**Legislation and Policies Report**

Created by

**UPTOWN IT**

For

**TURTLE MOVERS**

**PROJECT REFERENCE:**

**DATE:**

Contents

[1 Abstract 3](#_Toc124768025)

[2 Introduction 4](#_Toc124768026)

[3 Cyber Security Legislative and Regulatory Review 4](#_Toc124768027)

[3.1 Regulators 5](#_Toc124768028)

[4 Cyber Security Findings and Recommendations 5](#_Toc124768029)

[5 Privacy Policies and Best Practices Review 6](#_Toc124768030)

[6 Privacy Compliance Findings and Recommendations 6](#_Toc124768031)

[7 Ethical behaviour in cyber security 7](#_Toc124768032)

[7.1 Code of Practice (for only one of the two organisations) 7](#_Toc124768033)

[7.2 Ethical practices (this part covers both organisations) 7](#_Toc124768034)

[8 Conclusion 8](#_Toc124768035)

[Appendix 9](#_Toc124768036)

[Organisation policies, procedures and best practices documentation 9](#_Toc124768037)

Remove all blue text once your report is completed. The blue text is intended at giving you some pointers for the document content.

# 1 Abstract

Write the abstract after you have completed the report.

The abstract is not an introduction. The abstract must include a detailed summary of findings and recommendations.

# 2 Introduction

**The legislation and policies report for Turtle Movers is an in depth document that outlines the company's compliance with relevant laws, regulations, and industry standards. Turtle Movers is a small removalist family business that operates across Australia with a fleet of 50 trucks. The company operates exclusively online, and its only physical presence is its headquarters in Sydney, NSW.**

**Given the ever increasing threat of cyber attacks and data breaches, it is important for Turtle Movers to ensure the security and privacy of its clients' data. The company's management has acknowledged concerns about its online security and cyber legislation compliance. The report will examine Turtle Movers' policies and procedures for safeguarding client data and complying with relevant legislation. By conducting a thorough review of the company's policies and procedures, the report aims to identify any areas where Turtle Movers may be at risk of non-compliance and make recommendations for improving its overall compliance.**

# 3 Cyber Security Legislative and Regulatory Review

**Turtle movers operates in removal and logistics sector which involves the company collecting and relocating the goods and personal items of their customers to wherever they are moving to whether it be across cities or states.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SECTOR** |  |  |  |  |
| **CYBER SECURITY and related**  **LEGISLATION** | **SCOPE** | | | **BUSINESS AREAS/ACTIVITIES AFFECTED** |
| **Federal** | **State** | **Territory** |
| **Privacy Act 1988 (Cth)** | **X** |  |  | **All areas** |
| **Australian Privacy Principles (APPs)** | **X** |  |  | **All Areas** |
| **Electronic Transactions Act 1999 (Cth)** | **X** |  |  | **Online payments** |
| **Cybercrime Act 2001 (Cth)** | **X** |  |  | **Cyber crime and computer related offences** |
| **Notifiable Data Breach (NDB)** | **X** |  |  | **All areas** |
| **Crimes Act 1900 (NSW)** |  | **X** |  | **Cyber crime and computer related offences** |
| **Privacy and Personal Information Protection Act 1998 (NSW)** |  | **X** |  | **All areas** |

**Since Turtle Movers only operates in Australia, there are not any international legislation’s they must abide by. However they must follow the PCI-DSS (Payment Card Industry Data Security Standard). The PCI-DSS is not officially an international legislation but a global standard in regards to online payment so it will be included in the table below.**

|  |  |  |
| --- | --- | --- |
| **INTERNATIONAL**    **CYBER SECURITY**  **LEGISLATION** | **BUSINESS AREAS/ACTIVITIES AFFECTED** | **IMPACT on DATA SECURITY** |
|
| **PCI-DSS** | **Online payments** | **Data security of payment card information** |

**One example of an interdependency between different legislative instruments is the relationship between the Privacy Act 1988 (Cth) and the Notifiable Data Breaches (NDB) scheme. The Privacy Act outlines the requirements for how businesses handle personal information, while the NDB scheme requires businesses to report eligible data breaches and notify affected individuals of the breach. These two work together to ensure that businesses are held accountable for protecting the personal information they collect and use, and to provide individuals with greater transparency and control over their personal information that businesses collect.**

**The Office of the Australian Information Commissioner (OAIC) is a key regulator that has a significant impact on the security of Turtle Movers' business data operations. The OAIC is responsible for enforcing the Privacy Act and the NDB, and can investigate and impose penalties breach their obligations under these instruments. Therefore, it is important for Turtle Movers to ensure that they comply with these legislation's to avoid potential fines or have the business shut down.**

**The Privacy act 1988 had a review conducted in 2022 and several proposals were made to the act. One of the proposals to the act is to clarify what exactly is protected under the act. This would mean it would be easier for Turtle movers to know what data they need to protect when collecting and dealing with their customers data. Another proposal is to strengthen the requirement to keeping personal data secure and destroying it when it is no longer needed. This would mean the business would need to ensure the data is kept as secure as possible and destroyed when it is no longer needed.**

