A Data Risk Assessment addresses security, privacy, and legal risks posed to the University. A Data Risk Assessment is required for Stanford projects that involve any of the following:

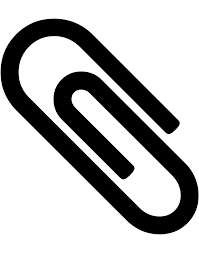
* High Risk or Moderate Risk Data
* Use of solutions other than [Stanford Approved Services](file:///C:\Users\pparsi\AppData\Local\Box\Box%20Edit\Documents\37048566526\dataclass.stanford.edu)
* Involvement of a new entity that will handle Moderate or High Risk Stanford Data

HOW TO INITIATE A DATA RISK ASSESSMENT:



1. Review the [**Stanford Risk Classifications**](https://itservices.stanford.edu/guide/riskclassifications) and the [**Data Risk Assessment process**](https://uit.stanford.edu/security/jsplr) before completing the intake form.
2. Complete the intake form as follows:
   * Sections A and B must be completed by a Stanford individual who has full programmatic knowledge of the project. Questions about these sections should be sent to [privacy@stanford.edu](mailto:privacy@stanford.edu).
   * Section C will require consultation with information security and the technical staff involved in the project who will administer the systems. This section may require detailed technical information from your outside collaborator(s). ***Provide the form to them as soon as possible to allow sufficient time for completion.*** Questions about this section should be sent to [iso-consulting@lists.stanford.edu](mailto:iso-consulting@lists.stanford.edu).
   * Completely answer ALL questions and specify “N/A” if a question does not apply to your project. Leaving any questions unanswered may delay the review process.



1. Once your intake form is completed and you have gathered all supporting documents, file a ServiceNow ticket as follows:
   * Log into stanford.service-now.com and select ‘Information Technology’.
   * Select ‘Request Something’, category “Security and Compliance,” and Request Type ‘Privacy and Security Review – General Request’.
2. Attach your completed intake form, data flow diagram, related agreements and, if applicable, your IRB application to the ServiceNow ticket. ***Review may be delayed if these documents are not attached. An application is considered complete only when the form is complete and all documents are attached.***

AFTER YOU SUBMIT YOUR COMPLETED APPLICATION:

After receiving your intake form and all supporting documents, your information will be reviewed. If more information or clarification is needed, your technical and programmatic staff and those of your collaborator(s) may be scheduled for a meeting. A report will be issued with recommendations for addressing the risks posed by the project.

QUESTIONS:

General questions about the form or process can be directed to [privacy@stanford.edu](mailto:privacy@stanford.edu). Thank you, and we look forward to collaborating with you on this project.

|  |  |
| --- | --- |
| **STANFORD APPLICANT** | |
| SUBMITTER NAME AND TITLE  Jimmy Jones, Program Manager | |
| **IF NOT SAME AS ABOVE,** PROJECT LEAD NAME AND TITLE | |
| DEPARTMENT  RD&E | |
| PHONE NUMBER  650-555-5555 | EMAIL  jj@stanford.edu |
| PROJECT TITLE  Gimmie | |
| TYPE OF PROJECT  Medical/Clinical Care  Student education  Quality improvement/assessment  Research  Fundraising/marketing  University administration/operations  Outsourcing (process, application/service)  Other (describe): | |
| IRB PROTOCOL NUMBER (if applicable)  N/A | |

**Please review Stanford’s** [**Risk Classification Guide**](https://itservices.stanford.edu/guide/riskclassifications) **before answering the next portion.**

1. **INFORMATION ABOUT THE PROJECT**
2. **Overview.**
3. Identify all **non-Stanford** parties involved in the project.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Third party/Organization name** | **Role**  (e.g., vendor, funding sponsor, business associate, subcontractor, collaborator, technical support, etc.) | **Point of Contact** | [**Moderate Risk Data**](https://uit.stanford.edu/guide/riskclassifications)will be transferred to/ received from / accessed by entity | [**High Risk Data**](https://uit.stanford.edu/guide/riskclassifications)  will be transferred to/ received from / accessed by entity |
| Gimmie Inc. | Vendor | Don Donaldson, Gimmie account representative. [dd@gimmie.com](mailto:dd@gimmie.com) | No | Yes |

1. In layperson’s language, briefly summarize the overall project, including what each organization/third party identified above will do in the project.

Gimmie Inc. is a credit card payment vendor considered by Stanford. Gimmie will provide SU with a mobile app that can be used to purchase items where point of sale system is unavailable, such as an outdoor market (similar to Square app). We will use Gimmie at the Stanford gift store to collect payments from customers. Stanford will have an option to pay a fixed subscription fee, or a small fee (~10%) per transaction.

