For more information about the PIA report, or doing the associated PIA, contact:

Rebecca Herold
rebeccaherold@rebeccaherold.com
www.privacyguidance.com
www.compliancehelper.com

<Name>
Privacy Impact Assessment
Full Report

[CLIENT LOGO]

Prepared by Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI
<date>

Table of Contents

Executive Summary

<Intro/background>

1. **Company information security and privacy administration**	Findings summary
2. **Corporate leadership**	Findings summary
3. **Data collection and processing**	Findings summary
4. **Data retention**	Findings summary
5. **Openness and transparency**	Findings summary
6. **Responsiveness**	Findings summary
7. **Hardware and software physical security**	Findings summary
8. **Customer control**	Findings summary
9. **Consent and opt-in/opt-out controls**	Findings summary
10. **Privacy Enhancing Practices & Technology**	Findings summary
11. **Privacy Invading Practices & Technology**	Findings summary
Assessment & Justification	Findings summary

LEGEND:

- **Green:** **Privacy-friendly and privacy enhancing**
- **Blue:** **Generally privacy aware but could be improved upon**
- **Yellow:** **Generally aware of privacy issues and requirements, but notable lapses exist**
- **Red:** **Substantial and comprehensive privacy threats**
- **Black:** **Significant lack of security for PII**

Table 1 – <Company X>PIA summary

<Company X>PIA Report

<Intro/background>

A. Summary of PIA Findings

<Info>

B. Purpose of a PIA

<Info>

C. <Company X><PIA scope> Description

<Description>

Data Item	Data Item Description
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	

Table 2 – Data Within <Company X><PIA scope> Processing

<Add additional details, flow diagrams, tables, illustrations, etc. describing the PIA scope here>

D. GAPP Alignment

1. Management, Accountability & Training

<Put findings here>

Information Security and Privacy Training and Awareness Practices

<Put findings here>

2. Notice & Purpose for PII Use

<Put findings here>

3. Choice & Consent to use PII

<Put findings here>

4. Collection of PII

<Put findings here>

5. Use and Retention of PII

<Put findings here>

6. Individual access

<Put findings here>

7. Disclosure and Limiting Use of PII

<Put findings here>

8. Security and Safeguards

<Put findings here>

9. Accuracy & Quality of PII

<Put findings here>

10. Openness, Monitoring & Challenging Compliance

<Put findings here>

E. PCI DSS Compliance <Include section only if applicable>

<Put findings here>

F. HIPAA/HITECH Compliance <Include section only if applicable>

<Put findings here>

G. <Put regulation/standard/etc. as applicable > <Include section only if applicable>

<Put findings here>

Work Papers

<Background info>

The recommendations include:

<Put recommendations here>

NOTE: This report is not, and should not be construed as, a legal opinion.

1. Project Scope

<Description>

2. <Company X><PIA scope> process

Figure 1 shows the <Company X>online <Company X><PIA scope> process.

<Put diagram here>

Figure 1 – <Company X><PIA scope> processing

Personally Identifiable Information (PII)

<Description>

Data Item	Data Item Description
14.	
15.	
16.	
17.	
18.	
19.	
20.	
21.	
22.	
23.	
24.	
25.	
26.	

Figure 2 – Data Within <Company X><PIA scope> Processing

Areas of concern

<fill in>

Recommendations

<fill in>

3. Privacy Complaints and Incidents

<Put description of review and work here>.

Areas of concern
<fill in>

Recommendations
<fill in>

4. Privacy Policies and Practices

<Description>

4.1 Website Privacy Policies

<Put description of work and review here>

Areas of concern

<fill in>

Recommendations
<fill in>

4.2 Internal Information Security and Privacy Policies

<Describe importance of policies and procedures here>

<Describe work, research and findings here>

Areas of concern
<fill in>

Recommendations
<fill in>

5. Privacy Programs and Executive Support

<Company X> <provide applicable information here>

Areas of concern
<fill in>

Recommendations
<fill in>

6. Awareness and Training

<Company X> <provide applicable information here>

Areas of concern
<fill in>

Recommendations
<fill in>

7. PII Collection and Access

<Background>

7.1 Customer PII Collection

Customer PII is collected within **<Company X>**through the **<Company X><PIA scope>**.