**The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 which was updated in 2021 is about how law enforcement can get warrants to access encrypted data that may relate to a serious crime etc. This affects Turtle Movers as if they hold data that may help an investigation they must provide it if there is a warrant or they can voluntarily hand it over to law enforcement.**

## 3.1 Regulators

|  |  |  |
| --- | --- | --- |
| **REGULATOR** | **ROLE** | **SCOPE** |
| Australian Prudential Regulation Authority (APRA) | **APRA is responsible for regulating financial institutes. They maintain the safety and soundness of the financial institutes and protect the interests of all who are invloved.** | **ARPA covers banks, insurance companies and superannuation companies.** |
| Australian Securities and Investments Commission (ASIC) | **ASIC is responsible for regulating financial markets and services so that the markets are fair and efficient.** | **The scope of ASIC's responsibilities covers all corporations, financial markets, and financial services providers.** |
| Australian Competition and Consumer Commission (ACCC) | **The ACCC maintains and promotes competition while making sure it is all fair and stop anything that is anti-competitive or harmful.** | **ACCC covers all markets and industries in Australia.** |
| Australian Energy Sector Cyber Security Framework (AESCSF) | **The AESCSF is a framework that helps energy organisations manage their cyber-security risks** | **AESCSF covers all organisations in the energy sector** |
| Protective Service Manual (Australian Government rules for cybersecurity) | **The Protective Security Policy Framework (PSPF) is a framework for protecting government resources and the Protective service manual (PSM) falls under the PSPF and outline rules/guidelines for government agencies to manager their cyber risks** | **The PSM covers all government agencies.** |

# 4 Cyber Security Findings and Recommendations

**As a Cyber consultant, I would recommend that Turtle Movers takes the following steps to ensure compliance with legislations and regulatory requirements.**

1. **Compliance with legislation and regulatory requirements:**
   1. **Conduct audits to ensure all areas are compliant.**
   2. **Ensure all customers data is protected in accordance with the Privacy Act.**
   3. **Develop an organisational policy that covers all aspects of cyber-security and data protection**
2. **International cyber security legislation impacting their businesses** 
   1. **Since the business only works in Australia there are no international legislations they must follow however they should still follow global standards such as the PCI-DSS.**
3. **Potential impact of upcoming reforms in privacy and consumer and surveillance legislation**
   1. **The company should monitor for changes to any of the legislations and implement them as soon as possible.**
   2. **Regularly review their own policies to ensure it is still in accordance with the privacy act as well as the consumer and surveillance legislation.**

# 5 Privacy Policies and Best Practices Review

Introductory paragraph.

Examine the privacy documentation provided. Review policy compliance across the organisation against current standards.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **STANDARDS**  **APPs** | **APP Desription** | **Turtle Movers** | **COMPLIANCE** | | | | |
| **Full** | **Partial** | **Poor** | **Non-Compliance** | **N/A** |
| **Open and transparent management of personal information** | **must have a clearly expressed and up-to-date Privacy Policy about how it manages personal information** | **Turtle Movers has a clear policy on how customers data is handled.** | **X** |  |  |  |  |
| **Anonymity and pseudonymity** | **Users must have the option of not identifying themselves or using a pseudonym** | **Nothing stated in policy** |  |  |  | **X** |  |
| **Collection of solicited personal information** | **Only collect data that is necessary for the operation.** | **Policy states they only collect information needed for the move** | **X** |  |  |  |  |
| **Dealing with unsolicited personal information** | **Entities must delete or de-identify unsolicited personal information** | **Not stated** |  |  |  | **X** |  |
| **Notification of the collection of personal information** | **Entities must inform individuals about the collection of their personal information** | **States what data is collected and how it will be used** | **X** |  |  |  |  |
| **Use or disclosure of personal information** | **Entities must only use or disclose personal information for the primary purpose it was collected** | **States what data is going to be used for** | **X** |  |  |  |  |
| **Direct marketing** | **organisation must not use or disclose personal information it holds for the purpose of direct marketing** | **Nothing stated** |  |  |  | **X** |  |
| **Cross-border disclosure of personal information** | **Before an** **entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information** | **Not applicable since they only operate in Australia** |  |  |  |  | **X** |
| **Adoption, use, or disclosure of government-related identifiers** | **restricts the adoption, use and disclosure of government related identifiers by organisations** | **Nothing stated** |  |  |  | **X** |  |
| **Quality of personal information** | **entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete** | **Nothing stated** |  |  |  | **X** |  |
| **Security of personal information** | **must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure** | **Secures data with encryption and strong passwords** | **X** |  |  |  |  |
| **Access to personal information** | **entity that holds personal information about an individual to give the individual access to that information on request** | **Nothing Stated** |  |  |  | **X** |  |
| **Correction of personal information** | **entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading** | **Nothing stated** |  |  |  | **X** |  |

|  |  |  |
| --- | --- | --- |
| **BEST PRACTICES** | **EVALUATION/SHORTCOMINGS** | **PROPOSED IMPROVEMENTS** |
| **Data backup** | **It is good that Turtle movers backs up their data but they do not state how often it is done, where it is store and how long it is kept for.** | **They should specify how often the data is backed up and make sure it is store somewhere else with encryption and correct access controls. They should also specify how long the backups are kept for.** |
| **Conducting proper disposal of electronic and physical copies of personal and protected data** | **It is good that the company disposes of data but does not state how it is done meaning it can be mishandled during disposal. There is no specified responsible party for the destruction of the data** | **The company should specify exactly how the data is handled and disposed of. It should also be stated who is responsible for the disposal and it should be made sure that it is disposed in a legal manner.** |

