Workplace Information Handling Procedures Worksheet

Step 1:

List all personally identifiable information your organisation collects.

As you list each piece of PII, consider whether it is actually necessary to collect and hold that PII in order to carry out your functions and activities. (Over-collection can increase risks for the security of personal information).

|  |  |
| --- | --- |
| Business Use | PII Collected |
| e-mail mailing list | e-mail address |
| Proof of purchase | Receipt information |
| Contact to buyer | Phone Number |
| To send items | Address |
| So you can charge the buyer | Card details |
| To see if they are old enough to purchase | Age |

Step 2:

For each piece of PII collected, plan how the PII will be handled.

List how the PII will be stored and who will have access to it.

Consider how privacy protections can be embedded into the handling process, or how existing privacy protections could be strengthened.

|  |  |
| --- | --- |
| PII Collected | Handling Process |
| e-mail address | e-mail addresses collected via web form and automatically stored in Mailchimp database Mailchimp password known only by marketing staff |
| Receipt information | Receipt information will be stored through the company’s income system and managed by salesperson/accountant |
| Phone Number | The AmeriList Cell Phone Database is derived from a multitude of online paths. Data is pulled from the sources using the wireless NPA/NXX blocks |
| Address | Address info will be stored with warehouse workers so they can load your order |
| Card details | The staff involving marketing will hold your info and store it in |
| Age |  |

Step 3:

Assess the PII security risks by conducting a privacy impact assessment. This can be done by completing *Privacy Impact Assessment Worksheet*. Return to complete this step after you have completed the privacy impact assessment.

Once you have identified the security risks, review your information security controls to determine if they are adequate in mitigating the risks.

|  |  |  |
| --- | --- | --- |
| PII Collected | Security Risks | Security Controls |
| e-mail address | Unauthorised access by internal staff | Use a password manager to ensure Mailchimp password only shared with key staff |
| e-mail address | Data breach of Mailchimp site | Use strong password  Change password regularly |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |