new employee with documentation about workplace ethics. The documentation itself may come in the form of an employee handbook, or a code of conduct. Whichever form the documentation comes in, there will be a breakdown within the document that has sections on different types of ethical behaviour.

Common workplace ethics:

- Commitment.
- Faithfully focused on the job, the organisation's missions, and goals.
- Honesty.
- Speaks the truth, keeps promises, follows the organisational and community rules, and has respect for other people's property.
- Professionalism.
- Acts and speaks in an appropriate social standard at work. Maintains work responsibility in performance and results.
- Tolerance.
- Respect for others regardless of ethical background, sex, age, religion, politics, and including respecting differences of opinions, suggestions, and perspectives.
- Dependability.
- Accomplishes work in a professional manner and takes pride in what they do.
- Desire to learn.
- Open to learn new processes, procedures, and systems in a constantly changing environment.

Some organisations may also include the following ethics.

- Primacy of public interest.
- Place the interests of the community above those of personal, business, or sectional interests.
- Enhancement of quality of life.
- Strive to enhance the quality of life of those affected by your work.

 © TAFE Queensland 2020

Codes of conduct

The purpose of a code of conduct is to provide a clear understanding of the standard of conduct expected when performing duties as an employee of an organisation.

The code of conduct places an obligation on all employees to take responsibility for their own conduct. To achieve this, all employees are expected to familiarise themselves with, and act in accordance with, the code of conduct.

Creating a code of conduct

Creating a code of conduct for an organisation can be a complicated and time-consuming undertaking. Two of the key aspects of this process are outlined below.

- **Drafting** – Creating a code of conduct normally requires a draft, and then possibly a number of revisions until the document meets with satisfaction from everyone involved. Therefore, it would be best to have a collaborative approach to the development of the document, and involve feedback from as many staff members as possible. Also, at every level of the organisation, which should include management, human resources staff, and other appropriate team members.
- **Adaptation** – There are very few businesses that operate exactly the same, therefore you will rarely have a number of organisations that have precisely the same code of conduct documentation. The code of conduct document needs to be adapted to match the different requirements of the organisation and their unique conditions. Over the long term, by understanding the consideration of the different characteristics of the organisation, the code of conduct document will be easier to implement and manage.

398445461 / photon_photo / stock.adobe.com

 © TAFE Queensland 2020

Below are some examples of good policies for a code of conduct.

Example

- What is and is not acceptable behaviour in the workplace.
- How to treat with equal respect all staff, management, and clients.
- The importance of good behaviour and the effect it has on the work environment.
- Examples of expected ethics and values to uphold.
- How to comply with relevant industry legislation.
- Clear examples of misconduct, serious misconduct, and the result of such actions.

Important

You should always release a draft of the document so as to obtain feedback from all staff and stakeholders. One final note, always compare the draft code of conduct document to the other organisational policies to make sure they align properly.

Weblink

For information about writing a code of conduct document, please visit the Queensland Government – Business Queensland website:

Writing a code of conduct[75]

The following link will take you to the i-sight.com website that has examples of different code of conduct documents used by major world-wide brand names.

18 of the Best Code of Conduct Examples[76]

[75] https://www.business.qld.gov.au/running-business/employing/taking-on-staff/staff-code-conduct/writing

[76] https://i-sight.com/resources/18-of-the-best-code-of-conduct-examples/

 © TAFE Queensland 2020

Implementing the code of conduct in the workplace

It is not enough just to write a code of conduct document for an organisation, it needs to be implemented to have any impact. To implement any type of policy or procedure communication is one of the keys to success. Another key is for management to take a lead role and lead by example.

There are many examples in all industries where management will enforce anti-bullying policies, only to be breaking these guidelines themselves. Some organisations will develop and implement a range of policies and procedures so as to gain government contracts, with no intentions of ever abiding by them.

Management needs to uphold the same values and ethics too. There are many ways to communicate the code to staff, however, be mindful of language barriers and the availability of information as obstacles to effective implementation. Selecting the right channels to get the message across is important.

Methods of delivering the code

The Business Queensland website has a clear and informative guide to delivering a code of conduct. Take a couple of minutes to read their step-by-step guide.

Weblink

The Business Queensland website has a clear and informative guide to delivering a code of conduct. Take a couple of minutes to read their step-by-step guide. Select the link below to go to the website.

Implementing a code of conduct[77]

372023873 / misterauto / stock.adobe.com

[77] https://www.business.qld.gov.au/running-business/employing/taking-on-staff/staff-code-conduct/implementing

 © TAFE Queensland 2020

Topic summary and review

This topic covered the knowledge and understanding of ethics in the workplace and what is involved in creating a code of conduct policy.

Self-check – Ethics in the workplace

Select two (2) of the following that you think would be an ethics category

- ☐ Tolerance
- ☐ Earnings
- ☐ Honesty
- ☐ Relationship status

Complying with relevant industry legislation is acceptable behaviour in the workplace.

- ☐ True
- ☐ False

Which two (2) of the following are methods for delivering the code of conduct?

- ☐ Online training course
- ☐ BBQ at the manager's residence
- ☐ Drinks on a work night
- ☐ Employee handbook

Check your answers at the end of this Learner Guide

© TAFE Queensland 2020

Self-check answers

Self-check – Policies and procedures

Identify two benefits of having workplace policies.

- [x] Clarify functions and responsibilities
- [ ] Identifies correct wage levels
- [x] Fosters stability
- [ ] Discount codes for online purchases

In business, the word alignment is used to describe the process of developing systems to support needs of the company.

- [x] True
- [ ] False

SOP is an acronym for?

- [ ] Systems Officer Programming
- [x] Standard Operating Procedures
- [ ] Simply Off Putting
- [ ] Standard Offset Policy

© TAFE Queensland 2020

Self-check – Legislation standards and policies

In which year was the Privacy Act enacted?

- ☐ 1984
- ☑ 1988
- ☐ 1996

The Queensland Information Privacy Act 2009 covers all businesses in Queensland.

- ☐ True
- ☑ False

Which ISO 27001 standard includes the appraisal and management of information security risks?

- ☑ ISO/IEC 27001:2013
- ☐ ISO/IEC 27001:2015
- ☐ ISO/IEC 27002:2013

© TAFE Queensland 2020

Self-check – Company privacy policies

The Privacy Act allows an individual to? Select the correct option/s.

- ☐ Have the option of not identifying yourself, or of using a pseudonym in certain circumstances.
- ☐ Ask for access to their personal information (including health information).
- ☐ Stop receiving unwanted direct marketing.
- ☑ All the above.

A Privacy Policy could also be known as a Responsible Use of Data Policy?

- ☑ True
- ☐ False

The Office of the Australian Information Commissioner has released a guide for securing personal information called?

- ☑ Guide to securing personal information – Reasonable steps to protect personal information.
- ☐ Guide to securing personal information – The step-by-step to protect personal information.
- ☐ Guide to securing personal information – 'Nearly all steps' to protect personal information.

© TAFE Queensland 2020

Self-check – Copyright

In Australia, the Copyright Act 1968 is the law that governs copyright.

- ☑ True
- ☐ False

The Copyright Act does allow you to use material without permission if you cannot contact the copyright owner.

- ☐ True
- ☑ False

Of the two (2) statements below, which one is correct?

- ☑ Unless the source states that the owner of the text or media file gives you permission to use the resource, either by a statement on the web site or verification by email, then no permission is granted until a yes is confirmed.
- ☐ After exhausting all avenues to identify and obtain permission from the copyright owner without success, you can contact and fill out the appropriate form to use the resource.

Before using copyrighted resources, you will need to obtain copyright clearance for their intended use.

- ☑ True
- ☐ False

© TAFE Queensland 2020

Self-check – Intellectual property

Domain names for websites are classed as intellectual property.

- ☐ True
- ☑ False

All concepts and processes have design rights protection.

- ☐ True
- ☑ False

A standard patent lasts for up to how many years?

- ☐ 15
- ☐ 30
- ☑ 20
- ☐ 50

© TAFE Queensland 2020

Self-check – Data

The Privacy Act allows an individual to:

- ☐ have the option of not identifying yourself, or of using a pseudonym in certain circumstances
- ☐ ask for access to your personal information (including your health information)
- ☐ stop receiving unwanted direct marketing
- ☑ All the above

Types of personal information can include ‘health information’, ‘credit information’, and ‘tax file number information’.

- ☑ True
- ☐ False

Which one of the following is defined in the Privacy Act as sensitive information?

- ☐ Sports club membership
- ☑ Racial or ethnic origin
- ☐ Opinion of the best NRL team

© TAFE Queensland 2020

Self-check – Sending and receiving sensitive data

Under APP 11.2, APP entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed.

- [x] True
- [ ] False

Under APP 3, you should only collect personal information that is reasonably necessary to carry out your functions or activities.

- [x] True
- [ ] False

Which one of the following is true in regard to emailing sensitive information?

- [ ] Use non-encryption messaging for speed and accuracy.
- [x] Obtain a recipient's consent to send their own personal information to them via email.
- [ ] Send the email addressed to the recipient and resend the unencrypted email if unsuccessful.

© TAFE Queensland 2020

Self-check – File location

Three (3) options for file storage are onsite storage, cloud storage, or a mixture of both.

- [x] True
- [ ] False

Which of the following is not a file storage area?

- [ ] HDD
- [ ] NAS
- [x] NVMe
- [ ] Cloud

Which one of the following is not a cloud service?

- [ ] Amazon Web Service
- [x] Cumulus cloud
- [ ] Azure Cloud

© TAFE Queensland 2020

Self-check – Data integrity and authorised access

Which of the following is not a hashing algorithm?

- ☐ HMAC
- ☐ MD5
- ☑ PC-7
- ☐ SHA

If a laptop is stolen, or maybe lost, and the files or hard drive are not encrypted, anyone can access any sensitive information.

- ☑ True
- ☐ False

Two-factor authentication (2FA) is where you will logon to a system, or gain access to an application, using two forms of verification. The first factor is something you know, such as your password and the other is something you have, which is?

- ☐ An asset such as a car or house.
- ☑ A device such as a mobile phone.
- ☐ Knowledge, such as training or experience.

© TAFE Queensland 2020

Self-check – Destroying data

Which of the following two (2) devices must be physically destroyed if they hold sensitive data?

- ☑ HDD
- ☐ SATA cable
- ☑ DVD
- ☐ Projector

All Queensland Government agencies must obtain authorisation from the State Archivist when destroying data.

- ☑ True
- ☐ False

The ‘reasonable steps’ an organisation should take to destroy sensitive data depend upon circumstances that include? Select the correct option.

- ☑ The amount and sensitivity of the personal information
- ☐ The time available to destroy the sensitive data
- ☐ Authorisation from shareholders

© TAFE Queensland 2020

Self-check – Privacy impact assessment

PIA stands for Privacy Intervention Assessment.

- ☐ True
- ☑ False

Which of these is not a reason to do a PIA? Select the correct option.

- ☐ Support good governance and informed decision-making.
- ☐ Identify problems early when it is easier and cheaper to address them.
- ☐ Address community concerns and build trust in the agency's information handling practices.
- ☑ Because it is mandatory.

How many steps are in a PIA normally?

- ☐ 7
- ☐ 8
- ☐ 12
- ☑ 9

© TAFE Queensland 2020

Self-check – Ethics in the workplace

Select two (2) of the following that you think would be an ethics category

- ☑ Tolerance
- ☐ Earnings
- ☑ Honesty
- ☐ Relationship status

Complying with relevant industry legislation is acceptable behaviour in the workplace.

- ☑ True
- ☐ False

Which two (2) of the following are methods for delivering the code of conduct?

