Legislation and Policies Report

Created by

UPTOWN IT

For

TURTLE MOVERS & ANGELONIA FASHION

PROJECT REFERENCE: AT2
DATE: 13/03/2023

Contents

Table of Contents

PART 1 – ANGELONIA FASHION

1 Introduction

The legislation and policies report for Angelonia Fashion is an in-depth document that outlines the company's compliance with relevant laws, regulations, and industry standards. Angelonia Fashion is a family business that owns multiple shops across Australia as well as export their creations internationally.

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

2 Cyber Security Legislative and Regulatory Review

Angelonia Fashion operates in the fashion sector which involves the company taking orders in both physical and online form. They also operate internationally and export their goods to customer in other countries

2.1 Local Legislations

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

2.2 International Legislations

Legislation	Area affected	Impact on data security
General data protection regulation	**All areas**	**Data needs to be encrypted, proper access controls implemented, incident response plan in place, regular security testing**
PCI-DSS	**Payments**	**Data security of payment card information and protecting cardholder data**

2.3 Interdepency between different legislations

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.

2.4 Key regulator

The Office of the Australian Information Commissioner (OAIC) is a key regulator that has a significant impact on the security of Angelonia Fashion’s 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 the company to ensure that they comply with these legislation's to avoid potential fines or have the business shut down.

2.5 Upcoming/current reforms to privacy legislations

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 Angelonia Fashion 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.

2.6 Upcoming/current reforms to surveillance legislations

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 the company 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 Cyber Security Findings and Recommendations

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

a) **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 and the GDPR.**
   3) **Develop an organisational policy that covers all aspects of cyber-security and data protection**

b) **International cyber security legislation impacting their businesses**
   1) **Ensure all data of EU customers is protected in accordance to the GDPR as well as the Australian Privacy act**
   2) **Ensure all payment data is secure as per the PCI-DSS in all forms of payment whether it be physical or online.**

c) **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 like they are currently doing.**
   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.**

4 Privacy Policies and Best Practices Review

STANDARDS APPs	APP Desription	Angelonia Fashion	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**	**States what data is collected and how it will be used**	**X**				
Anonymity and pseudonymity	**Users must have the option of not identifying**	**Nothing stated about the option for anonyminity**				**X**	

	themselves or using a pseudonym						
Collection of solicited personal information	**Only collect data that is necessary for the operation.**	**States they only collect the data needed to the operation**	**X**				
Dealing with unsolicited personal information	**Entities must delete or de-identify unsolicited personal information**	**Nothing stated about disposal of data**				**X**	
Notification of the collection of personal information	**Entities must inform individuals about the collection of their personal information**	**States that clients will be informed about data collection**	**X**				
Use or disclosure of personal information	**Entities must only use or disclose personal information for the primary purpose it was collected**	**Only use data for the purpose of the operation**	**X**				
Direct marketing	**organisation must not use or disclose personal information it holds for the purpose of direct marketing**	**Offers and opt-in/out system for their marketing**	**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**	**Nothing stated**				**X**	
Adoption, use, or disclosure of government-related	**restricts the adoption, use**	**Nothing stated**				**X**	

identifiers	**and disclosure of government related identifiers by organisations**						
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 states**				**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**	**Encrypts all data collected**	**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,**	**Nothing stated**				**X**	

	relevant and not misleading						

BEST PRACTICES	EVALUATION/SHORTCOMINGS	PROPOSED IMPROVEMENTS
Secure Password Policy	**It is good that the company is using a password policy, but it does not state what it is meaning it could be not a strong as recommended.**	**They should specify exactly what their password policy is and also include the time frame for when every employee should change their password.**
Encryption data	**It is a good practice for Angelonia Fashion to encrypt customer's data but they do not specify how they encrypt and what standard they use.**	**The company should specify what encryption method is used e.g. AES with 32 character password so that users can be reassured their data is safe.**

5 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. **Angelonia Fashion's 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:**
    a) **Access of data: The company should state how user's are able to request and access their data as it is one of the privacy principles**
    b) **Retention and disposal of data: Angelonia Fashion does not state if they dispose of users data and how they do it, this should be updated to explicitly state that data will be destroyed when no longer needed.**
    c) **GPDR: There is no explicit mention of the GDPR and the document should mention how the company is compliant when interacting with EU customers.**

2. **Adequacy of current practices and required improvements: Angelonia Fashion's current practices are quite in depth and cover most required things however the are a few improvements that can be made:**
    a) **The company should be more specific about how they complete each practice such as specifying how the data is encrypted and what the password policy is.**

b) **The practice must also mention how data is destroyed when not needed and who is responsible for that.**

Overall, Angelonia Fashion's takes their customer's data and privacy very seriously but there are a few areas that can be improved to be more transparent to customers especially those in the EU. Otherwise the company obliges by most of the legislations required in Australia.

