|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Name | Amirmahdi Sarikhanifard | Student Number | | 474807620 |
| 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 |  | Date Submitted | | 24 / 09 /2024 |
| 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 | Amirmahdi Sarikhanifard | | Date | 24 / 09 /2024 |
| **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 regarding 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:  Part1: 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, peripherals and internet access  Students will require permission to install the required software  Students will require access to Microsoft Office or a 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, as well as 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 can 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** (if relevant) | **Evidence Required to be Submitted:**  Insert your details on page 1 and sign the Student Declaration. Include this form 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  Assessment to be submitted via:   * TAFE Queensland Learning Management System (Connect): [*https://connect.tafeqld.edu.au/d2l/login*](https://connect.tafeqld.edu.au/d2l/login) * **Username:** 9 digit student number * **For Password:** Reset password go to: [*https://passwordreset.tafeqld.edu.au/default.aspx*](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, peripherals and internet access  Students will require permission to install the required software  Students will require access to Microsoft Office or a 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 can 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. You are also allowed to research online, using appropriate referencing when doing so. 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 questions or need help regarding this assessment item, please contact your teacher/tutor through email or during face-to-face sessions.* |

|  |  |
| --- | --- |
| Scenario-01 | 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 primarily sold Australian labels.

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 shops

**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 which 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 concerns 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 applicability. You are encouraged to add additional legislation, standards and regulators 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

First organization’s sector:  
Fashion covers a wide range of activities related to the design, production, marketing, and retail of clothing itself and clothing accessories. It is a competitive industry which is over influence of people’s preferences. It also has recently has used E-commerce to enhance its market by providing the online market for people who keen to perform online shopping. It deals with both local and global brands.

Second organization sector:  
It is a critical sector where they organize movements of goods around Australia. As there was a explode in online shopping, they also have been benefiting from this and transferring goods after purchases. They are dealing with different types of cargo and customer needs. They are also are having a wide range of data collected from bookings, cancellations and their reward cards.

1. 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.

I used the below table to answer.

You can use the table below to provide the answer.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SECTOR: | Fashion Retail, Garment Arrangements, Fashion Label Creation, Retail and Online Sales | | | |
| CYBER SECURITY and related  LEGISLATION | SCOPE | | | BUSINESS AREAS/ACTIVITIES AFFECTED |
| Federal | State | Territory |
| Australian Cyber Security Centre (ACSC) Guidelines |  |  |  | Their employees and their interactions with insiders and outside actors. Their fashion label in the way being protected, shared, used and get printed, the data of their customers and their deliveries both in Australia and overseas. Their operations in headquarters and branches. Practices during online and physical sales, practices during refunding, details of purchases from suppliers both nationally and internationally, the password policy, the firewall usage, and backup processes. |
| Privacy Act 1988 |  |  |  | The data collected from customers after sales, refunds and also data shared with suppliers or received from them. Data stored or in transfer between employees in headquarters and branches. |
| Spam Act 2003 |  |  |  | Online marketing and communication practices happening in this organization, this act regulates those advertisements undergone across all states and territory in Australia. |
| Information Privacy Act 2009 (QLD) |  |  |  | Personal information of staffs, customers, and other actors stored from physical and online sales in Queensland. This can be also staffs’ employment details stored when they applied for the role. |
| Privacy and Personal Information Protection Act 1998 (NSW) |  |  |  | personal information of staffs, customers, and other actors stored from physical and online sales in New south Wales. This can be also staffs’ employment details stored when they applied for the role. |
| Privacy and Data Protection Act 2014 (VIC) |  |  |  | Personal information of staffs, customers, and other actors stored from physical and online sales in New south Wales. This can be also staffs’ employment details stored when they applied for the role. |
| Telecommunications (Interception & Access) Act 1979 |  |  |  | First of all, it has got impacts on the how service is being delivered and how it can be directly or indirectly accessed by customers. Then after a search, as they have got 7 shops, each having internal and also external telephone connections and they and their stuffs need to use this technology and safeguard themselves and also the customers while using it by obeying this regulation. |
| The **Criminal Code Act 1995** |  |  |  | Interactions happening between Owner and stakeholder, interactions between manager and staffs, interactions happening among staffs, interactions between staffs and external actors, the manner company or staffs handling orders are all areas where can be under this law to protect their interactions and keep them out of criminal approaches to them. |
| **Corporations Act 2001 (Cth)** |  |  |  | Risks organization face need to be handled based on this Act, the incidents happening need to be handled and reported based on this act, the data and its protection is also followed in this act. |
| **Prudential Standard CPS 234** |  |  |  | The framework being used for security of this organization needs to be aligned with this standard. Risk and incident management need to be performed based on this standard. Sometimes this organization needs to have knowledge of third-parties service providers and how do they comply with this standard. The approaches for identifying and classifying information assets, and then managing them in order to protect them. |
| Australian Competition and Consumer Commission (ACCC) |  |  |  | Customer right and the guarantees given to them has been controlled in this law, the manner for advertising and marketing has been regulated, some product safety also has been considered in this law, the online sales of the organization need to be operate based on this law, contract terms need to be design based on this law. |

Office of the Australian Information Commissioner (OAIC), 2024. *Preventing data breaches: Advice from the Australian Cyber Security Centre*. Available at: <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/preventing-data-breaches-advice-from-the-australian-cyber-security-centre> [Accessed 24 September 2024].

Lawpath, 2024. *Guide to the Corporations Act 2001*. Available at: <https://lawpath.com.au/blog/guide-corporations-act-2001> [Accessed 24 September 2024].

Office of Legislative Drafting and Publishing, 2001. Corporations Act 2001. Available at: <http://www5.austlii.edu.au/au/legis/cth/num_act/ca2001172/> [Accessed 24 September 2024].

Australian Prudential Regulation Authority (APRA), 2019. CPS 234 Information Security. Available at: <https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf> [Accessed 24 September 2024].

