Data Privacy Risk Assessment

for

***Insert Organization Name***

***Name of System/Product/Service***

**Date**

***Student Name***

**Table of Contents**

[1 System Overview 1](#_Toc94515280)

[2 Data Type, Sources, and Use 1](#_Toc94515281)

[3 Internal Policies and Procedures 3](#_Toc94515282)

[4 Data Access and Sharing 4](#_Toc94515283)

[5 Notice and Consent 5](#_Toc94515284)

[6 Data Accuracy and Security 6](#_Toc94515285)

[7 Data Retention and Disposal 6](#_Toc94515286)

[8 Website Privacy Evaluation 7](#_Toc94515287)

[9 Privacy Risks and Evaluation 7](#_Toc94515288)

[10 Questions and Assumptions 8](#_Toc94515289)

[*Update the following table to document and track changes made to the PIA. Clear all blue text in table before use*.]

| **Version Number** | **Version Date** | **Author/Owner** | **A=Add, M=Modify, D=Delete** | **Description of Change** | **Substantive Change**  **[Y/N]** |
| --- | --- | --- | --- | --- | --- |
| **1.0** | **07/10/2023** | **Carlos Fernando Chicata** | **N/A** | **Initial report.** | **N/A** |
|  |  |  |  |  |  |

Note: This Privacy Impact Assessment template is based on those published by the US Federal Trade Commission (FTC) at <https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments> and as such should be considered a public document.

# System Overview

* 1. **Organization Name and description**

Agarwal, Becker, and Cooper (ABC) PC, a Certified Public Accounting firm, has been providing financial guidance to individuals and businesses

* 1. **System, Product or Service Name**

*Provide the name of the system, produce or service under assessment.*

* 1. **Describe the system/product/service and its purpose.**

*Provide a written description of the system, product or service under review.*

* 1. **List responsible parties associated with the system/product/service.**

*List the roles, names and contact details for the organization members with privacy responsibilities. This is the person responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system. Add more rows as needed.*

|  |  |  |
| --- | --- | --- |
| Role / Responsibility | Name | Contact (Email, Phone, etc.) |
|  |  |  |
|  |  |  |

# Data Type, Sources, and Use

**2.1 Specify the types of personally identifiable information (PII)[[1]](#footnote-1)** **that are or may be collected, stored, shared, or maintained in the system/product/service.**

*List PII types.*

**2.2** **What types of information other than PII will be collected, stored, shared, or maintained by the system/product/service? Provide a general description below and be sure to include all data elements.**

*List and describe related non-PII information.*

**2.3 What is the purpose for collection of the information listed above?**

*Describe the organization’s purpose(s) for the collection of individual information.*

**2.4 What are the source(s) of the information in the system/product/service? How is the information collected?**

*List and describe the source of individual information as it relates to the system, product, or service under review. Include the data type, classification and method for collection.*

|  |  |
| --- | --- |
| ***Source of Data*** | ***Type of Data Provided & How It Is Collected*** |
|  |  |
|  |  |

**2.5 What specific legal authority allows for the collection, maintenance, or dissemination of information for this system/product/service?**

*List legal authorities for the use of individual information. This includes any applicable laws, regulations or standards, and any third-party or supplier contracts.   
See* [*https://iapp.org/resources/article/us-state-privacy-legislation-tracker/*](https://iapp.org/resources/article/us-state-privacy-legislation-tracker/) *for US Laws and Data Protection Laws of the World,* [*https://www.dlapiperdataprotection.com/*](https://www.dlapiperdataprotection.com/)*.*

**Applicable Laws & Regulations:**

| **ID #** | **Title** | **Date** | **Link** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

**Contracts:**

| **ID #** | **Contract Source** | **Date** | **Organizational Contact** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Not Applicable.

# Internal Policies and Procedures

**3.1 Specify the relevant organizational policies in place related to data privacy within this system/product/service.**    
**Have policies and/or procedures been established for this responsibility and accountability?  Yes  No**

*Complete the table below.*

|  |  |  |
| --- | --- | --- |
| ***Policy Name*** | ***Implementation Date*** | ***Review  Date*** |
|  |  |  |
|  |  |  |

**3.2 Specify the relevant organizational procedures in place related to data privacy within this system/product/service.**

*List any published organizational processes or procedures.*

**3.3 Specify relevant security or privacy training provided to organizational employees or contractors with PI access.**

# Data Access and Sharing

**4.1 In the table below, specify the systems/applications and groups that will have access to or share data in the system/product/service.**

|  |  |
| --- | --- |
| ***Data Will Be Accessed By and/or Provided To:*** | ***How and Why the Data Will Be Accessed/Shared*** |
|  |  |
|  |  |
|  |  |