- ☑ Online training course
- ☐ BBQ at the manager's residence
- ☐ Drinks on a work night
- ☑ Employee handbook

© TAFE Queensland 2020

References

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities/, viewed 22/04/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/australian-privacy-principles, viewed 22/04/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/data-breaches/what-is-a-data-breach/, viewed 22/04/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach/, viewed 22/04/2021

Queensland Consolidated Acts, INFORMATION PRIVACY ACT 2009 - SECT 3 Object of Act, http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/qld/consol_act/ipa2009231/s3.html, viewed 23/04/2021

Queensland Consolidated Acts, INFORMATION PRIVACY ACT 2009 - SECT 12 Meaning of personal information, http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/qld/consol_act/ipa2009231/s12.html#personal_information, viewed 23/04/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/collection-of-personal-information/#:~:text=An%20organisation%20may%20only%20collect,unless%20the%20information%20is%20sensitive, viewed 26/04/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/use-and-disclosure-of-personal-information/, viewed 26/04/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/, viewed 27/04/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/about-us/our-corporate-information/key-documents/privacy-policy/, viewed 27/04/2021

Australian Law Reform Commission website – www.alrc.gov.au, 16.08.2010, https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/6-the-privacy-act-some-important-definitions/sensitive-information/, viewed 29/04/2021

 © TAFE Queensland 2020

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/#:~:text=The%20Privacy%20Act%20defines%20%27personal,a%20material%20form%20or%20not., viewed 29/04/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/, viewed 30/04/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties/#ftn1, viewed 04/05/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/, viewed 05/05/2021

Queensland Government, how to destroy records, 27/04/2021, https://www.forgov.qld.gov.au/how-destroy-records#-a-name-methods-a-methods-of-destruction, viewed 07/05/2021

Office of the Australian Information Commissioner website — www.oaic.gov.au, https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/#what-does-app-11-say, viewed 07/05/2021

ISMS.online, ISO 27001 – Annex A.8: Asset Management, https://www.isms.online/iso-27001/annex-a-8-asset-management/, viewed 07/05/2021

© The State of Queensland (Office of the Information Commissioner) 2012, Undertaking a Privacy Impact Assessment, 25/07/2018, https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment, viewed 07/05/2021

IP Australia, IP Explained, 04/02/2021, https://www.ipaustralia.gov.au/understanding-ip/getting-started-ip/ip-explained, viewed 27/07/2021

IP Australia, Patents Explained, 11/11/2020, https://www.ipaustralia.gov.au/patents/understanding-patents/patent-basics, viewed 27/07/2021

IP Australia, Trademarks Explained, 11/06/2019, https://www.ipaustralia.gov.au/trade-marks/understanding-trade-marks/trade-mark-basics, viewed 27/07/2021

IP Australia, What Is Design Right, 06/10/2020, https://www.ipaustralia.gov.au/designs/understanding-designs/what-design-right, viewed 27/07/2021

IP Australia, PBR Basics, 01/07/2019, https://www.ipaustralia.gov.au/plant-breeders-rights/understanding-pbr/pbr-basics, viewed 27/07/2021

Australian Government Business © Commonwealth of Australia 2020, Policies, procedures, and processes, viewed 24/06/2020, https://business.gov.au/risk-management/risk-assessment-and-planning/policies-procedures-and-processes, viewed 28/07/2021

Queensland Government Business Queensland, Business processes, procedures, and standards, 21/05/2021, https://www.business.qld.gov.au/starting-business/planning/business-planning/processes-procedures-standards, viewed 29/07/2021

© State of New South Wales through NSW Industrial Relations, Workplace Policies and Procedures Checklist, https://www.industrialrelations.nsw.gov.au/employers/nsw-employer-best-practice/workplace-policies-and-procedures-checklist/, viewed 29/07/2021

Business Victoria, Privacy policy template, 31/03/2021, https://business.vic.gov.au/tools-and-templates/privacy-policy-template, viewed 29/07/2021

Queensland Government – Business Queensland, Implementing a code of conduct, 25/05/2020, https://www.business.qld.gov.au/running-business/employing/taking-on-staff/staff-code-conduct/implementing, viewed 16/08/2021