|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Name |  | Student Number | |  |
| Unit Code/s & Name/s | VU23223 Apply cyber security legislation, privacy and ethical practices | | | |
| Cluster Name  *If applicable* | N/A | | | |
| Assessment Name | Cyber security legislation, privacy and ethical practices Portfolio | Assessment Task No. | | 2 of 2 |
| Assessment Due Date | Week 8 | Date submitted | | / / |
| Assessor Name |  | | | |
| **Student Declaration:** I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature. | | | | |
| Student Signature |  | | Date | / / |
| **PRIVACY STATEMENT:** TAFE Queensland is collecting your personal information on this form for the purpose of assessment. In accordance with the Information Privacy Act 2009 (Qld), your personal information will only be accessed by staff employed by TAFE Queensland for the purposes of conducting assessment. Your information will not be provided to any other person or agency unless you have provided TAFE Queensland with permission, if authorised under our Privacy Policy (available at <https://tafeqld.edu.au/global/privacy-policy.html>) or disclosure is otherwise permitted or required by law. Your information will be stored securely. If you wish to access or correct any of your information, discuss how it has been managed or have a concern or complaint about the way the information has been collected, used, stored, or disclosed, please contact the TAFE Queensland Privacy Officer at [privacy@tafeqld.edu.au](mailto:privacy@tafeqld.edu.au) | | | | |

|  |  |
| --- | --- |
| **Instructions to Student** | **General Instructions:**  You are employed by MidTown IT as a Cyber Security Analyst/Consultant. Your task is to analyse the cyber security legislative requirements of two organisations and prepare a written report on each organisation. The organisations are:  Angelonia Fashion and Turtle Movers.  Your teacher/assessor will take on the role of the Project Manager assigned to this project by MidTown IT.  Read the project documentation provided and familiarise yourself with the Project Scenario or Case Study before proceeding with portfolio tasks. Confirm anything you are not sure about the project with your manager (teacher/assessor). It is essential that you have a clear understanding of the scenario and tasks that you need to complete.  This assessment instrument requires the student to complete a project portfolio that is divided into four (4) parts:   * PART 1 Review of cyber security legislative and regulatory requirements for Australian organisations * PART 2 Examine an organisation’s policies and procedures compliance * PART 3 Review an organisation’s ethical practices and procedures * PART 4 Contingency task   **Storage Devices:**   * Students are required to provide their own storage device.   **Materials Required:**   * Access to PCs and peripherals * Access to the Internet * Access to Connect (LMS) * Access to Word processing software, such as Microsoft Word * Access to special-purpose tools, equipment and materials to complete the assessment.   **Online Delivery:**   * Student to supply their own PC or laptop and peripherals and internet access * Students will require permission to install the required software * Students will require access to Microsoft Office or similar application   **Documentation:**   * MidTown IT Scenario or Case Study * MidTown IT Cyber Legislation and Policies Report Template * Policy and Privacy Practices for the two organisations   **Assessment Criteria:**  To achieve a satisfactory result, your assessor will be looking for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard. Demonstrated ability to:   * Identify Federal, State/Territory and sector-specific legislation * Identify relevant international legislation that affects Australian organisations * Recognise interdependencies between regulators and legislative instruments * Identify current legislation reforms * Determine compliance with policies and procedures against current standards * Understand red and blue team tools and the consequences of misusing skills gained through their implementation * Consequences of unethical behaviour regarding cyber security practices   Refer to the marking criteria for specific details:  VU23223\_AT2\_MC\_TQM\_V1  **Details of location:**  TAFE will provide a simulated work environment in the classroom. Research activities may be conducted in the classroom or at home.  If you are unable to attend a scheduled assessment activity, you must notify your teacher before the assessment is due and supply a doctor's certificate and approval from the team manager for an extension.  **Time restrictions:**  This assignment is designed to take place over 8 weeks or approximately 32 hours. The student is expected to attend classes as per timetable details and should be able to commit up to 3 hours per week of their own time to study or study related activities.  **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Level of assistance permitted:**  Staff cannot directly show students answers or solutions but support and guide them to complete tasks individually. Teachers and tutors should be available in class, and accessible by email for students working from home.  **Reasonable Adjustments:**  Reasonable adjustments are available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. Talk to your teacher, counsellor or disability officer if you require extra support or an extension based on the conditions identified.  **Number of Attempts:**  You will receive up to two (2) attempts at this assessment task. Should your 1st attempt be unsatisfactory (U), your teacher will provide feedback and discuss the relevant sections / questions with you and will arrange a due date for the submission of your 2nd attempt. If your 2nd submission is unsatisfactory (U), or you fail to submit a 2nd attempt, you will receive an overall unsatisfactory result for this assessment task. Only one re-assessment attempt may be granted for each assessment task.  ***For more information, refer to the Student Rules.***  **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Submission details** | **Evidence Required to be Submitted:**  Insert your details on the cover page and sign the Student Declaration. Include this template with your submission.  **Submission via Connect:**  Upload a single file into Assessment 2 (AT2) Assignment Folder in Connect.  Multiple files can be compressed into a single file.  Name the file:  VU23223\_AT2\_Surname\_Student Number  TAFE Queensland Learning Management System (Connect)  **Accessing Connect:**  Connect URL: https://connect.tafeqld.edu.au/d2l/login  Username: 9 digit student number  Password: <your password>  For password reset go to: <https://passwordreset.tafeqld.edu.au/default.aspx> |
| **Instructions to Assessor** | **Specifications of assessment:**  To be judged competent in this assessment item the student is required to demonstrate competence in all indicators shown in the marking guide.  Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the cyber security field of work and include access to:   * project requirements   Ensure that students read and familiarise themselves with the Project Scenario provided and relevant files and/or resources before attempting the assessment.  **Storage Devices:**   * Students are required to provide their own storage device.   **Materials Required:**   * Access to PCs and peripherals * Access to the Internet * Access to Connect (LMS) * Access to Word processing software, such as Microsoft Word * Access to special-purpose tools, equipment and materials to complete the assessment.   **Online Delivery:**   * Student to supply their own PC or laptop and peripherals and internet access * Students will require permission to install the required software * Students will require access to Microsoft Office or similar application   **Documentation:**   * MidTown IT Scenario or Case Study * MidTown IT Cyber Legislation and Policies Report Template * Privacy Policy and Privacy Practices for the two organisations   **Level of Assistance Permitted:**  Teachers and tutors should be available in class, and accessible by email for students working from home. Staff cannot directly show students answers but support and guide them to complete tasks individually. Students with disability will receive reasonable adjustments.  **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Contingencies:**  Reasonable adjustment is available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances.  **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Note to Student** | An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.  If you have any question or need help regarding this assessment item please contact your teacher/tutor through email or during face-to-face sessions. |