1. What is the target start date for this project or this project phase?

Test phase start – April 2017

Production roll out – July 2017

1. Is this a new project or an enhancement/adjustment to an existing project?

New Enhancement/Adjustment

If enhancement/adjustment, what is being changed?

Technology Vendor Data Other (specify):

1. **Project Funding.**  If this project is externally funded, provide the sponsor name, SPO number, or agreement.

Sponsor Name:

SPO/Agreement #:

Project is not externally funded

1. **Contracts and Other Obligations.** Identify ***and attach*** to your ServiceNow ticket any agreements, obligations or regulatory requirements related to this project, this dataset, or the third parties involved.

No known obligations  Master Agreement

Non-disclosure/Confidentiality Agreement  Umbrella Agreement

Sponsored Research Agreement  Business Associate Agreement (BAA)

Collaborative Agreement  Data Use Agreement

FIPS, FISMA, NIST requirements in contract  Other (explain):

PCI-DSS

1. **Other Involved/Interested Stanford Entities.** Identify any other Stanford entity with whom you have worked or consulted as part of this project.

Office of General Counsel (OGC)  Procurement  Office of Sponsored Research (OSR)

Office of Technology Licensing (OTL)  Office of Development  Office of Risk Management

Industrial Contracts Office (ICO)  Registrar  SoM Information Resources & Technology

Global Services/International Affairs  Stanford Hospital/Clinic  Institutional Review Board (IRB)

Other Stanford schools or units:

SU PCI team

Provide the point(s) of contact for the office(s) selected above.

Corrina – SU PCI team, Alice - Procurement

1. **INFORMATION ABOUT THE DATA INVOLVED IN PROJECT**
2. **Data Owner is:** Stanford Stanford Hospital/Clinic  Other (specify): ­­­­
3. a) **Will Non-Stanford parties access Stanford Data?** Yes No

IF yes, how?

Paper  Thumb-drive/hard drive

Web portal / Server access (non-SUNet credentials) View-only

Web portal / Server access (sponsored SUNet credentials)  Download

Other:

PCI data is transmitted over TLS

b) **Will Stanford individuals access non-Stanford data?** Yes No

IF yes, how?

Paper  Thumb-drive/hard drive

Web portal / Server access (non-SUNet credentials) View-only

Web portal / Server access (SUNet credentials)  Download

Other:

1. **Data Elements involved in any part of the project**. Select all that apply and explain, where necessary. Attach a data dictionary, if available.

Full names (students, alumni)

Full names (patients, research subjects)

Full names (employees)

Full names (all others)

Geographic subdivisions smaller than a state

Dates (except year) directly related to an individual

Telephone numbers

Fax numbers

E-mail addresses

Social Security numbers

Medical record numbers

Health plan beneficiary numbers

Account numbers (e.g., medical or insurance)

Certificate/license numbers

Vehicle identifiers and serial numbers, including license plate numbers

Device identifiers and serial numbers

Web URLs

IP address numbers

Biometric identifiers, including finger and voice prints

Full face photographic images and any comparable images

Other photographic images, video or audio

Stanford ID number (student, employee)

Lab or pathology test results

Diagnoses or procedures

Psychology or mental health information

Clinical records

Prescriptions or medications

Images or radiology reports

Passport or Visa numbers

Employee personnel files

Grades or performance (students, alumni)

Disciplinary actions or proceedings (students, alumni)

Demographics (age, sex, etc.)

Financial account numbers (e.g., bank accounts, credit)

Financial records, including credit card or bank information

Donor contact and gift information

Salary information

Employment benefits

Other health, medical or physical or mental status information (describe):

Any other unique identifying numbers, characteristic, or code (describe):

Other:

1. **Population Size.** Provide an estimate of the number of individuals whose data will be involved in this project.

1-500  501 – 10,000  > 10,000

1. **Data is Sourced from** (select all that apply):

STRIDE Epic or hospital medical records**\*** Oracle Financials

Registrar HR records Participant provided (e.g., surveys, mobile apps) Government records/systems  Stanford email or other technical system

Other non-Stanford system, database, or party

Other (describe):

Credit card data is collected via Gimmie mobile app.