# 6 Privacy Compliance Findings and Recommendations

**After reviewing Turtle Movers' privacy policy and privacy practices, here are the findings and recommendations:**

**a) Level of compliance with current privacy legislation and required improvements:**

1. **Turtle Movers' privacy policy appears to be generally compliant with the Australian Privacy Act 1988 (Cth) and other relevant privacy laws and regulations. However, there are a few areas where improvement is needed, including:** 
   1. **Consent: Even though it is stated in the privacy policy that consent will be seeked when data is needed to be shared with a third party, it does not state how this consent is gathered and the documentation process.**
   2. **Retention and disposal of data: Turtle Movers do state that data will be disposed off after being kept for the required time but it does not state how long this time is and how the data is disposed of.**
   3. **Transparency: The policy could be more transparent in how the company collects, uses, retains and discloses personal information by being more specific about each of the mentioned categories.**
2. **Adequacy of current practices and required improvements: Turtle Movers' privacy practices appear to be adequate in protecting the privacy of customers' personal data. However, there are a few areas where improvement is needed, including:**
   1. **Employee training: Although staff go through training, the company should ensure this training is up to date and when any of the laws/legislations change, the staff should be retrained.**
   2. **Insider threats: Turtle Movers should continue to improve their efforts to protect against insider threats by implementing access controls, monitoring employee activity, and conducting regular audits.**
   3. **Disposal of data: Turtle Movers should ensure that they dispose of personal data securely and in a legal manner to prevent data breaches and protect the privacy of customers' personal data.**
   4. **Data backup: While Turtle Movers states that they back up their data, they ensure the backups are regular and stores somewhere else with proper encryption and access controls as well as define how long they are retained for.**

**Overall, Turtle Movers does appear to take privacy and their customer’s data seriously, there are several area that need to be improved to follow laws and legislations within Australia.**

# 7 Ethical behaviour in cyber security

## 7.1 Code of Practice (for only one of the two organisations)

Write a complete Ethics Code of Practice for the organisation’s cyber security technicians.

Explain how the code will be distributed and implemented in the organisation.

As a cyber security technician at Turtle Movers, you are expected to adhere to the following code of practice to ensure all data is handled ethically and securely:

1. Respect confidentiality and privacy: As a technician, you will have access to the customers personal data included and not limited to financials, addresses and other personal information. You must not share or disclose any information to any unauthorised party.
2. Maintain data integrity: You must ensure that any and all data transmitted or stored must be accurate and complete. You must regularly check for any signs of tampering or any unauthorised access to the data.
3. Ensure compliance with legislations and laws: You must ensure that everything you do adheres to the relevant legislation and ensure everything related to cyber within the company also is compliant.
4. Deal with vulnerabilities ethically: As the technician you must immediately report any vulnerabilities found within the system. You should not exploit it for your own personal gain or any other malicious activities.
5. Maintain up to date awareness and training: With the ever evolving cyber world, you must ensure you are up to date with the latest in vulnerabilities and developments in the field. It is also highly recommended that you participate in training and skill development.
6. Ensure system availability: The availability of the companies website is crucial to business so it is your responsibility that the website is available to customers at all times and when it goes you should have a plan in place.

By adhering to these practices you will keep the data of Turtle Movers secure while doing it all ethically.

The code will be distributed throughout the organisation by training all technicians about the code of practice. This training will include the importance of the CIA triad and how best to follow the ethics code of practice. Regular monitoring and accountability will also ensure that the code is being followed at all times.

## 7.2 Ethical practices (this part covers both organisations)

Introductory paragraph.

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

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

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

Consequences of unethical behaviour:

1. 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.
2. Outline the consequences of unauthorised access to network devices
3. Outline the consequences of bypassing copyright media and applications obtained via file sharing or downloading

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 |  |

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** |
|  |  |  |
|  |  |  |
|  |  |  |

# 8 Conclusion

Write a conclusion for the report.

# 9 Contingency task

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.

# Appendix

## Organisation policies, procedures and best practices documentation

In this section, you should include all the organisation’s documentation provided to the MidTown IT Analyst/Consultant before the review and report completion.

If the documentation exists, it may include:

* Cyber Security Policy
* Cyber Security Best practices
* Privacy Policy
* Privacy Best practices
* Ethics policies and/or policies and procedures

Other appendices can be created as necessary