Federal Register of Legislation, 2004. Crimes Legislation Amendment Act 2004. Available at: <https://www.legislation.gov.au/C2004A02124/latest> [Accessed 24 September 2024].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SECTOR: | Transportation | | | |
| CYBER SECURITY and related  LEGISLATION | SCOPE | | | BUSINESS AREAS/ACTIVITIES AFFECTED |
| Federal | State | Territory |
| Australian Cyber Security Centre (ACSC) Guidelines |  |  |  | Interactions those taking place online between their employees with customers and external actors. data Protection those received or generated online during transactions including bookings, cancellations, insurance, payments, and refunds. Also, their website’s security and the approaches on managing client’s rewards and loyalty benefits in addition to information associated with them. |
| Privacy Act 1988 |  |  |  | Data collected from online transactions, including bookings, cancellations, insurance details, payments, and refunds. Data shared with or received from clients, and data transfer within the organization. |
| Spam Act 2003 |  |  |  | Practices for Email and online marketing, including advertisements and other communications sent to clients. Regulates all forms of electronic communication. |
| Privacy and Personal Information Protection Act 1998 (NSW) |  |  |  | Personal information of clients and employees collected during online transactions and interactions in New South Wales. Data related to bookings, insurance, payments, and refunds. |
| Telecommunications (Interception & Access) Act 1979 |  |  |  | Online communications including transactions happening over phone and other client interactions. data transmitted over telephone and internet connections used for business operations. |
| |  | | --- | | **The Criminal Code Act 1995** |  |  | | --- | |  | |  |  |  | Criminal activities and unsafe activities can be prevented by aligning the manner they handle transactions and client data . online interactions and internal communications among staff. |
| **Corporations Act 2001 (Cth)** |  |  |  | |  | | --- | |  |  |  | | --- | | online operations of this organization, risks being faced by this  company faces in cyber security. Data protection steps taken  must be in line with the Act. | |
| **Prudential Standard CPS 234** |  |  |  | Risk and incident management practices need to be reviewed based on this. |
| **Australian Competition and Consumer Commission (ACCC)** |  |  |  | They need to assure that online transactions, advertising, and customer interactions comply with consumer rights and guarantees. online bookings, payments, and refunds need also to be in a manner that meets ACCC regulations. |
| **Work Health and Safety Act 2011 (WHS Act)** |  |  |  | Their online systems and possible risks to their health and safety. any cybersecurity risks those can impact the safety of the employees while using online systems. |
| **Electronic Transactions Act 1999** |  |  |  | transactions and communications. Ensures that Turtle Movers’ online transactions, including bookings, payments, and communications, are legally recognized and secure. |

Attorney-General's Department, 2024. Electronic signatures, documents and transactions. Available at: <https://www.ag.gov.au/legal-system/electronic-signatures-documents-and-transactions> [Accessed 24 September 2024].

Federal Register of Legislation, 2004. Crimes Legislation Amendment Act 2004. Available at: <https://www.legislation.gov.au/C2004A02124/latest> [Accessed 24 September 2024].

Business Queensland, 2024. Work Health and Safety Act 2011. Available at: <https://www.business.qld.gov.au/running-business/whs/whs-laws/whs-act> [Accessed 24 September 2024].

Queensland Government, 2011. Work Health and Safety Act 2011. Available at: <https://www.legislation.qld.gov.au/view/pdf/inforce/current/act-2011-018> [Accessed 24 September 2024].

* 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

First organization, in this scenario they have mentioned that they export their creations globally, they need to consider GDPR which stands for General Data Protection Regulation and must comply to it if they are handling data of EU citizens. GDRP requires strict data protection rules need to be used such organizations. After this, this organization need to comply with the Budapest Convention on Cybercrime because they are operating in Australia but also have got international interactions. This will help them to ensure that the organization adheres to consistent regulations and standards across borders, aiding them in handling of international data. By adhering this convention, the organization can ensure that no legal consequences and risks they will face when there is a company or customer interacting with them in a country those who have signed Budapest convention. The Budapest convention is not only about some rules, but they also address investigate techniques and let the one who obey their convention respond to breaches or any other incident in a way preventing damage to investments and also actors in and out of organization. Then we have got PCI DSS which stands for Payment Card Industry Data Security Standard. Since Angelonia fashion has mentioned that they process credit card payments for both Australian and international clients., they need to be complied with PCI DSS in order to ensure secure handling of card information as it is considered as a sensitive data.

On the other hand, we have got the second organization which only operates in Australia. Here this organization need to check even if there is any possible interaction overseas and then check for relevant laws.

Investopedia, 2024. General Data Protection Regulation (GDPR). Available at: <https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp> [Accessed 24 September 2024].

Council of Europe, 2024. The Budapest Convention. Available at:

<https://www.coe.int/en/web/cybercrime/the-budapest-convention> [Accessed 24 September 2024].

1. Identify the areas of the business affected by the international legislation

When it comes to international interactions, there are several areas such as International Marketing ( including the way the organization perform the advertisements), online presence for receiving orders ( sometimes there need to be website localization based on the IP of that country), payments being received globally or other transactions, their approaches for distributing their products, warehouse management, data protection, foreign customer support, cultural considerations.

1. 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 DATA SECURITY** |
|
| GDPR (General Data Protection Regulation) | Affecting promotional practices and data protection while advertising | The compliance increases operational costs and heightens security risks due to complex data protection regulations. |
| CCPA (California Consumer Privacy Act) | affecting terms, conditions, and refund policies, website localization | More resources are necessary for policy and website localization can lead to challenging management. There would be a need to alter data protection practices for each region. |
| PCI DSS (Payment Card Industry Data Security Standard) and AML Regulations | Security of payments being made ,anti-money laundering procedures | security requirements will be increased in order to prevent fraud and data breaches during and after transactions. |
| NIST Cybersecurity Framework | In the process of handling data, cyber threats to the process of importing material, cyber threats to material itself and shipping process. | Complex import rules can lead to unwanted delays to prepare and increase costs to securing shipping data before departing. |
| |  | | --- | | ISO/IEC 27001 |  |  | | --- | |  | | Managing the warehouse by systems those are working based on ISO/IEC 27001 to manage and protect inventory data, customer data, and organizational data. | Compliance is costly but necessary to prevent data breach. This will certainly be helpful in mitigating risks they are facing for their data |

|  |  |  |
| --- | --- | --- |
| eIDAS (Electronic Identification and Trust Services Regulation) | When it comes to handling international customers’ data, including their electronic identity, their signatures, | It again makes the process complex and more costly as there would be a need to compliance. Non-compliances can lead to serous financial and legal consequences. |

* 1. For **each organisation**,identify and explain at least one (1) interdependency between different legislative instruments related to cyber security.