\*If you selected Epic or hospital medical records, permission from hospital Privacy Office may be required

1. **Is the data coming into or going out of the United States?** No Yes (where?):
2. **data is:**

Identifiable  A limited data set

De-identified using the HIPAA Safe Harbor Method  De-identified using the HIPAA expert determination method

(if expert opinion, **attach** the written opinion to SNOW ticket)

Not PHI but de-identified, pseudonymized, anonymized, or otherwise masked as described

**REQUIRED:** If data is not identifiable, describe the process for removal of identifiers.

1. **FOR VENDOR OR TECHNICAL/SECURITY STAFF TO COMPLETE: INFORMATION ABOUT ADMINISTRATIVE SAFEGUARDS, APPLICATIONS, SYSTEMS, and DATA FLOW OUTSIDE STANFORD**
2. **Name and Contact information for Third Party’s Privacy Officer:**

Name**:**

Bob Bobbinson, CISO – [bb@gimmie.com](mailto:bb@gimmie.com)

443-555-5555

Contact Number:

1. **Name and Contact information for Third Party’s Security Officer:**

Name**:**

Charles Charlson, CPO – cc@gimmie.com

443-555-5556

Contact Number:

1. **Audits, Certifications, and Attestations.**

Please specify **and attach** the most recent annual third party audit report, certification, or attestation covering privacy, security and IT operations and processes, including risk assessment and risk management process; data collection, use, disclosure, storage and destruction policies; software development life cycle; breach/Incident response process; privacy and security awareness training for anyone who handles data; and contingency plan for data recovery in case of an emergency.

Soc 1, Type 2  HITRUST  PCI DSS  ISO 27001/27002  NIST 800-53

Soc 2, Type 2  FEDRAMP  None (**If None**, please attach Privacy Policy and Information Security Policy)

Other (describe below)

PCI-DSS AoC is current and attached to HelpSU ticket

SOC report is dated September 29, 2016 and bridge letter can be provided on request.

1. **Application Authentication.**
2. Provide the application URL in support of this project, if applicable.

URL for SU users and merchants is: stanford.gimmie.com

1. Does web portal support Security Assertion Markup Language (SAML)?  Yes  No

**If no,**

1. Does it support two-step authentication?  Yes No
2. What are the password complexity requirements (e.g., minimum 8 characters, alphanumeric, etc)?
3. **Hosting Environment.** Identify the hosting environment (e.g. Amazon Web Services, physical data center, etc.), backup environment and geographical location of each.

Gimmie core PCI environment is hosted in AWS.

1. **Data Flow.**
2. **Diagram and System Components.** Attach a diagram(s) depicting the proposed data flow in detail. Diagram should include details, such as protocols, ports, and of each system component. Indicate any connections in which the system may exchange [Moderate Risk](https://itservices.stanford.edu/guide/riskclassifications) and/or [High Risk](https://itservices.stanford.edu/guide/riskclassifications) information with another system.



1. **Storage, Retention and Destruction.** Provide a data flow description for each stage of the data lifecycle (collection, storage, use, transmission, access, and destruction).

Gimmie mobile app will be installed on Stanford-owned devices at the gift store. Credit and debit card information will be collected at the time of sale and processed in Gimmie’s AWS platform. Once a credit card transaction has been finalized, the funds will be sent to an SU account. However, Stanford does not receive any credit/debit card information.

Gimmie stores a ledger of credit card numbers, names, expiration dates, CVV, IP address, item purchased and amount of payment for a period of 30 days. This information is stored on servers in Utah. After 30 days, it destroys the card number and name. It purges all credit card data on a semi-annual basis.

Gimmie is affiliated with a network of marketing firms and will disclose type of card used, items purchased, location of purchaser, and amount of purchase with the network. It does not share credit card numbers unless required by law.

Gimmie follows PCI requirements for data collection, storage, use, transmission, access, and destruction.

See PCI-DSS AoC for details.

1. **Data in Transit.**
2. What protocols are supported and enabled to transmit application encrypted data? Select all that apply.

TLS 1.1 TLS 1.2 Other (specify):

1. Is Stanford initiating the transmission?  Yes No
2. Is Stanford pushing or pulling data from other vendor systems? Pushing Pulling Both
3. **Data at Rest**
4. Is data encrypted at rest?  Yes  No
5. Are backups encrypted?  Yes  No
6. Describe how encryption keys are being secured, including who has access to the keys.

Encryption keys are secured using AWS key management.

Only relevant security and system admins have access to encryption keys.

1. **Access.**
2. **Users and Administrators.** Identify the individuals, or classes of individuals, and their roles who will have administrator access and who will have user access to the system. Specify who manages access.

System admins and security personnel have administrative access to Gimmie’s PCI environment in AWS.

Users have a separate web login for administering accounts with Gimmie.

1. **User Methods.** Check the different methods by which the users can access the system

SSH Web Application Client Application

Other (specify)

Portal access can be federated via SAML or username/password with 2nd factor, such as a PIN.

1. **Admin Methods.** Check the different methods by which the administrators can access the system

SSH Web Application Client Application

Other (specify)

Gimmie system administrators and security personnel access system via SSH with username/password and a 2nd factor.