**Legislation and Policies Report Template**

Created by

**UPTOWN IT**

For

**<<Turtle Movers >>**

**PROJECT REFERENCE:****474807620**

**DATE:28/09/2024**

**Amir Mahdi Sarikhani fard**

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)

# 1 Abstract

Here in this report, I have tried to cover details on my analysis of the Turtle Movers’ operation and their compliance with Australian cyber security legislatives based on the details and documents provided. The performed analysis on privacy policies and procedures was a necessary step for this organization, as we found that they are now enforcing basic facilities and policies while they are operating nationally across Australia. Moreover, after reviewing relevant Australian laws and regulations associated to their operations, we believe it is beneficial to briefly describe upcoming reforms in privacy legislation and possible ways in which this organization will benefit from them. Furthermore, we researched and analysed this organization’s operations, which allowed us to evaluate their impact on data security. Our findings highlighted the importance of adhering to relevant national regulations, enabling us to provide an overview of how their operations will be affected by these legislative changes. We also narrated how interdependencies between different legislative instruments of cyber security may occur and provided an example. Lastly, we examined the organization’s policies and procedures (the organization’s ethical practices were also subject to evaluation) and suggested revisions to improve them based on the Australian Privacy Principles. We finished the report by making suggestions and recommendations, stating that there is a need for them to read and review our suggested techniques and policies if they wish to implement them (although we mentioned that they are necessary and need to be used eventually).

# 2 Introduction

This organization is called Turtle movers. They are specialized in removal and movement services. They used to only operate in New South Wales region with 2 trucks but today they are operating around Australia with 50 trucks of different capacity. This company’s operation seems to be relying on their online services and the only physical presence is its headquarter located in Sydney, NSW. As mentioned, their website is where almost all of transactions are handled. One of these transactions can be bookings (their cancellations and rescheduling). Then we have got insurance, payments through credit cards and bank transfers, refunds, and also clients reward and loyalty benefits. Their security system is reported to be basic, a protection provided by the one who provided the website and also security person who is self-trained in his house.

# 3 Cyber Security Legislative and Regulatory Review

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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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].

As we started analysing their operations, we found that this organization only operates in Australia. Here this organization need to check even if there is any possible interaction overseas and then check for relevant laws.

|  |  |  |
| --- | --- | --- |
| **INTERNATIONAL**  **CYBER SECURITY**  **LEGISLATION** | **BUSINESS AREAS/ACTIVITIES AFFECTED** | **IMPACT on DATA SECURITY** |
|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

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>

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.

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>.

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>

## 3.1 Regulators

|  |  |  |
| --- | --- | --- |
| **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. |

# 4 Cyber Security Findings and Recommendations

* 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.

# 5 Privacy Policies and Best Practices Review

Introductory paragraph.

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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>.

Yellow highlighted ones are for organization 1

|  |  |  |
| --- | --- | --- |
| **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, |

# 6 Privacy Compliance Findings and Recommendations

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.

# 7 Ethical behaviour in cyber security

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

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>.

They need to engage stakeholders, employees and possible experts who are working with organization externally to learn about it and share their thoughts if they are allowed to. Communication can be good if organization invite stakeholders and employees to a launch event or a meeting to introduce the ethical code to all of those who gathered there. In this way everyone will be involved in this process and will be informed. But this is not enough and there will be a need for reminders, policies need to be broadcasted by email, newsletters and posters on wall where lots of people can see it. Moreover, there would be a need for training programs or workshops to help them understand them in better way.

After this for implementing them, they need to integrate the ethical code into their existing policies and procedures on where are storing all of them. There should be a committee to monitor and enforce these codes. They need to encourage, monitor and feedback for improvement. In this way, they can find a way to revies and update codes.

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

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. 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/>.

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.

A)

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/.

B)

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. 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.

2. 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.

3. 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.

4. 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. |

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** |
| 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. |

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

# 8 Conclusion

In conclusion, I highlighted this organization overall level of compliance with Australian cyber security laws as they are now operating widely around Australia. While most of their privacy policy seems to be current and meet standards, I found that their policy requires enhancements as they are also growing their presence in the market. In order to assure that they will stay secure in a longer period of time, we encourage them to establish response plans, conducting regular audits and also implementing data minimization practices to save only essential information. Additionally, I recommended adopting advanced encryption techniques and enforcing password policy which will boost their data protection efforts. Lastly, we discussed about possible new reforms in privacy and consumer legislation emerge, Turtle Movers must adapt their policies prevent facing challenges of being compliant with them. In this way, they will not only take steps to safeguard customer data but also enhance their reputation.