Organization one:

When I was searching for connections and interdependency between two different legislative instruments associated with the cyber security for Angelonia Fashion, I saw the Criminal Code Act 1995 and the Notifiable Data Breaches (NDB) scheme under the Privacy Act 1988. When there is a cyber incident, such as unauthorized access to this organization’s system, the organization needs to comply with NDB scheme’s requirements for notifying affected parties in addition to addressing criminal aspects those covered in Criminal Code Act. This will ensure that the response given by the Angelonia Fashion is a comprehensive reaction, addressing both the legal implications of occurred breach under Criminal Code Act and also liabilities to inform and protect affected individuals.

Second organization:

This time among acts and other legislative instruments, I found Privacy Act 1988 the Australian Consumer Law (ACL) having interdependency. The connection found here is that the Privacy Act assures about personal data protection, while compliance with the ACL is ensuring that customers can trust the service and having their own rights. If this organization faces an online security failure, this will impact both data privacy and consumer rights, remembering that company needs to maintain its compliance across both legal frameworks.

Office of the Australian Information Commissioner (OAIC) 2023, *About the Notifiable Data Breaches scheme*, OAIC, viewed 24 September 2024, <https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme>

Australian Government 2023, *Criminal Code Act 1995*, Attorney-General's Department, viewed 24 September 2024, <https://www.ag.gov.au/crime/publications/commonwealth-criminal-code-guide-practitioners-draft/criminal-code-act-1995>.

Australian Government 2023, *Australian Consumer Law*, Consumer Affairs, viewed 24 September 2024, <https://consumer.gov.au/australian-consumer-law>

* 1. 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.

I do believe that the Office of the Australia Information Commissioner (OAIC) is the one can contribute to the security of business data operations of this organization. There are guidance and resources being provided by OAIC to aid this business to enhance their understanding of obligations they have got under Act and scheme mentioned before. They have been providing with best practices for data protection, incident response plans and more in event of a data breach. Its guidelines will help the organization to enhance data protection, their compliance leading to building trust.

Office of the Australian Information Commissioner (OAIC) 2023, *About the OAIC*, viewed 24 September 2024, <https://www.oaic.gov.au/about-the-OAIC>.

* 1. For each of the regulators presented below, identify and explain their role and scope.

|  |  |  |
| --- | --- | --- |
| REGULATOR | ROLE | SCOPE |
| Australian Prudential Regulation Authority (APRA) | It supervises financial institutions to enhance their stability and enforce prudential standards. | It covers banks, insurers, and superannuation funds, focusing on risk management and their cybersecurity. |
| Australian Securities and Investments Commission (ASIC) | Its role is to regulates companies and financial services to ensure market integrity and investor protection. | It governs corporations, financial markets, and service providers to create a fair environment. |
| Australian Competition and Consumer Commission (ACCC) | It ensures that there is a fair competition and it always trying to protect consumers by enforcing trade practices and other rules. | It applies to all sectors, focusing on those rights belonging to the customer, competitions happening in market, and prevention of any anti-competitive behaviours. |
| Australian Energy Sector Cyber Security Framework (AESCSF) | It is here to enhance cybersecurity resilience for the energy sector. | It aims is about energy providers, focusing on helping them managing cyber risks and protecting their critical infrastructure. |
| Protective Service Manual (Australian Government rules for cybersecurity) | It has established cybersecurity rules for entities under supervision of Australian government to ensure information protection. | It usually Applies to those sectors or agencies having direct interactions with government, focusing on safeguarding data, personnel safety, and physical security. |

**Australian Prudential Regulation Authority (APRA) 2023, Home, viewed 24 September 2024,** [**https://www.apra.gov.au/**](https://www.apra.gov.au/)**.**

**Australian Securities and Investments Commission (ASIC) 2023, Home, viewed 24 September 2024,** [**https://asic.gov.au/**](https://asic.gov.au/)**.**

**Australian Competition and Consumer Commission (ACCC) 2023, Home, viewed 24 September 2024,** [**https://www.accc.gov.au/**](https://www.accc.gov.au/)**.**

**Department of Climate Change, Energy, the Environment and Water (DCCEEW) 2023, Australian Energy Sector Cyber Security Framework, viewed 24 September 2024,** [**https://www.dcceew.gov.au/energy/security/australian-energy-sector-cyber-security-framework**](https://www.dcceew.gov.au/energy/security/australian-energy-sector-cyber-security-framework)**.**

**Australian Cyber Security Centre (ACSC) 2023, Information Security Manual - March 2023, viewed 24 September 2024,** [**https://www.cyber.gov.au/sites/default/files/2023-03/Information%20Security%20Manual%20-%20%28March%202023%29.pdf**](https://www.cyber.gov.au/sites/default/files/2023-03/Information%20Security%20Manual%20-%20%28March%202023%29.pdf)**.**

* 1. Investigate current and upcoming reforms in privacy legislation and explain how these could benefit **each organisation**.

Answer for both organization:

The Privacy Law has been subjecting to a reform in recent years. They have stated by enhancing the data security and destruction obligations in order to ensure a secure personal data storing and handling practices and also its proper destruction when no longer needed. This will benefit both organizations by minimizing risks associated with data breaches by implementing stronger security measures. Moreover, they are going to have more efficient operation when they will receive clear updated guidelines on data destruction, they will ensure that only necessary data is retained. Furthermore, they have decided to expand enforcement powers of courts for enforcing privacy laws. This can include the ability to impose higher penalties for non-compliance. If there are going to be higher penalties rates, this will make both organizations motivated to prioritize data privacy preventing facing any fines. Lastly, they are planning to increase transparency and accountability in how organizations handle data, which will also make auditing process more convenient. This will benefit both organizations by improving their reputation and build consumer confidence.