6 Ethical behaviour in cyber security

6.1 Code of practice

Completed in TURTLE MOVERS

6.2 Ethical Practices (Completed by Muzammil)

6.2.1 Red Team tools

1. **BloodHound: BloodHound is a tool that helps red teams identify and exploit Active Directory (AD) vulnerabilities. It maps out the AD environment and identifies potential attack paths, allowing red teams to identify connections between different users.**
2. **Mimikatz: Mimikatz is a password-dumping tool that can be used by red teams to extract plaintext passwords and other sensitive information from target systems. It works by exploiting vulnerabilities in the Windows authentication system, and can be used to escalate privileges using the found passwords.**
3. **Metasploit: Metasploit is a popular penetration testing framework that can be used by red teams to identify and exploit vulnerabilities in target systems. It provides a range of exploit modules, payloads, and tools that can be used to compromise systems, gain access to sensitive information, and escalate privileges.**
4. **Cobalt Strike: Cobalt Strike is a powerful tool that enables red teams to simulate advanced persistent threats (APTs) and launch sophisticated attacks that simulate real world attacks. It includes features like command-and-control (C2) servers and a range of post-exploitation tools that can be used to maintain persistence and evade detection.**

6.2.2 Blue Team Tools

1. **Firewalls: Firewalls are a type of security tool that monitor and control traffic between a network and the internet. Firewalls can block traffic from known malicious sources, prevent unauthorized access to the network, and help to identify and stop attacks in progress. Angelonia Fashion could use firewalls to protect their network from cyber-attacks by configuring them to block unauthorized traffic and limit access to sensitive information.**
2. **Intrusion Detection Systems (IDS): IDS are tools that monitor network traffic for signs of unauthorized access or suspicious activity. IDS can detect anomalies such as unusual network traffic patterns, unexpected data transfer, and unauthorized access attempts. Angelonia Fashion could use IDS to detect and respond to cyber-attacks in real-time, minimizing damage and preventing the attackers from gaining further access to the network.**
3. **Vulnerability Scanners: Vulnerability scanners are tools that identify security weaknesses in software, operating systems, and other network components. Angelonia Fashion could use vulnerability scanners to identify vulnerabilities and prioritize patching efforts. This could help to prevent attackers from exploiting known vulnerabilities and gaining access to the network.**
4. **Endpoint Protection: Endpoint protection tools are designed to secure individual devices such as laptops, desktops, and mobile devices. These tools can protect against malware, viruses, and other threats by scanning for malicious files and behavior. Angelonia Fashion could use endpoint protection tools to protect their devices and prevent them from becoming infected with malware, which could be used to gain access to the network.**

6.2.3 Ethical practices on public networks

1. **Obtain proper authorization: Employees should only use red and blue team tools on public networks after obtaining proper authorization from the company. Unauthorized testing can be considered as hacking and may lead to legal consequences.**
2. **Use the tools only for intended purposes: Employees should use the red and blue team tools only for their intended purposes, which is to test the security of public networks. Using these tools for any other purposes, such as personal gain or to harm other organizations, is unethical and illegal.**
3. **Respect privacy: Employees should respect the privacy of others while conducting security testing on public networks. They should avoid accessing or collecting any personal or sensitive information that is not related to the intended purpose of the testing.**
4. **Avoid damaging systems: Employees should take care not to cause any damage to the systems they are testing. They should ensure that they do not delete, modify or corrupt any data or files while conducting the testing.**
5. **Follow ethical guidelines: Employees should follow ethical guidelines while using red and blue team tools on public networks. They should not engage in any activity that could harm organisations, and should report any vulnerabilities or issues discovered during the testing to the appropriate authorities.**
6. **Document all findings: Employees should document all findings and keep accurate records of their testing activities. This documentation can be used to inform security policies and procedures, as well as to demonstrate compliance with ethical and legal standards.**

7. **Protect sensitive information: Employees should protect any sensitive information that they may come across while conducting security testing. They should not share this information with unauthorized individuals or organizations, and should take appropriate measures to secure it.**

