Data Privacy Risk Assessment

for

***Agarwal, Becker and Cooper PC***

***Microsoft 365 Business Premium***

**07/10/2023**

***Carlos Fernando Chicata Farfan***

**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**

The evaluation is about Microsoft 365 business premium service to work with clients and staff.

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

The products that company will evaluate:

* Outlook: service of email.
* Excel: service of spreadsheet management.
* Word: service of document management.
* OneDrive: service of cloud storage.
* Teams: Service of online meeting.
* SharePoint: service to collaboration among users.
* Azure Active Directory: service of identity management.
* Intune: management service to assess and protect apps and devices.
* Server 2019 servers: server to store uploaded files by clients.
  1. **List responsible parties associated with the system/product/service.**

|  |  |  |
| --- | --- | --- |
| Role / Responsibility | Name | Contact (Email, Phone, etc.) |
| IT Analysts | N/A | N/A |
| System/Network/App administrator | N/A | N/A |
| Data Protection Officer | Tracy Bingham | N/A |
| Information Security Officer | Thomas Brooks | N/A |
| Tax/Finance accountants | N/A | N/A |

# 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.*

* Full name (first and last names).
* Photographic facial image.
* License number(s).
* Social security or employer identification number.
* Email address(es).
* Phone number(s).
* Driver’s license number.
* Passport number.
* Background check information.
* Account number.
* Website(s).
* Demographic information.
* Voice recording(s)

**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.*

* Tax information.
* Payment information: ACH and credit card(s)
* Account receivable/payable
* Job history
* Education history
* Income sources
* Expenses
* Health plan information

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

We collect all of information to work in our financial services like tax management, accounting service, financial statements audits, preparation of financial statement or consulting and financial planning.

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

|  |  |
| --- | --- |
| ***Source of Data*** | ***Type of Data Provided & How It Is Collected*** |
| Financial Management Systems | The clients upload their financial informations like file. Tax and payment information are uploaded. All information is classified like confidential. |
| Hosted website | First and last name, phone number, email, demographic information and so on. This information is uploading by forms to contact the client. All information is classified like confidential. |

**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** |
| --- | --- | --- | --- |
| **1** | NIST security framework | 01/01/2021 | https://www.nist.gov/cyberframework |
| **2** | AICPA | N/A | https://us.aicpa.org/forthepublic |

**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**

|  |  |  |
| --- | --- | --- |
| ***Policy Name*** | ***Implementation Date*** | ***Review  Date*** |
| Information Security and Acceptable Use policy | 01/01/2021 | 01/01/2021 |
| Data Classification and Protection policy | 01/01/2018 | 30/06/2020 |
| Privacy policy | N/A | 30/09/2020 |
| Data retention policy | N/A | N/A |

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

* Incident response and disaster recovery procedure.
* System and data destruction procedures.
* Individual access to PI procedures.
* Employee onboarding and termination procedures.

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

* Annual security and privacy training for employees and contractors.
* Training about security and privacy for contractors previously to sign in ABC.

# 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*** |
| SharePoint | The tax and financial records are accessing and sharing by SharePoint for clients and business analysts or accountants to work and get status of progress. The staff need the authorization to access these information. |
| OneDrive | The tax and financial records are accessing and sharing by OneDrive for clients and business analysts or accountants to work and get status of progress. The staff need the authorization to access this information. |
|  |  |

**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 Microsoft 365 premium. 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.**

Yes, all contractors are subject to background investigations and suitability reviews in accordance with HR policies and procedures; and also apply them the principle of least privilege to access data. Previous to access the data, they need to complete the security and privacy training.

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.**

The contractors must follow the ABC’s Incident Response Plan. The documentations don’t describe this plan.

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.**

They notify the data collection in contracting process of service in regular activities; and irregular occasions they will provide notice in website privacy policy.

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.**

The service isn’t use to collect personal identity information directly; so the clients have the responsibility don’t share their personal information; and we notify it to them.

They ensure any PII is scrubbed or de-identified prior to use in testing or training case.

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

Yes, they may request access to their personal identity information through their account manager.

**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.**

No; this procedure doesn’t mention in documentations.

# Data Accuracy and Security

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

No, they don’t collect data using Microsoft 365 directly; so the accurate, complete and up-to-date data depend how work for clients.

**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.**

Yes, they implement identity access management guided by the principle of least privilege, monitor system and audit logs; in technical focus. The system administrator uses these methods to protect service and system. The ABC contractors and staff are subject to background investigations and suitability reviews by HR.

**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?**

They ensure any PII is scrubbed or de-identified to use in testing or training cases. They don’t use Microsoft 365 for testing, training or research cases.

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.**

The retention periods for kind of data is documented in Data Retention Schedules.

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

The responsibility of employees destroys all data based in retention schedule in case of local non-cloud storage owned of employees. Microsoft 365 delete the data based in give retention schedule in cloud storage cases.

# 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: 9/30/2020 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.**

Yes, the website is use to show company information, blog of capacitation of users, form for contacting clients and contact information. Website doesn’t use to collect personal data from clients; and documentations doesn’t mention about tracking technology in this platform.

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 | 5 | 5 | 5 | All users must agree to the AAA’s acceptable use policy. Monitoring actions of users by logs. Generate monthly auditory for employees in their activities. |
| Unauthorized system access | 2 | 5 | 3 | All employees need to have authentication process (Active directory) to access data and infrastructure by AAA account. By default, all users have denied access to data storage from computers. Implement and review the principle of least privileges in access control. |
| Data leakage | 2 | 5 | 3 | Monitoring of data access from employees and contractors in network. Log of activities in infrastructure to monitoring the employees actions. |
|  |  |  |  |  |

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.**

Yes, they use encryption, authentication method with passwords, audit logs, firewalls, malware identification and data loss prevention policies to control the privacy in Microsoft 365.

**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?**

Microsoft meets the following standards: FedRAMP, ISO 27701 and 27001, GDPR and so on.

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

*List your recommendations to address privacy risks.*

1. Implement the NIST privacy framework.
2. Testing and training about Incident response plan.
3. Research and implement a best way to get access in case of temporary workers.
4. Automatization of alerts in logs of activities.

# 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)