Russell Kennedy 2024, *New privacy legislation in 2024: Government responds to proposed reforms to Australia’s privacy laws*, viewed 24 September 2024, <https://www.russellkennedy.com.au/insights-events/insights/new-privacy-legislation-in-2024-government-responds-to-proposed-reforms-to-australia-s-privacy-laws>.

Jones Day 2024, *US Congress reintroduces new comprehensive federal privacy law*, viewed 24 September 2024, <https://www.jonesday.com/en/insights/2024/04/us-congress-reintroduces-new-comprehensive-federal-privacy-law>.

PwC Australia 2023, *Privacy Act review report*, viewed 24 September 2024, <https://www.pwc.com.au/cyber-security-digital-trust/2023-privacy-act-review-report.html>.

* 1. Investigate current and upcoming reforms in consumer and surveillance legislation and explain how these could benefit **each organisation**.

There are going to be some changes in consumer laws like Australian consumer Law and Privacy Act. They have announced that reforms will make stricter on unfair contract terms to identify them as illegal ones. This will prevent organizations being only into their own favourable agreements, ensure fairer competition. Moreover, they have mentioned that they will enforce more new regulations those will require businesses to ensure their products satisfy safety standards prior to entering the market. This will encourage both businesses to enhance their compliances in order to prevent any fines. This will not only about fines, but the stricter data protection and surveillance by the laws can lead to better security practices which will protect both organizations from data breaches and other cyber threats. Lastly, this will lead to an increase in trust being made by both organizations’ trust.

Australian Competition and Consumer Commission (ACCC) 2023, *Contracts*, viewed 24 September 2024, <https://www.accc.gov.au/business/selling-products-and-services/contracts>.

Australian Competition and Consumer Commission (ACCC) 2023, *Unfair contract terms: A guide for businesses and legal practitioners*, viewed 24 September 2024, <https://www.accc.gov.au/system/files/Unfair%20contract%20terms%20-%20A%20guide%20for%20businesses%20and%20legal%20practitioners.pdf>.

Australian Government Department of Home Affairs 2021, *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, viewed 24 September 2024, <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-act-2021>.

Australian Government 2024, *Reform Australia’s electronic surveillance framework*, viewed 24 September 2024, <https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance/reform-australias-electronic-surveillance-framework>

* 1. 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:
  2. Compliance with legislation and regulatory requirements
  3. International cyber security legislation impacting their businesses
  4. Potential impact of upcoming reforms in privacy, consumer and surveillance legislation
* As I have previously listed here, there are lots of Australian and international regulations and standards need to be discovered and then have investigations on them to find their requested requirements and receive suggested policies or techniques to be added in procedures. In this way, both organizations can assure that they have found all relevant regulations and standards, and they know about them in all aspects. This will prevent any possible mistake which can lead to serious legal consequences or financial loses. When checking the scenarios presented, only Angelonia Fashion has got international operations, and second organization doesn’t have any operation in overseas directly. The Angelonia Fashion need also review their presence and find out in each region what possible conventions, regulations and standards they are facing with. They have not specifically mentioned which countries they are operating in. For example, Budapest convention is the one they need to have compliance if they are operating in Europe. They need to review their policies by found regulations and enhance their practices further. Their business will certainly require adopting in each region as all laws are not always suitable for another region. For example, their website may subject to the change based on the location it is being used in. After this we have got upcoming reforms in the Privacy, consumer and surveillance legislation. These reforms will have impact on the operation of both organizations. They will certainly need to make changes to the current practices, and this will costly and complex for them as I mentioned before (maybe it is not always about money, but it can be also about time), but they will benefit from a more efficient and safer operation. As mentioned before, safeguarding the personal information with new updates in these three legislative instruments will enhance their reputation as they are respecting customers and staffs with valuing importance of protecting their data.

## 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).

First of all, I started with checking the structure presented in both privacy policy of both organizations. I investigated about the suggested structure for privacy on reliable websites and then began review both policies based on findings. The structure found was as below:

1. Introduction 2. What Information We collect 3. How We Collect Your Information

4. How We Use Your Information 5. Disclosure of Your Information 6. How We Protect Your Information 7. Your Rights and Choices 8. International Data Transfers ( if they have international operations) 9. Retention of Personal Information 10. Changes to this Privacy Policy ( if there was an update or there is a possible upcoming update) 11. Complaint and Dispute Resolution 12. Contact us