6.2.4 Consequences of unethical behaviour

1) **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 unauthorized can be severe. Misusing these tools could result in criminal charges for violating various laws, including the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and state laws governing unauthorized access to computer systems. Such violations could lead to fines, imprisonment, or both. Additionally, if Angelonia Fashion stores personal data of its customers, a data breach resulting from unauthorized use of these tools could lead to civil liability for damages, regulatory fines, and loss of reputation.**
2) **Unauthorised access to network devices can result in significant consequences for Angelonia Fashion. The unauthorized access can lead to the loss of confidential information, data breaches, or even theft of intellectual property. In addition, unauthorized access can allow attackers to install malware or modify the configuration of network devices, resulting in system downtime or a complete system failure. Such an attack can have significant financial implications for the company, including loss of revenue, legal costs, and expenses associated with repairing the system.**
3) **Bypassing copyright media and applications can result in legal consequences for Angelonia Fashion. The company could face legal action for copyright infringement, which could result in significant financial penalties, including damages and legal fees. Additionally, Angelonia Fashion could face loss of reputation and potential loss of customers who do not wish to associate with a company that engages in unethical behavior. Finally, bypassing copyright media and applications may also be a violation of the terms of service of the software or media, which could result in the loss of the right to use the software or media.**

6.2.5 Unethical behaviour from technicians

UNETHICAL BEHAVIOUR	IMPACT ANALYSIS
Unauthorized Access	**A cyber security technician could intentionally access confidential or sensitive data without proper authorization. This unethical behavior can lead to serious implications, such as theft of personal information, financial loss, and damage to the reputation of Angelonia Fashion. It can also lead to legal consequences if the unauthorized access violates any regulations or laws.**
Data Manipulation	**A cyber security technician could manipulate data to create false information or hide**

	information from the management. This unethical behavior can lead to incorrect business decisions, loss of reputation, and financial loss. Moreover, it can also violate regulations or laws, leading to legal consequences.
Data Breach	**A cyber security technician may intentionally or unintentionally cause a data breach, allowing hackers or other unauthorized parties to gain access to sensitive or confidential data. This unethical behavior can lead to serious implications, such as financial loss, reputation damage, and legal consequences. Moreover, it can also violate regulations or laws, leading to further legal consequences.**
Cyber Espionage	**A cyber security technician may engage in cyber espionage to gain an unfair advantage over competitors. This unethical behavior can lead to serious implications, such as loss of intellectual property, damage to the reputation of Angelonia Fashion, and legal consequences. Moreover, it can also lead to the loss of trust and confidence from clients and partners.**

Part 2 – TURTLE MOVERS

1 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.

2 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.

2.1 local legislations

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**

2.2 International legislations

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 and protecting cardholder data**

2.3 Interdepency between different legislations

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.

2.4 Regulator

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.

2.5 Upcoming/current reforms to privacy legislations

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.

2.6 Upcoming/current reforms to surveillance legislations

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.

2.7 Regulators and their roles

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.**

3 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.

a) **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**

b) **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.**

c) **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.**

4 Privacy Policies and Best Practices Review

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	States what data is going to be used for	X				

	information for the primary purpose it was collected						
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.**

5 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:**
    a) **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.**
    b) **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.**
    c) **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:**
    a) **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.**
    b) **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.**
    c) **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.**
    d) **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.

6 Ethical behaviour in cyber security

7.1 Code of Practice

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 (Completed by Muzammil)

7.2.1 Red Team tools

1. **Metasploit Framework: This is a popular open-source exploitation framework that allows red teams to launch attacks against various types of systems and applications. It has a wide range of modules and exploits that can be customized to suit different attack scenarios, making it a powerful tool for testing and identifying vulnerabilities in an organization's defenses.**
2. **Cobalt Strike: This is a commercial penetration testing tool that enables red teams to simulate advanced threat actors and launch targeted attacks against a company's network infrastructure. It has features such as beaconing, social engineering, and phishing that can be used to compromise user credentials and gain access to sensitive information.**
3. **Empire: This is another open-source tool that provides a modular framework for red teams to launch post-exploitation attacks against Windows, macOS, and Linux systems. It includetwork exploration and reconnaissance tool that can be used to map an organization's network topology, identify open ports, and discover potential vulnerabilities. It can be used to gather valuable intelligence that can be used by red teams to plan and execute targeted attacks.s features such as keylogging, credential theft, and lateral movement that can be used to pivot through a network and gain deeper access to target systems.**
4. **Nmap: This is a network exploration and reconnaissance tool that can be used to map an organization's network topology, identify open ports, and discover potential vulnerabilities. It can be used to gather valuable intelligence that can be used by red teams to plan and execute targeted attacks.**

7.2.2 Blue Team tools

1. **Intrusion Detection System (IDS): An IDS monitors network traffic for suspicious activity and alerts security personnel when potential threats are detected. IDS can be host-based or network-based, and they use various methods to detect attacks such as signature-based, anomaly-based, and heuristic-based techniques.**
2. **Security Information and Event Management (SIEM): A SIEM system collects, analyzes, and correlates security events from various sources such as firewalls, IDS, antivirus, and other security devices. SIEM systems can provide real-time alerts and detailed reports that help security teams to identify and respond to security incidents.**
3. **Endpoint Detection and Response (EDR): EDR tools protect endpoints such as servers, desktops, and laptops from advanced threats such as malware, ransomware, and fileless attacks. EDR solutions use behavioral analysis, threat intelligence, and machine learning to detect and respond to threats in real-time.**
4. **Vulnerability Management (VM): VM tools scan the network and endpoints to identify vulnerabilities and provide prioritized recommendations for remediation. VM solutions can automate the patching process and ensure that the network is up-to-date with the latest security patches.**

7.2.3 Ethical practices on public networks

1. **Red and blue team tools can be valuable for testing the security of public networks, but they should be used responsibly and ethically. Here are some ethical practices that employees can follow when using these tools:**
2. **Obtain proper authorization: Employees should obtain proper authorization before using red and blue team tools on public networks. They should ensure that they have the necessary permissions to perform security testing.**
3. **Use the tools only for security testing: Employees should use the tools only for security testing purposes and not for any other purposes.**
4. **Respect privacy: Employees should respect the privacy of others when using red and blue team tools. They should not access or collect any personal information unless it is necessary for security testing and they have obtained proper authorization.**
5. **Avoid causing harm: Employees should avoid causing any harm to the network or its users while using red and blue team tools. They should ensure that their testing activities do not disrupt the network or cause any damage.**
6. **Report vulnerabilities: If employees find any vulnerabilities during their testing activities, they should report them to the appropriate authorities immediately. They should not exploit the vulnerabilities or share them with unauthorized parties.**
7. **Keep the testing activities confidential: Employees should keep the details of their testing activities confidential. They should not disclose any information about their testing activities to unauthorized parties.**
8. **Use secure communication channels: Employees should use secure communication channels when discussing the results of their testing activities. They should ensure that the communication is encrypted and that only authorized parties have access to it.**

7.2.4 Consequences of unethical behaviour

1. **Misusing skills gained using red and blue team tools and engaging in unauthorized data breaches can lead to severe legal consequences. Individuals who engage in such unethical behavior may be subject to criminal prosecution, fines, and imprisonment. Additionally, the affected parties may sue them for damages resulting from the breach, leading to civil lawsuits.**
2. **Unauthorized access to network devices can lead to several consequences. Firstly, the individual may be breaking the law, leading to criminal charges, fines, and imprisonment. Secondly, unauthorized access may disrupt the network's functionality, leading to downtime, financial loss, and reputational damage. Lastly, it can compromise sensitive data stored on the network, leading to data breaches and exposure of private information.**
3. **Bypassing copyright media and applications obtained via file sharing or downloading can lead to both legal and reputational consequences. The individuals can face legal charges for violating copyright laws, leading to fines and criminal prosecution. Additionally, it can lead to reputational damage for the individuals, such as loss of credibility, trust, and respect in the industry. Furthermore, the copyright owner may sue the individuals for damages resulting from copyright infringement, leading to civil lawsuits.**

