**Legislation and Policies Report Template**

Created by

**UPTOWN IT**

For

**<<** **Turtle Movers >>**

**PROJECT REFERENCE: 474807620**

**DATE:27/09/2024**

**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 analyse over privacy policy of Angelonia fashion based on the details and documents provided. Performed analyse on privacy, policy and procedures was a necessary step to be taken for this organization as we found that they are now enforcing basic facilities and policies meanwhile they are operating both nationally around Australia and overseas. Moreover, after reviewing both relevant Australian and international law and regulations to their operation, we believed that it is beneficiary to briefly describe upcoming reforms in privacy legislation and possible manners in which this organization will benefit from it. Furthermore, we researched and analyse this organization’s operation which allowed us to identify international cyber security legislation in order to evaluate their impact on their data security. From GDPR to Budapest convention (which had relevant sections regarding handling data securely) was found to be necessary to be adhered, enabling us to come an overview of how their international operation will be affected by these legislatives. Next, we classified International cyber security legislation and their impact on data security by those business areas being affected by them. We also narrated how can an interdependency between different legislative instruments of cyber security may happen and we provided an example. Lastly, here we have examined organizations’ policies and procedures (Organization’s ethical practices and procedures were also subject to evaluation.) compliance and suggested a revision to improve them based on the Australian Privacy principles. We ended report by making recommendation as they needed to read and review our suggested techniques and policies if they want to implement them (although we mentioned that they were necessary and need to be used eventually.)

# 2 Introduction

As I started, we started we witnessed an organization who had family-based beginning in the industry. This organization has been growing in shorter span of time compared to others to operate along with most recent technologies. Stakeholders at this organization are concerning about their cyber security and how it is compliant with legislation. Before going further, lets state that Angelonia fashion’s industry is fashion and clothing. They are operating both in Australia and overseas. Moreover, they have got both physical and online operation. At the start they had only 3 employees employed in their organization who seemed to be their family members. They were specialised in garment arrangements and those sold with Australian labels. By now, they have employed 40 people, distributed across Australia in their branches. Their company now has designed their own fashion label on their creations those are being exported to overseas. The company’s headquarters are located at Southport and Gold Coast, but company’s branches are 7 shops, 2 shops at New South Wales, 2 at Queensland, and 2 at Victoria. When we investigated, we found that they are handling data transactions both online and physical as mentioned above. This data is being collected while receiving an online or in person order or performing a refund. This data can be included the credit card payments or bank transfers with suppliers both in Australia and internationally. Their website is being run by a basic security setup which contains strong password policy, implementing firewall, and conducting regular backup.

# 3 Cyber Security Legislative and Regulatory Review

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SECTOR:** | **Fashion Retail, Garment Arrangements, Fashion Label Creation, Retail and Online Sales** | | | |
| **CYBER SECURITY and Related**  **LEGISLATION** | **SCOPE** | | | **BUSINESS AREAS/ACTIVITIES AFFECTED** |
| Federal | State | Territory |
| Australian Cyber Security Centre (ACSC) Guidelines |  |  |  | Their employees and their interactions with insiders and outside actors. Their fashion label in the way being protected, shared, used and get printed, the data of their customers and their deliveries both in Australia and overseas. Their operations in headquarters and branches. Practices during online and physical sales, practices during refunding, details of purchases from suppliers both nationally and internationally, the password policy, the firewall usage, and backup processes. |
| Privacy Act 1988 |  |  |  | The data collected from customers after sales, refunds and also data shared with suppliers or received from them. Data stored or in transfer between employees in headquarters and branches. |
| Spam Act 2003 |  |  |  | Online marketing and communication practices happening in this organization, this act regulates those advertisements undergone across all states and territory in Australia. |
| Information Privacy Act 2009 (QLD) |  |  |  | Personal information of staffs, customers, and other actors stored from physical and online sales in Queensland. This can be also staffs’ employment details stored when they applied for the role. |
| Privacy and Personal Information Protection Act 1998 (NSW) |  |  |  | Personal information of staffs, customers, and other actors stored from physical and online sales in New south Wales. This can be also staffs’ employment details stored when they applied for the role. |
| Privacy and Data Protection Act 2014 (VIC) |  |  |  | Personal information of staffs, customers, and other actors stored from physical and online sales in New south Wales. This can be also staffs’ employment details stored when they applied for the role. |
| Telecommunications (Interception & Access) Act 1979 |  |  |  | First of all, it has got impacts on the how service is being delivered and how it can be directly or indirectly accessed by customers. Then after a search, as they have got 7 shops, each having internal and also external telephone connections and they and their stuffs need to use this technology and safeguard themselves and also the customers while using it by obeying this regulation. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| The **Criminal Code Act 1995** |  |  |  | Interactions happening between Owner and stakeholder, interactions between manager and staffs, interactions happening among staffs, interactions between staffs and external actors, the manner company or staffs handling orders are all areas where can be under this law to protect their interactions and keep them out of criminal approaches to them. |
| **Corporations Act 2001 (Cth)** |  |  |  | Risks organization face need to be handled based on this Act, the incidents happening need to be handled and reported based on this act, the data and its protection is also followed in this act. |
| **Prudential Standard CPS 234** |  |  |  | The framework being used for security of this organization needs to be aligned with this standard. Risk and incident management need to be performed based on this standard. Sometimes this organization needs to have knowledge of third-parties service providers and how do they comply with this standard. The approaches for identifying and classifying information assets, and then managing them in order to protect them. |
| Australian Competition and Consumer Commission (ACCC) |  |  |  | Customer right and the guarantees given to them has been controlled in this law, the manner for advertising and marketing has been regulated, some product safety also has been considered in this law, the online sales of the organization need to be operate based on this law, contract terms need to be design based on this law. |

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

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

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

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

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

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

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

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

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

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

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

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

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>.

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

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

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

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

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

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

Yellow ones are for first organization.

|  |  |  |
| --- | --- | --- |
| 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

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

# 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>.

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

1. Metasploit Framework

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

1. Nmap

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

1. Wireshark

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

1. Burp Suite

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

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

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

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

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

1. Splunk:

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

1. Snort

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

1. Wireshark:

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

1. Nessus:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Unauthorized Data Access

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

1. Installing Backdoors

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

1. Manipulating Logs and Audit Trails

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

1. Sharing Confidential Information

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

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

|  |  |  |
| --- | --- | --- |
| **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

To conclude, I highlighted Angelonia Fashion's compliance progress with Australian cyber security laws as they are always expanding their operations around the country. While their privacy policy seems to be updated and meets current standards, I found that there is a need to enhance it as they are expanding their operations. They need to assure about long term security, we suggested the organization to establish response plans, try conducting monthly basis audits, and further implement data minimization practices to ensure that they are only retaining necessary information. In addition, they can boost their data protection ability by adopting advanced encryption methods and also enforcing a password policy. Lastly, as I discussed new reforms in privacy and consumer legislation shared with us, Angelonia Fashion is required to adapt their policies to avoid any possible challenges associated with compliance. Using this approach, they will be able to both protect customer data and also enhance their reputation in the industry and between cutomers.

# Appendix

## Organisation policies, procedures and best practices documentation

**POLICES 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 who 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**

Contact information

Name and surname

Address

Email address

Phone number

Transaction details and history

Order details

Payment method

Returns details

Refunds

Banking and/or credit details

Details of payment method (For example, institution, account)

Correspondence and communication

Emails

Phone messages

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:

process your online purchases

deliver a personalised experience

manage internal administrative and taxation processes

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 patterns 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 at any time.

**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 lodgement 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

**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 are 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 “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.

**ORGANISATIONAL 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 receipts. The customer receives a consent receipt each time they consent to processing 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:**

Timely handling of refunds and faulty products (garments).

24-hour response to customer queries regarding products and delivery arrangements.

Do not assume all customers want the same thing.

Adapt to customer communication styles. If appropriate, use your customer’s language.

Know the ropes. Customers need to be reassured that the person they are talking to knows the system.

Honesty is the best communication policy.

Avoid close-ended responses when dealing with clients, as they can block communication.

Keep calm and professional at all times.

The priority is to address and resolve the customer's issue.