So, I checked both Privacy and Policy for both organizations and found that there would be a need to add an extra section as “Your Rights and Choices” for both organizations. Then it is time to get to the contents of each section of both organizations’ Privacy Policy. I have listed my reviews and classified them all for both organizations in tables below:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Organization 1** | | | | | | |
| **POLICY** | **STANDARDS APPs** | **REVIEW DETAILS** | **COMPLIANCE** | | | |
| **Full** | **Partial** | **Poor** | **Non-  Compliance** |
| Privacy Policy | APP1 | I revied the section of “Information We May Collect” and it was clearly outlining the collection of various types of personal and transaction information. The only improvement needed is anonymizing communications and how they ensuring there is a clear consent for collecting sensitive data. |  |  |  |  |
| APP1 | They have mentioned that they collect data from online transactions, including information related to online purchases. However, I believe this section need to provide more details on how the data is collected, ensure explicit consent is obtained, and clarify how data derived from existing information is handled. This is essential for compliance with APP 1, which requires transparency in data collection and user consent processes. |  |  |  |  |
| APP 7 | They have mentioned that the personal data collected from online transactions is used to process customer purchases, where the user experience will be enhanced, and support their marketing strategy. Moreover, they stated that personal data linked to sales is retained for the period mandated by the taxation department, while other information is only kept for the duration of business activities. However, I do believe this section is missing clarity on how user consent is granted for marketing purposes, which is necessary for compliance with APP 7. Furthermore, it does not mention users' rights to access, rectify, or request deletion of their data, which is important for obeying APP 1. |  |  |  |  |
| APP 1, APP 6 | They have stated that they manage personal information in a transparent manner and that consent is required before disclosing any personal information to third parties. However, while this practice complies with APP 1, the section lacks details on how customers are notified about third-party disclosures, particularly concerning online sales and transactions, which are a significant part of their business. Additionally, the policy does not clarify the customers' rights to request the cessation of the use of their personal data, which is crucial for compliance with APP, as well as standards like GDPR. |  |  |  |  |
| APP 1 , APP 8 and APP 5 | They have mentioned that If you access a third-party website through our website, the third-party website may collect your personal information. They have decided to take no responsibility for third-party websites' privacy policies or lack of policies. But if you check the APP 1 or some parts of GDPR, this organization is responsible for investigate and ensure that any third parties processing personal data of their customer and if they have linked any of them, comply with APP 1 and GDPR requirements .This section is not clearly outlining the responsibilities of Angelonia Fashion when being linked to third-party websites. According to what just mentioned, organizations must have clear communication about data collection practices. |  |  |  |  |
|  | APP 1, APP3 and APP 5 | In the cookies section, this organization need to clarify users regarding of cookies used, the data they collect, and the purpose of their use based on APP1. While Australian law does not mandate cookie consent pop-ups, it is important to notify users about the storing of their personal information using cookies and obtain their consent where necessary |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Organization 2** | | | | | | |
| **POLICY** | **STANDARDS APPs** | **REVIEW DETAILS** | **COMPLIANCE** | | | |
| **Full** | **Partial** | **Poor** | **Non-  Compliance** |
| Privacy Policy | APP 1 | The first part (introduction) revealed that there is compliance with the Australian Privacy Act 1988. |  |  |  |  |
| APP 5 | They have listed the types of personal information collected, which is important for transparency, but the policy is missing details on how individuals are informed about the collection of their information, especially if collected indirectly. |  |  |  |  |
| APP 6 | They have described the process of how data is collected on online transactions but the policy states that consent is obtained for third-party data sharing, it could clarify the specific situations that require this disclosure. |  |  |  |  |
| APP 7 | They have mentioned their purposes for data collection, which aligns with APP 6. The policy said they are using data for marketing but does not specify how individuals can stop their data usage in this process. |  |  |  |  |
| APP 6 | They have clearly mentioned that personal data is not shared without consent, except under legal obligations. I do believe that the circumstances under which data may be shared without consent could be more specifically defined. |  |  |  |  |
|  | APP 11 | The policy mentions secure retention and destruction of data, complying with APP 11. It can be an advantage if they provide more detail on the retention periods for various types of data, in addition to methods of secure disposal. |  |  |  |  |

Office of the Australian Information Commissioner (OAIC) 2023, *Australian Privacy Principles*, viewed 24 September 2024, <https://www.oaic.gov.au/privacy/australian-privacy-principles>.

Office of the Australian Information Commissioner (OAIC) 2023, *Read the Australian Privacy Principles*, viewed 24 September 2024, <https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles>.

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 |
| Establishing secure password policy, proper classification of sensitive data, Encryption of sensitive data in rest and transit, control access to sensitive data, minimization of data collection, Implement a Robust Data Security System, | No regular audits and enforcement mechanisms, outdated or incorrect classifications of data, outdated or incorrect classifications, Poor key management practices for encrypted data, misunderstanding of employees about necessary data, one time training event conducted, | Implementing MFA, Password Audit, Regular review for classification of sensitive data, developing clear guidelines on data classification, implementing Automated tools for data classification, Key Management System, conducting regular audits,  Implementing encryption algorithms, Implementing Role based Access Control, Zero Trust policy, developing clear data collection guidelines, Ongoing Privacy Training Programs |
| Timely Handling of Refunds and Faulty Products, 24-hour response to client’s questions, Not assuming all clients need the same thing, Adapt to customer behaving styles and discover communication channels available, honest communication, Avoiding Close-ended Responses when dealing with clients, Priority is always the customer’s issue | No clear deadlines for refunds or product replacements, No clear instructions on how to personalize service for each customer, Not enough training for staff to recognize different communication styles, Rush in resolving and overpromising solutions that cannot be delivered in reality | Set clear timeframes for refunds and replacements, Automatic responses and resolution timeframes, train staff for service personalization based on the customer’s needs, Ongoing employee training systems, establishing incident response plan, |
| Enforcing strong passwords, employing Encryption for their data especially sensitive one, compulsory Privacy Training, back up data, protecting data from Insider threats | Not enough and still can be compromised through phishing and brute force attacks, no details on encryption method and how encryption key is managed, missing mention of training frequency, no information on how often backups are performed, did not mention what type of endpoint security system are in use, no mention on example of data control | Add MFA, stating advanced encryption methods, detail regular privacy training updates, tested backups, practices for monitoring insider threats, |
| User endpoint security systems to protect data, conducting proper disposal of electronic and physical copies of personal data, implement a trifecta of Technical, physical and administrative control, | No mention on how these controls being audited, lack of policies on secure deletion, lacks mitigating strategies for third party partners such as security contracts, doesn’t mention testing the backups regularly to ensure it is working, no detail about practices to handle customers questions | information on auditing physical and technical controls, specifying standards of endpoint security software or tool, establishing incident response plan and associated practices, |

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

organization one:  
After reviewing the Angelonia Fashion, I found that they have been trying to comply with Australian laws such as Australian Privacy Act 1988, and other relevant laws. The policy has almost mentioned all needed sections to meet legal requirements. I do believe it may can be for them for a while but after that I am not sure it would be really compliant as they are interacting all around Australia and also globally using physical and online presence. They certainly need to enhance their international compliance. As I have mentioned before they may need regular audit over their operation checking compliance. As I mentioned before, there are going to a need to data minimization in order to review data collection and assure they only save necessary data. Moreover, they need to state and start advanced encryption. Further, they need to maintain key encryptions and state practices associated with it.