# Project Scenario

MidTown IT employs you as a Cyber Security Analyst/Consultant. Your task is to analyse two organisations' cyber security legislative requirements and prepare a written report on each. The organisations are:

Angelonia Fashion and Turtle Movers.

Your teacher/assessor will take on the role of the Project Manager assigned to this project by MidTown IT.

Although the clients are from two very different industry sectors, they have some common points:

* Both started a small family business
* Have grown too fast to keep pace with technology
* Are concerned about their cyber security compliance with legislation.

The major differences between the two organisations are:

* Industry sectors
* Only one company trades internationally (Angelonia)
* Turtle Movers trades only online
* Angelonia has both a physical and online presence

**ORGANISATION 1 - Angelonia Fashion**

Started 10 years ago as a small family business that employed 3 people. They were the owners of a local fashion shop that specialised in garment arrangements and sold Australian labels primarily.

Today they employ 40 people distributed across Australia.

They have created their own fashion label and export their creations internationally.

Company headquarters: Southport, Gold Coast.

The company has 7 shops across Australia:

NSW - 3 shops

Qld – 2 shops

VIC – 2

Data transactions include:

* Physical and online sales
* Online ordering
* Refunds
* Credit card payments and bank transfers with major fabric and haberdashery suppliers - nationally and internationally

They operate a basic security setup to run their website and database. Their security includes:

* Strong passwords
* Firewall
* Backups

**ORGANISATION 2 - Turtle Movers**

A small removalist family business started with 2 trucks 7 years ago and operated mainly in NSW.