7.2.5 Unethical behaviour from technicians

UNETHICAL BEHAVIOUR	IMPACT ANALYSIS
Unauthorized Access	**An unethical behavior by a cyber security technician could be to access confidential data or networks without permission. This could have a severe impact on overall network and data security as it could lead to data theft, unauthorized modification or deletion of data, and exposure of sensitive information to unauthorized individuals. Such unethical behavior could also compromise the integrity and confidentiality of the data, leading to legal and financial repercussions.**
Neglecting Security Patches	**Another unethical behavior is to neglect security patches that are critical for the security of the system. This could lead to vulnerabilities in the system that can be exploited by hackers, resulting in data breaches, theft, or even complete loss of data. Neglecting security patches could also have a severe impact on the overall network and data security, as it could leave the system exposed to various forms of cyber attacks.**
Selling Sensitive Information	**An unethical behavior by a cyber security technician could be to sell sensitive information to unauthorized individuals or organizations. This could lead to data breaches, theft, and other forms of cyber attacks that could have a severe impact on the overall network and data security. Selling sensitive information could also compromise the integrity and confidentiality of the data, leading to legal and financial repercussions for the organization.**
Sabotage	**An unethical behavior by a cyber security technician could be to intentionally sabotage the system, either by disabling security measures or by introducing malware or viruses. This could have a severe impact on the overall network and data security, as it could compromise the confidentiality, integrity, and availability of the data. Sabotage could also lead to significant financial and reputational losses for the organization, as well as legal consequences**

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
Google Drive	**Google Drive is a cloud-based file-sharing service that allows users to upload, store and share files. It is suitable for individuals, small businesses and large organizations as it offers a range of features and storage options. It has a user-friendly interface and can be accessed from multiple devices.**	**One of the security risks associated with Google Drive is data breaches, where sensitive information can be accessed by unauthorized users. Another risk is the potential for malware or viruses to be uploaded to the platform. Users must also be cautious of sharing files publicly, as it can lead to data leaks.**
Dropbox	**Dropbox is a popular cloud-based file-sharing service that allows users to store and share files. It is suitable for individuals, small businesses, and large organizations as it offers various features such as file syncing, collaboration tools, and mobile apps.**	**One of the security risks associated with Dropbox is data breaches. Another risk is the potential for sensitive information to be accessed by unauthorized users due to weak passwords or shared links. Additionally, Dropbox's mobile app has been known to have vulnerabilities that can be exploited by hackers.**
WeTransfer	**WeTransfer is a file-sharing service that allows users to send files up to 2GB for free. It is suitable for individuals who need to share large files quickly and easily.**	**One of the security risks associated with WeTransfer is the potential for sensitive information to be accessed by unauthorized users. Another risk is the potential for malware or viruses to be uploaded to the platform. Users must also be cautious of phishing scams, where attackers can use fake WeTransfer emails to trick users into downloading malware or providing login credentials.**

8 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.

To assist the juniors in with transitioning into their new role, the following support measure could be implemented:

1. **Training and development: By providing some training to the juniors, this can help them get a feel for their new role and be able to be on their own sooner.**
2. **Mentoring: By having the Senior technician mentor the new junior ones, they will gain invaluable knowledge about how to work efficiently in the business. This will mean they will feel more comfortable in their roles sooner.**
3. **Regular check-in: Regular checkins and feedback sessions with the juniors can help them feel supported and provide a way for them to ask any questions they have. This will also help the Senior get an idea of any area's needed for improvement.**

If the senior technician implements the recommendations above, the juniors will feel supported and will be able to be left on their own sooner.

Appendix

Appendix A:

Turtle Movers Privacy Policy:

PRIVACY POLICY

DATE	AUTHOR	SUMMARY of CHANGE	APPROVED BY
3rd Oct 2022	George Brown	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 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

d) Contact information
    1) Name and surname
    2) Pickup address
    3) Delivery address
    4) Email address
    5) Phone number
e) Transaction details and history
    1) Bookings
    2) Cancellations and rescheduling
    3) Insurance
    4) Payment method
    5) Refunds
    6) Rewards and loyalty benefits
f) Banking and/or credit details
    1) Details of payment method (For example, Financial institution, account)
g) Correspondence and communication
    1) Emails
    2) Phone messages
    3) 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:

3. process your online removalists bookings and related activities
4. deliver a personalised experience
5. manage internal administrative and taxation processes
6. 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 lodge 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

Appendix B

Turtle Movers Privacy Procedures:

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 resolution of 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 or concerns and negotiating a resolution.
- If more information or investigation is required and the process is delayed, management will maintain 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 resolve all complaints promptly and amicable.

Appendix C:

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.

Appendix D:

Privacy policy for Angelonia Fashion:

PRIVACY POLICY

DATE	AUTHOR	SUMMARY of CHANGE	APPROVED BY
3rd Sept 2022	George Green	Created	Manager

Angelonia Fashion 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 work for our company.
Angelonia's 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 Angelonia Fashion and outlines how we collect, use, retain and disclose personal information gathered to carry out our business activities.