Second organization:

After reviewing the Turtle Movers, I found that they are complying with Australian laws in most aspects. Their privacy policy covers most necessary aspects to meet legal standards. However, I don’t believe it will continue to be fully compliant in the long term, especially as they operate across Australia. It is obvious that they need to enhance their compliance to the Australian laws and standards . As I have mentioned before, establishing response planes along with regular audits, operation will be more secure and efficient. There is also always a need for data minimization practices to review the data they collect. In this way, they can assure that they retain only essential information. Furthermore, they need to enforce more advanced encryption and password policy with more specific requirements.

## Part 3: Review the organisations’ ethical practices and procedures

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

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

Organization one:

1. Metasploit Framework

It is a strong penetration testing tool which allows users to identify, exploit and check vulnerabilities. It has got a wide range of exploits and payloads in its library. It can be used to simulate attacks happening in real world.

1. Nmap

It is a network scanning tool. It is able to identify hosts and services on a computer network using packets. It can analyse the responses received from returned packets. It can be used to create a map of the network and finding information on ports and system itself.

1. Wireshark

It is a network protocol analyser that captures and browse the traffic running on a computer network. Red team can use it to analyse network in order to identify potential vulnerabilities and learn about how data is being transferred among devices in network.

1. Burp Suite

It can be used to test web applications for vulnerabilities and security flaws. Red team can use it as a scanner that helps identifying security problems in web applications.

Pluralsight 2024, *Exploit Development and Execution with the Metasploit Framework*, viewed 24 September 2024, <https://www.pluralsight.com/courses/exploit-development-execution-metasploit-framework>.

Jaber, A. 2024, ‘Basics of Burp Suite: A comprehensive guide’, *Medium*, viewed 24 September 2024, <https://medium.com/@jaber_5689/basics-of-burp-suite-a-comprehensive-guide-eb3dfb9410c2>.

Wireshark 2023, *Wireshark User’s Guide*, viewed 24 September 2024, <https://www.wireshark.org/docs/wsug_html/>.

Comparitech 2024, *The definitive guide to Nmap*, viewed 24 September 2024, <https://www.comparitech.com/net-admin/the-definitive-guide-to-nmap/>.

Organization two:

1. Cobalt Strike

It is good tool to simulate advanced attacks. It has got features like deploying payloads and establishing command and control channels.

1. BloodHound:

It is a tool for creating a map and visualizing the organization’s active devices and other facilities. It can aid organisation to identify potential attack paths in their environment. Red teams can use it to recognize relationships and permissions in Active directory which can be exploited.

1. Empire :

It is a framework that uses PowerShell and Python agents to make a platform for maintaining access to compromised systems. They can use it to execute commands, gather information and maintain their presence on compromised systems.

1. Social Engineer Toolkit or SET:

It is a toolkit designed for creating and running social engineering attacks. These attacks can be phishing emails and downloads from malicious websites. Red team can use it to trick users to reveal sensitive information or executing malicious payloads.

SentinelOne 2024, *What is Cobalt Strike?*, viewed 24 September 2024, <https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-cobalt-strike/>.

Pentest Partners 2024, *BloodHound walkthrough: A tool for many tradecrafts*, viewed 24 September 2024, <https://www.pentestpartners.com/security-blog/bloodhound-walkthrough-a-tool-for-many-tradecrafts/>.

Alpine Security 2024, *Empire: A PowerShell post-exploitation tool*, viewed 24 September 2024, <https://www.alpinesecurity.com/blog/empire-a-powershell-post-exploitation-tool/>.

Kali Linux Tutorials 2024, *Social Engineering Toolkit tutorial*, viewed 24 September 2024, <https://kalilinuxtutorials.com/social-engineering-toolkit-tutorial/>.

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

Organization one:

1. Splunk:

It is a security information that can collect and analyses and manage security data. Blue team can use its real time monitoring and its alerting system for potential security incidents.

1. Snort

It is an open-source Intrusion Detection and Prevention System that can supervise network traffic for any abnormal activities. It can detect attack patterns and can be customized based on the needs.

1. Wireshark:

It is a network protocol analyser which is able to capture and browse the traffic running on a computer network. It can be used by Blue team for troubleshooting, analysing and developing current protocols.

1. Nessus:

IT is a vulnerability scanner which aids in identifying vulnerabilities, any possible misconfigurations, and compliance issues in network devices and their applications. Blue team can use it as a scanner and receive detailed reports on security weaknesses to find a way to prioritize steps need to be taken.

Splunk 2024, *Splunk Certified Cybersecurity Defense Analyst*, viewed 24 September 2024, <https://www.splunk.com/en_us/training/certification-track/splunk-certified-cybersecurity-defense-analyst.html>.

Snort 2024, *Documents*, viewed 24 September 2024, <https://www.snort.org/documents>.

Wireshark 2023, *Wireshark User’s Guide*, viewed 24 September 2024, <https://www.wireshark.org/docs/wsug_html_chunked/>.

Tenable 2023, *Nessus 10.4 documentation*, viewed 24 September 2024, <https://docs.tenable.com/nessus/10_4/Content/PDF/Nessus_10_4.pdf>.

Organization 2:

1. OSSEC:

It is an open-source Intrusion Detection System which is able to monitor and analyse system activity for signs of abnormal behaviour. It can provide log analysis, integrity checking, detecting rootkit, and alerting in case of incident.

1. Bro (Zeek):

It is an open-source network security monitoring tool. It supports a wide range of traffic analysis tasks. It can perform performance measurement and troubleshooting.

1. Kibana:

Kibana act as data visualization and exploration tool. It can help Blue team in visualizing and analysing security data, creating dashboards, and finally exporting reports for making decision in a better manner.

1. Maltego:

It is a very genesis platform which is able to provide data mining and link analysis capabilities. The Blue team can generate a map for relationships among departments, such as IP addresses, domain names, and social profiles to reveal potential threats and any attack vectors or actors.

OSSEC 2023, *Documentation*, viewed 24 September 2024, <https://www.ossec.net/docs/>.

Zeek 2023, *Quick start guide*, viewed 24 September 2024, <https://docs.zeek.org/en/master/quickstart.html>.

Elastic 2024, *Kibana User Guide*, viewed 24 September 2024, <https://www.elastic.co/guide/en/kibana/current/index.html>.

Stationzilla 2024, *How to use Maltego*, viewed 24 September 2024, <https://www.stationx.net/how-to-use-maltego/>.

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

Both Red team and Blue team in both organizations need to assure all the mentioned activities comply with relevant laws and regulations. They both need to inform all departments involved regarding tests. They need to seek permission from the head office and all stakeholders associated before starting activity. They need to avoid accessing, collecting or disclosing sensitive information during tests in this way they can protect the privacy of individuals and organizations. They need to minimizing impact on organisation preventing harm to the performance of the devices. Finally, they need to keep all findings and sensitive information confidential by sharing them only with authorized personnel.

SentinelOne 2024, *The realm of ethical hacking: Red, blue, and purple teaming explained*, viewed 24 September 2024, <https://www.sentinelone.com/blog/the-realm-of-ethical-hacking-red-blue-purple-teaming-explained/>.

CSO Online 2024, *Best tools for red and blue teams: Methodology and experience*, viewed 24 September 2024, <https://www.csoonline.com/article/558313/best-tools-for-red-and-blue-teams-are-methodology-experience.html>.

1. Consequences of unethical behaviour:
2. 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.

Both organizations, can face legal charges. Their employees can receive fines and penalties. If they commit serious offences can face imprisonment. Their information can be exposed which can result in identity theft, financial fraud, and other malicious activities. If data breaches happen, the trust between organization, stakeholders and customers will be lost. (loss of reputation)

TechCrunch 2020, *Red team, ethical limits*, viewed 24 September 2024, <https://techcrunch.com/2020/02/02/red-team-ethical-limits/>.

Data Space Academy 2024, *Red team vs. blue team: Understanding key differences and skills*, viewed 24 September 2024, <https://blog.dataspaceacademy.com/red-team-vs-blue-team-understanding-key-differences-skills/>.

1. Outline the consequences of unauthorised access to network routers.

While both Blue team and Red team are performing tests, they need to get permission before accessing networking facilities like the router. If they have unauthorized access to the network routers, they may face criminal charges, fines, and penalties. This can lead to exposure of sensitive data, like financial data or other type of data. This can lead to damage the router by deleting some configuration. This can lead to the service being disrupted. This can lead to unauthorized changes. The organization also will face reputational damage.

Norton 2024, *How to tell if someone hacked your router*, viewed 24 September 2024, <https://us.norton.com/blog/privacy/how-to-tell-if-someone-hacked-your-router>.

RouterSecurity.org 2024, *What can go wrong?*, viewed 24 September 2024, <https://routersecurity.org/whatcangowrong.php>.

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

Bypassing media and application which is subject to the copyright, can have serious legal, financial, consequences. They can face civil penalties. Those are holding copyright can ask money for possible damage. There is also imprisonment sometimes. Sometimes, the criminal need to pay fees and other costs associate with copy right holder presence in court.

University of California, Santa Cruz (UCSC) 2024, *File sharing security*, viewed 24 September 2024, <https://its.ucsc.edu/security/filesharing.html>.

North Carolina State University (NCSU) 2020, *University warns against illegal peer-to-peer file sharing*, viewed 24 September 2024, <https://oit.ncsu.edu/2020/09/15/university-warns-against-illegal-peer-to-peer-file-sharing/>.

1. 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.
2. Unauthorized Data Access

This can result in data breaches, loss of reputation and possible legal consequences. This can harm organization itself and individuals interacting with organization directly and indirectly.

1. Installing Backdoors

Sometimes, technician install backdoors on purpose to gain unauthorized access to ends for malicious purposes. This can result in data breaches, system compromises, and potential financial losses.

1. Manipulating Logs and Audit Trails

A staff can alter or change logs to cover up unauthorized activities . This can damage the organization’s ability when it comes to detect and respond to the security incidents.

1. Sharing Confidential Information

A staff can share confidential information, such as information on vulnerabilities in security, the organization has faced, or a critical process with unauthorized party. This can lead to serious attacks on organization, it also damages organization’s reputation among clients and parties leading to financial lose.

|  |  |
| --- | --- |
| UNETHICAL BEHAVIOUR | IMPACT ANALYSIS |
| Unauthorized Data Access | This can result in data breaches, loss of reputation and possible legal consequences. This can harm organization itself and individuals interacting with organization directly and indirectly. |
| Installing Backdoors | Sometimes, technician install backdoors on purpose to gain unauthorized access to ends for malicious purposes. This can result in data breaches, system compromises, and potential financial losses. |
| Manipulating Logs and Audit Trails | A staff can alter or change logs to cover up unauthorized activities . This can damage the organization’s ability when it comes to detect and respond to the security incidents. |
| Sharing Confidential Information | A staff can share confidential information, such as information on vulnerabilities in security, the organization has faced, or a critical process with unauthorized party. This can lead to serious attacks on organization, it also damages organization’s reputation among clients and parties leading to financial lose. |

Future of Tech 2024, *4 ethical issues in cybersecurity*, viewed 24 September 2024, <https://www.futureoftech.org/cybersecurity/4-ethical-issues-in-cybersecurity/>.

Managing Life at Work 2024, *Unethical behavior in the workplace*, viewed 24 September 2024, <https://managinglifeatwork.com/unethical-behavior-in-the-workplace/>.

1. **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.

Ethics Code of Practice

Introduction

Technicians working in Angelonia Fashion are committed to give hand to each other and maintain highest standards of below ethical conduct in their operations. This Ethics Code of Practices contains guidelines regarding employees, especially ones dealing with cyber security, for protecting the company’s data, systems, reputation and actors including customers and staffs.

Core Values

Integrity and Honesty

* Everyone needs to act with honesty in all of their professional activities.
* Everyone needs to assure about transparency in all actions and decisions being made.