**4.2 Complete if a Cloud Service Provider is used for this system/product/service.**

*Cloud Service Providers (CSPs) perform an annual analysis to determine if PII is collected by any of the system components. Clouds that do not collect PII and would like to opt-out of hosting privacy information may elect to do so and are not required to fill out the Privacy Impact Assessment Questions. If a CSP is willing to host PII, the Privacy Impact Assessment Questions should be answered given the current knowledge of the CSP. A CSP is not required to solicit customers for the information.*

Check one.

|  |  |
| --- | --- |
|  | Cloud Service Provider not in use. |
|  | Opt-out. This cloud will not host privacy information. |
|  | This cloud is willing to host privacy information.  Select the cloud layers that are represented by <System Name>. Select all that apply. |
|  | This cloud includes Software as a Service (SaaS). |
|  | This cloud includes Platform as a Service (PaaS). |
|  | This cloud includes Infrastructure as a Service (IaaS). |

The Cloud Service Provider used for this service has the following certifications:

|  |  |
| --- | --- |
|  | FedRAMP |
|  | SOC2 |
|  | HITRUST |
|  | Other - List |

**4.3 Do contractors and/or third-party service providers have access to data in the system/product/service? If yes, explain what privacy requirements are in place to ensure that data is properly protected.**

Not Applicable.

**4.4 If you answered “yes” to 4.3, describe the privacy incident response plan maintained by the contractor’s organization or third-party service provider.**

Not Applicable.

# Notice and Consent

**5.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.**

*Describe the notification method(s) provided to individual prior to the collection of their PII within this system/product/service.*

Notice is provided via (*check all that apply*):

Privacy Act Statement ( Written  Oral)

Website Privacy Policy

Privacy Notice (e.g., on Social Media platforms)

Login banner

Other (*explain*): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Notice is not provided (explain): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**5.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?** **Explain applicable processes.**

**5.3 Are there procedures in place to allow individuals access to their personally identifiable information contained within this system? Explain.**

**5.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.**

# Data Accuracy and Security

**6.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?**

**6.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/product/service? What controls are in place to ensure proper use of the data? Please specify.**

**6.3 Is PII used in the course of system testing, training, or research within this system/product/service? If so, what steps are taken to minimize and protect PII during this process?**

.

Not Applicable

# Data Retention and Disposal

**7.1 Specify the period of time that data is retained in the system/product/service. Include any relevant policies or regulations regarding records.**

**7.2 What are the specific procedures for disposing of the data at the end of the retention period?**

# Website Privacy Evaluation

**8.1 Does the organization have a Privacy Policy published on their Internet-facing / external website?   
If so, provide the publication date:**

Yes, Date Published: Click or tap to enter a date. No

**8.1 Does the system/product/service employ the use of a website? If so, describe any tracking technology used** **by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.**

Not Applicable

# Privacy Risks and Evaluation

**9.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated? If the mitigation strategy is not in place, include proposed methods.**

*Focus on significant privacy risks associated with the in-scope systems. Security risks may be included if they directly relate to the real or potential compromise of the confidentiality or integrity of PI. Complete the Likelihood (L), Impact (I), and overall Risk Rating (RR) values based on the perceived risks and information provided.   
Include an explanation of the risk along with the current or proposed mitigation strategy to address the risk. NOTE: This information should be documented in the organization’s risk register. It is provided here for reporting purposes.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Risk Description*** | ***L*** | ***I*** | ***RR*** | ***Explanation & Mitigation Strategy*** |
| Misuse of data by authorized users |  |  |  |  |
| Unauthorized system access |  |  |  |  |
| Data leakage |  |  |  |  |
|  |  |  |  |  |

L = Likelihood of Risk, Scale 1-5 (1-Low, 5-High)

I = Impact of Risk, Scale 1-5 (1-Low, 5-High)

RR = Risk Rating, Overall risk, Scale 1-5 (1-Low, 5-High)

**9.2 Does the system/product/service employ the use of automated privacy controls, security protections, or enhanced capabilities designed to support privacy? Explain.**

**9.3 How does the system/product/service ensure that the information is collected, used, stored, or disseminated in accordance** **with regulations, standards, and stated corporate practices?**

**9.4 Provide recommendations in priority order to overcome *privacy* risks listed above.**

*List your recommendations to address privacy risks.*

# Questions and Assumptions

**10.1 List any questions you would ask the client and/or any assumptions you made in completing this report.**

1. Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. [↑](#footnote-ref-1)