Information we may collect

h) Contact information
    1) Name and surname
    2) Address
    3) Email address
    4) Phone number
i) Transaction details and history
    1) Order details
    2) Payment method
    3) Returns details
    4) Refunds
j) Banking and/or credit details
    1) Details of payment method (For example, Institution, account)
k) Correspondence and communication
    1) Emails
    2) Phone messages
    3) Phone records

How data is collected

We collect data from your online transactions. This includes information on your online purchases and online interactions.

How data is used

We use the data collected from your online transactions to:

7. process your online purchases
8. deliver a personalised experience
9. manage internal administrative and taxation processes
10. support our marketing strategy

We retain your personal information linked to sales 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

We use a system consent receipt each time we intend to disclose your information to third parties. For all other situations, we will disclose your personal information only as permitted by the law.

Cookies

Angelonia Fashion uses cookies on its website. Cookies do not personally identify you but your devices, browsers and navigation pattern on our website. The purpose of the cookies is

to improve your online experience. You can disable cookies on your browser but this may affect the way the website displays.

Marketing information

It is your choice to subscribe to receive marketing communications and information from Angelonia Fashion. You can subscribe and unsubscribe to our marketing emails and SMS messages anytime.

Third-party data collection

If you access a third-party website through our website, the third-party website may collect your personal information. We take no responsibility for third-party websites' privacy policies or lack of policies.

Concerns and complaints

To lodge a complaint against this policy download the complaint form from our website and follow the lodge instructions. All complaints are addressed promptly and professionally. Contact us if you have any questions or concerns regarding this policy. Contact details:
Email: angelonia@af.com.au
Phone: 123456789

Appendix E:

Privacy procedures for Angelonia Fashion:

Privacy Policy Distribution and Maintenance Procedure

Purpose: This procedure outlines the actions that Angelonia Fashion takes to ensure the distribution and maintenance of the company's Privacy Policy.

Scope: All employees of Angelonia Fashion

Responsibilities:

The responsibility for distributing and maintaining the Privacy Policy over time rests with management.

Distribution options:

- All employees of Angelonia Fashion are made aware of the Privacy Policy when first joining the company during the induction or orientation process.
- After the induction session is completed, all new employees are emailed the Privacy Policy and are invited to raise any questions or concerns.
- All employees are provided with ongoing privacy training and support through refresher programs every twelve months and issued with a completion certificate.
- Employees can access the Privacy Policy on the company intranet and also on the company website.
- Angelonia Fashion's clients can access the Privacy Policy through the company website. They are encouraged to raise questions or concerns with management via email.

Maintenance options

Policy scheduled reviews:

- The Privacy Policy is reviewed every twelve months and updated before a new round of refresher privacy training takes place.
- After a policy review:
  - A notification email is sent to all employees including the policy or a link to it.
  - The website is updated to include the newly updated policy

- Privacy refresher training sessions are scheduled

What can trigger an unscheduled review?

- A change in privacy legislation will result in a policy review to ensure compliance with legislation.
- Once the policy is updated in accordance with the new legislation the steps outlined in the “After a policy review” in the Review section will take place.
- Another event that can trigger an out-of-scope review is an unusual increase in the number of complaints against the policy from employees and clients. This will trigger a review and subsequent update of the policy.
- Once the policy is updated in accordance with the new legislation the steps outlined in the “After a policy review” in the Review section will take place.

Appendix F:

Privacy Practices for Angelonia Fashion:
Angelonia Fashion has in place a number of practices to ensure that employees adhere to company policy and offer the best possible service to customers. This document outlines the privacy and handling of customer query practices.

Privacy practices:

- Secure password policy.
- Identify and classify sensitive data.
- Encrypt sensitive data.
- Control access to sensitive data.
- Minimal data collection. Collect only the data required to carry out the transaction.
- Use a system of consent receipt. The customer receives a consent receipt each time they content to process personal data and can keep the receipt as proof.
- Implement a robust data security system.
- Compulsory privacy training and awareness of all employees

Practices to handle customer queries:

7. Timely handling of refunds and faulty products (garments)
8. 24-hour response to customer queries regarding products and delivery arrangements
9. Do not assume all customers want the same thing.
10. Adapt to customer communication style. If appropriate use your customer’s language.
11. Know the ropes. Customers need to be reassured that the person they are talking to knows the system.
12. Honesty is the best communication policy.
13. Avoid close-ended responses when dealing with clients as they can block communication.
14. Keep calm and professional at all times.
15. The priority is to address and resolve the customer's issue.