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 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 |
| Mailing list | Residential address |
| Paying employees | Bank details |
| Customer accounts | Username and passwords |
| Background checks | Medical history |
|  |  |

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 |
| Residential address | Collected from website and stored in secure database, only accessible by staff sending mail or products to the address. |
| Bank Details | Collected by website or phone, store it securely with encryption. Only Human Resources need access, and an access control system should be in place. |
| Username and passwords | Collected by website, stored on secure servers. Only IT department need to access if there are any issues with customers struggling to access accounts. |
| Medical History | Collected by medical professionals, stored on secure servers. Only needs to be accessed by HR and medical professionals. |
|  |  |

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 |
| Residential address | External hack into company records | Use passwords, 2 factor authentication and encryption |
| Bank Details | External data breach to steal employee’s bank details | Encrypted and implement a access control system to log who can see the PII |
| Username and password | Unauthorised access by internal staff | Request users update password regularly and access control system so only IT department can access |
| Medical History | Unauthorised access to employee medical history | Stored on secure servers, access control system, only Human Resources need to access. |