Today they have a fleet of 50 trucks of different capacities and operate across Australia.

The company operates strictly online, and its only physical presence is its headquarters in Sydney, NSW.

Online data transactions are handled through their website. The transactions include:

* Bookings
* Cancellations and rescheduling
* Insurance
* Payments through credit cards and bank transfers
* Refunds
* Client reward and loyalty benefits, for example, referrals.

Management has acknowledged concern about their online security and cyber legislation compliance. Their security system is basic as they rely upon the protection offered by the website provider and an in-house self-trained security person.

**Portfolio Instructions:**

You need to provide two reports, one for each organisation presented in the scenario.

Use the templates provided to complete the two reports.

**Legislation, standards and regulators**

To give you a starting point, the list below contains examples of relevant legislation, standards and regulators. As these are subject to changes and updates, you should carry out your own research to confirm their currency. You are encouraged to add additional legislation, standards and regulators and if they apply to the organisation’s needs.

**Commonwealth Legislation**. Examples are:

* + Telecommunications (Interception & Access) Act 1979
  + Criminal Code Act 1995
  + Corporations Act 2001 (Cth) on their IT management systems (Australian Securities and Investments Commission (ASIC) Regulatory Guide 104: Licensing: Meeting the general obligations)
  + Privacy Act 1988

**Australian Regulators**. Examples are:

* + Australian Prudential Regulation Authority (APRA) - CPS 234 (Prudential regulator)
  + Australian Securities and Investments Commission (ASIC) (Corporate Regulator)
  + Australian Competition and Consumer Commission (ACCC) (Consumer & consumer data rights)
  + Australian Energy Sector Cyber Security Framework (AESCSF) (Energy regulator)
  + Protective Service Manual (Australian Government rules for cybersecurity)
  + Australian Signals Directorate (ASD)
  + Australian Cyber Security Centre (ACSC)

**International Law and conventions**. Examples are:

* + Budapest convention (Convention on Cyber Crime)
  + Australian Criminal Code Act 1995
  + Payment Card Industry Data Security Standard (PCI DSS) (payment cards)
  + General Data Protection Regulation (GDPR)

**Global Standards.** Examples are:

* + ISO/IEC 27001 information security management systems
  + AS 27701: 2022 Security techniques – Extension to ISO/IEC 27001
  + NIST SP 800-53 & Essential 8

**PART 1 Review of cyber security legislative and regulatory requirements for Australian organisations**

This part of the assessment must be completed for **each organisation** presented. The organisations correspond to two industry sectors.

* 1. Read the scenario and complete the following tasks:

1. Provide an overview of the sector of the scenario presented
2. Identify the current Federal, State/Territory and sector-specific cyber security and related legislation that applies to the organisation. Use the table below to present the information.

You can use the table below to provide the answer.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SECTOR:** |  | | | |
| **CYBER SECURITY and related**  **LEGISLATION** | **SCOPE** | | | **BUSINESS AREAS/ACTIVITIES AFFECTED** |
| **Federal** | **State** | **Territory** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  | Add rows as required |

* 1. For **each organisation** presented, analyse their business operations:

1. Identify if there is any international cyber security legislation that has an impact on their data security
2. Identify the areas of the business affected by the international legislation
3. Evaluate the impact on the business operation and data security

You can use the table below to provide the answer for a), b) and c).

|  |  |  |
| --- | --- | --- |
| **INTERNATIONAL**    **CYBER SECURITY**  **LEGISLATION** | **BUSINESS AREAS/ACTIVITIES AFFECTED** | **IMPACT on BUSINESS OPERATIONS and DATA SECURITY** |
|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | Add rows as required |  |

* 1. For **each organisation**,identify and explain at least one (1) interdependency between different legislative instruments related to cyber security.
  2. For **each organisation**, identify one (1) instance where a regulator can contribute to the security of business data operations. Clarify the impact of the contribution.
  3. For each of the regulators presented below, identify and explain their role and scope.

|  |  |  |
| --- | --- | --- |
| **REGULATOR** | **ROLE** | **SCOPE** |
| Australian Prudential Regulation Authority (APRA) |  |  |
| Australian Securities and Investments Commission (ASIC) |  |  |
| Australian Competition and Consumer Commission (ACCC) |  |  |
| Australian Energy Sector Cyber Security Framework (AESCSF) |  |  |
| Protective Service Manual (Australian Government rules for cybersecurity) |  |  |

* 1. Investigate current and upcoming reforms in privacy legislation and explain how these could benefit **each organisation**.
  2. Investigate current and upcoming reforms in consumer and surveillance legislation and explain how these could benefit **each organisation**.
  3. After completing the review of the two organisations in the preceding tasks, write the recommendations you would make as the Cyber Analyst/Consultant for each organisation, regarding:
  4. Compliance with legislation and regulatory requirements
  5. International cyber security legislation impacting their businesses
  6. Potential impact of upcoming reforms in privacy and consumer and surveillance legislation

**PART 2 Examine organisations’ policies and procedures compliance**

This part of the assessment must be completed for **each organisation** presented.

2.1 Examine the privacy documentation provided. Review policy compliance across the organisation against current standards. Current privacy standards can be understood as the Australian Privacy Principles (APPs).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **POLICY** | **STANDARDS/**  **APPS** | **REVIEW DETAILS** | **COMPLIANCE** | | | |
| **Full** | **Partial** | **Poor** | **Non-Compliance** |
| **Privacy Policy** |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Add rows as required |  |  |  |  |  |

2.2 Access the Organisational Practices from the documentation provided for the two organisations. For each organisation, select two (2) practices that could be improved.

a) Evaluate each practice and identify their shortcomings

b) Propose improvements for each practice selected.

|  |  |  |
| --- | --- | --- |
| **BEST PRACTICES** | **EVALUATION/SHORTCOMINGS** | **PROPOSED IMPROVEMENTS** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

2.3After examining the two organisations’ privacy policies and practices, write a report including your findings and a set of recommendations for each organisation, regarding:

a) The level of compliance with current privacy legislation and required improvements

b) Adequacy of current practices and required improvements

**PART 3 Review the organisations’ ethical practices and procedures**

This part of the assessment must be completed for **each organisation** presented.

3.1 Identify and describe four (4) red team tools the organisation could use to exploit and compromise blue team defences.

3.2 Identify and describe four (4) blue team tools the organisation could use to protect the network from cyber-attacks.

3.3 Outline a set of ethical practices employees can apply when using red and blue team tools in public networks.

3.4 Consequences of unethical behaviour:

a) Outline the legal consequences of misusing skills gained using red and blue team tools and the potential data breaches that can occur when using these skills unauthorised.

b) Outline the consequences of unauthorised access to network devices

c) Outline the consequences of bypassing copyright media and applications obtained via file sharing or downloading

3.5 Identify a minimum of four (4) examples of unethical behaviour that could happen in the organisations by the hand of cyber security technicians. For each example, explain the impact on the overall network and data security.

|  |  |
| --- | --- |
| **UNETHICAL BEHAVIOUR** | **IMPACT ANALYSIS** |
|  |  |
|  |  |
|  |  |
| Add rows as required |  |

3.6 **Ethics Code of Practice**

Select one of the two organisations presented and prepare an Ethics Code of Practice for their cyber security technicians. Explain how the code will be distributed and implemented in the organisation.

3.7 Identify three (3) downloading file-sharing services. For each service, identify its suitability and the security risks associated with it.

|  |  |  |
| --- | --- | --- |
| **FILE-SHARING SERVICE (Downloading)** | **SUITABILITY** | **ASSOCIATED SECURITY RISKS** |
|  |  |  |
|  |  |  |
|  |  |  |

**PART 4 Contingency task**

4.1 Assume that due to staff shortages, two junior cyber security technicians have been assigned responsibilities above their expertise level. They are happy with the new job but concerned about their new responsibilities. Provide at least three (3) support measures that could be used to ease their role transition.

**End of Assessment**