- The **<Company X><PIA scope>** **<provide applicable information here>** The data items are listed in Table 2. PII items are highlighted in green. Information that, when coupled with a PII item, becomes sensitive are highlighted in yellow.

Data Item	Data Item Description
1.	
2.	
3.	
4.	
5.	

6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	

Table 2 – Data Within <Company X><PIA scope> Processing

<Illustrations> **<Company X><PIA scope>** looks on a website.

<Include diagrams, illustrations, screen prints, etc. as appropriate to the PIA scope.>

<Describe all types of PII collection activities here>

Areas of concern
<fill in>

Recommendations

<fill in>

7.2 Use Limitation & Sharing Customer PII With Third Parties

<Background>

<Describe PII sharing practices here>

Areas of concern

<fill in>

Recommendations

<fill in>

7.3 Purpose Specification

<Describe how purposes for PII use are, or are not, provided>

Areas of concern

<fill in>

Recommendations

<fill in>

7.4 Individual Participation

<Describe how individuals can access their own PII>

Areas of concern

<fill in>

Recommendations

<fill in>

8. Customer PII Storage

<Describe PII storage practices and locations>

Areas of concern
<fill in>

Recommendations
<fill in>

9. Laws, Regulations and Contracts

<include an description and appropriate list>

Areas of concern

<fill in>

Recommendations

<fill in>

10. Contractual Obligations

<Description>

Areas of concern

<fill in>

Recommendations

<fill in>

11. Background checks

<Description>

Areas of concern

<fill in>

Recommendations

<fill in>

12. Safeguards & Data Integrity

<Company X>has <**include information here as appropriate>**

Areas of concern

<fill in>

Recommendations

<fill in>

13. Data Quality

The **<Company X><PIA scope>** **<include information here as appropriate>**

Areas of concern
<fill in>

Recommendations

<fill in>

14. Customer PII Used for Test Purposes

Currently production **<Company X>**customer PII is **<provide details as applicable here>**

Areas of concern

<fill in>

Recommendations

<fill in>

15. Limiting access within applications and systems

<Company X>controls access to customer PII through **<provide applicable details here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16. Oversight, Maintenance & Evaluation

16.1 Accountability

The **<Company X>** **<provide applicable details here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16.2 Openness

<Company X>has **<provide applicable details here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16.3 Customer PII Retention

<Company X> **<provide applicable details here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16.4 Customer PII Disposal

The **<Company X>** **<include applicable information here>**

Areas of concern

<fill in>

Recommendations

<fill in>

16.5 Compliance and enforcement

<Company X> **<include applicable information here>**

Areas of concern

<fill in>

Recommendations

<fill in>

Appendix A – <Company X>Privacy Survey Responses

<Put verbatim copies of completed PIA surveys here>

Appendix B – Existing <Company X>Information Security and Privacy Policies

<Fill in as appropriate>

Appendix C – Recommended Information Security and Privacy Policies & Supporting Documents

<Fill in as appropriate>

Appendix D – <Company X>PIA Project Meeting Notes

<Copy all PIA meeting notes here>

Appendix E –U.S. State Breach Notice Laws

Appendix F – <Company X>Website Privacy Policies

<Copy here verbatim>

Appendix G - Data Protection (Privacy) Laws

<Describe applicable laws here>

Appendix H - <Company X>Information Security and Privacy Training and Awareness Program

<Fill in as appropriate>

Appendix I - Recommended <Company X>Website Privacy Policy

<Fill in appropriately>

Appendix J - Updated <Company X>Website Privacy Policy

<Fill in as applicable>

Appendix K – <Change to PIA Specific Issue>

Appendix L – <Change to PIA Specific Issue>

Appendix M – Updated <Company X>Security Policies

<Change appropriately>