# Appendix

## Organisation policies, procedures and best practices documentation

# POLICES for TURTLE MOVERS

# PRIVACY POLICY

|  |  |  |  |
| --- | --- | --- | --- |
| DATE | AUTHOR | SUMMARY of CHANGE | APPROVED BY |
| 3rd Oct 2022 | George Green | Created | Manager |
|  |  |  |  |

Turtle Movers is committed to protecting the privacy of the personal information of our clients and employees. We value and respect the privacy of the people we do business with and who work for our company.

Turtle Movers’ Privacy Policy complies with the Australian Privacy Act 1988 (Cth) and other relevant privacy laws and regulations.

This Privacy Policy covers all employees and clients of the company and outlines how we collect, use, retain and disclose personal information gathered to carry out our business activities.

**Information we may collect**

* Contact information
* Name and surname
* Pickup address
* Delivery address
* Email address
* Phone number
* Transaction details and history
* Bookings
* Cancellations and rescheduling
* Insurance
* Payment method
* Refunds
* Rewards and loyalty benefits
* Banking and/or credit details
* Details of payment method (For example, financial institution, account)
* Correspondence and communication
* Emails
* Phone messages
* Phone records

**How data is collected**

Turtle Movers collect data from your online transactions. Transactions include information on your online removalists’ queries, service bookings and payments.

**How data is used**

We use the data collected from your online transactions to:

* process your online removalists bookings and related activities
* deliver a personalised experience
* manage internal administrative and taxation processes
* support our marketing strategy

We retain your personal information linked to removalists’ jobs for the period of time required by the taxation department. For other situations, we only retain the data collected for the duration of the business activity.

**Disclosure of information**

Turtle Movers does not share or sell your data to third parties and will seek your consent if personal data needs to be shared with a third party, such as an insurance company.

There may be circumstances where we need to disclose your data to legal authorities, and we will do so as permitted by the law.

**Retention and disposal of data**

Turtle Movers will keep your personal contact details and transaction data stored securely for the required period of time to comply with taxation legislation. After that period has elapsed, your data will be destroyed.

**Concerns and complaints**

To lodge a complaint against this policy, download the complaint form from our website and follow the lodgement instructions. All complaints are addressed promptly and professionally.

Contact us if you have any questions or concerns regarding this policy. Contact details:

* Email: turlemovers@tm.com.au
* Phone: 123456789

# PRIVACY PROCEDURES for Turtle Movers

**Lodging a Privacy Complaint**

**Purpose:** This procedure outlines the actions that need to be carried out to lodge a Privacy Policy complaint.

**Scope:** All employees and clients of Turtle Movers

**Responsibilities:**

The responsibility for actioning, processing and resolving privacy complaints falls on Turtle Movers’ management.

**Lodging a privacy complaint:**

* To lodge a privacy complaint, you need to access the Privacy Complaint Form from the company website. It is located in the legal section of the website. You can request the form to be sent to you via email.
* Once you have the form, complete all sections with as many details as possible to ensure that there are no delays in processing the complaint.
* Submit the completed form if you accessed the website form, or email the form if you requested one via email.

**Acknowledgement of privacy complaint**

* Turtle Movers take complaints seriously, and will endeavour to acknowledge receipt of the complaint within 48 hours.

**Processing a privacy complaint**

* Management will investigate the complaint within 7 days of receiving it. During this period, they may contact the complainant if further information is required.
* In most cases, complaints are resolved in conversation with the complainant by addressing all the issues and concerns and negotiating a resolution.
* If more information or investigation is required and the process is delayed, management will keep the complainant continuously updated on the process.

**Resolving and closing a privacy complaint**

* Once processing, investigation and communication with the complainant has concluded, management will communicate the resolution to the complainant. If both parties agree at this stage, the resolution will be formally documented and archived by management.
* If it is pertinent, management will formally apologise to the complainant and take the necessary measures to eradicate the problem.
* In the event that a mutually agreeable resolution has not been reached, either party may decide to get independent legal advice on the matter.
* Turtle Movers is committed to resolving all complaints promptly and amicably.

# PRIVACY PRACTICES for TURTLE MOVERS

Turtle Movers has in place a set of privacy practices to ensure that employees comply with company policy regarding privacy. These practices aim to protect the privacy of customers’ personal data.

**Privacy practices:**

* Enforce strong passwords.
* Employ encryption for sensitive data.
* Compulsory privacy training and awareness of all employees.
* Back up data.
* Protect data from insider threats. This type of threat may originate from:
* Negligent employees
* Third-Party Partners
* Ex-employees
* Policy Evaders
* Use end-point security systems to protect data
* Conduct proper disposal of electronic and physical copies of personal and protected data.
* Implement a trifecta of physical, technical, and administrative controls to safeguard personal information.