Confidentiality

* Everyone is supposed to protect confidentiality of all critical information such as clients’ data, organization’s financial records or other important data.
* Employers are required to prevent disclosing any confidential information without prior permission

Compliance with Regulations

* Everyone working at this organization need to obey relevant regulations and company’s policies
* especially ones related to data protection and cyber security.
* Employers need to stay informed about changes in laws and regulations in order to assure current condition of compliance.

Respect for Privacy

* Employees need to respect the privacy of customers, employees, and Stakeholders
* They need to assure that personal data is collected, processed, and stored in compliance with
* Privacy laws and companies’ policies.

Professional Conduct

* Employers need to maintain a high a level of professionalism in all interactions and activities
* Employees should avoid conflicts of interest and disclose any potential conflicts to management.

Accountability

* Employees need to take responsibility for actions and decision they make.
* Employees have to report any unethical behaviour or security breaches to the appropriate
* authorities.

Australian Community Workers Association (ACWA) 2024, *Ethics and standards*, viewed 24 September 2024, <https://www.acwa.org.au/workers/ethics-and-standards/>.

Indeed 2024, *How to create a code of ethics*, viewed 24 September 2024, <https://www.indeed.com/career-advice/career-development/create-code-of-ethics>.

Status.net 2024, *Code of conduct and ethics: What to include with examples*, viewed 24 September 2024, <https://status.net/articles/code-of-conduct-and-ethics-what-to-include-with-examples/>.

WikiHow 2024, *How to develop a code of ethics*, viewed 24 September 2024, <https://www.wikihow.com/Develop-a-Code-of-Ethics>.

National Health and Medical Research Council (NHMRC) 2018, *Australian Code for the Responsible Conduct of Research*, viewed 24 September 2024, <https://www.nhmrc.gov.au/about-us/publications/australian-code-responsible-conduct-research-2018>.

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

Suitability:

1. It is widely being used for both personal and commercial purposes because it has got friendly interface and its good features. Further, it supports real time collaboration, making it a good platform for those are working at a team on a project. Lastly, it also works with lots of third-party applications, boosting its functions.

Security risks:

1. This platform, has experienced data breaches in the last years. There are also some fishing attacks are always in progress to steal credentials associated with this platform. Moreover, Every person who acts as a team member can access to sensitive files saved on the account but there might be security based rules features in such platforms.
2. Google Drive

Suitability:

1. This platform is popular among individuals and academical institutions because of being suitable to the Microsoft’s products such as its operation system the “Windows”. It offers excellent collaboration tools. It also has got Multi-Factor Authentication enabled. It has got also an amount of free storage where you are also enabled to upgrade for more space.

Security risks:

B) Same as Dropbox, we can experience phishing attacks from fake notifications and emails. Lastly, if a user’s Google account is stolen, all data in Google drive can be accessed.

3. We Transfer

Suitability:

1. It is very good for those who need to transfer large files quickly without the need for an account. This platform has got a simple interface make it much easier than other platforms those downloadable to work with, even if you don’t have any previous training. There are also beneficial functions like temporary file storage in this platform.

Security risks:

1. This platform has mentioned that they do not provide end to end encryption, which can expose files to interception in transit. In this platform, there are temporary links are in use. This links if being shared with unauthorized users can lead to data breaches. Lastly, in this platform, when you upload files, after that you will have limited access to them which will be a concern for sensitive data.

Tom's Guide 2024, *Best file sharing apps*, viewed 24 September 2024, <https://www.tomsguide.com/buying-guide/best-file-sharing-apps>.

|  |  |  |
| --- | --- | --- |
| FILE-SHARING SERVICE (DOWNLOADING) | SUITABILITY | ASSOCIATED SECURITY RISKS |
| Dropbox | interface and its good features. Further, it supports real time collaboration, making it a good platform for those are working at a team on a project. Lastly, it also works with lots of third-party applications, boosting its functions. | This platform, has experienced data breaches in the last years. There are also some fishing attacks are always in progress to steal credentials associated with this platform. Moreover, Every person who acts as a team member can access to sensitive files saved on the account but there might be security based rules features in such platforms. |
| Google Drive | This platform is popular among individuals and academical institutions because of being suitable to the Microsoft’s products such as its operation system the “Windows”. It offers excellent collaboration tools. It also has got Multi-Factor Authentication enabled. It has got also an amount of free storage where you are also enabled to upgrade for more space. | Same as Dropbox, we can experience phishing attacks from fake notifications and emails. Lastly, if a user’s Google account is stolen, all data in Google drive can be accessed. |
| We Transfer | It is very good for those who need to transfer large files quickly without the need for an account. This platform has got a simple interface make it much easier than other platforms those downloadable to work with, even if you don’t have any previous training. There are also beneficial functions like temporary file storage in this platform. | This platform has mentioned that they do not provide end to end encryption, which can expose files to interception in transit. In this platform, there are temporary links are in use. This links if being shared with unauthorized users can lead to data breaches. Lastly, in this platform, when you upload files, after that you will have limited access to them which will be a concern for sensitive data. |

## Part 4: Contingency task

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.

They need to receive training programs as they start this role. This training needs to provide them knowledge associated with their area they work on. They need to know more about their responsibilities in this role. This training programs can be run online or in person while they are working in form of courses, workshops and hands-on training in office.

Next one is to connect these two junior technicians with experienced mentors who can navigate correct path for them and provide them guidance and support. They need both mentors help and peer support to learn best practices.

I do believe that the organization need to gradually increase the responsibility and workload in those area necessary instead of overwhelming them with lots of new responsibilities at once, aiding them adjust them self to adapt more comfortably to the new area.

ISACA 2022, *How to transition from general IT to cybersecurity*, viewed 24 September 2024, <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/how-to-transition-from-general-it-to-cybersecurity>.

CompTIA 2024, *From IT support to cybersecurity*, viewed 24 September 2024, <https://www.comptia.org/blog/from-it-support-to-cybersecurity>.

**End of Assessment**