Colgate University
Information Technology Services, Office of the CIO
ITS Data Sharing with External Entities
Audience: Colgate University Community

Contents:
- Preface
- Policy
- Audit and Risk of Non Compliance
- Appendix A - Colgate University Addendum for Data Security Compliance Requirements
- Appendix B - Colgate University Confidentiality and Non-Disclosure Agreement

Section 1. Preface

A. Name
The formal name of this policy is the ITS Data Sharing with external entities.

1. Status of This Policy
   a. Draft.
   b. Public Review and Comment Period or Presidential Cabinet Review.
   c. Redraft.
   d. Working Group Review and Comment.
   e. Accepted.

B. Scope and Purpose.
This document outlines the requirements that must be met prior to providing personally identifiable information (PII) or sensitive personal information (SPI) taken from University owned and managed electronic systems to external entities (for example, affiliated third party vendors or subcontractors working on, or storing, data on behalf of the university).

C. Spirit and Intent.
Colgate University ITS supports the responsible use of data (within the bounds of laws, regulations and broadly accepted best practices) to further the institutional mission. In order to mitigate University liability and protect the individuals about whom the University stores data, it is important that PII/SPI data be handled in compliance with applicable laws and regulations, and in line with generally accepted information security best practices.

Section 2. Policy
Any department or individual entering into an agreement with an external entity to handle PII or SPI must comply with the requirements outlined below prior to providing, or entering into an agreement to provide, PII or SPI data.

A. Requirements

1. Information Security and Data Ownership Consultation. Beginning a minimum of three weeks prior to the expected signature date of any agreement, requestors must contact the Colgate Information Security Officer or CIO to request security and data ownership consultation. As part of the consultation, ITS will work with those requesting permission to allow external entities to handle PII/SPI data to gather the following information and documentation, and keep the following information and documentation on file:

   i. Data Ownership and Permission. ITS serves as the University’s custodian of all data in centrally managed systems. However, much like a bank is a custodian of others’ funds, the data is typically “owned” by specific operational units of the University. Data owners’ permission is required prior to the use or release of any such data.

   ii. Business Need. A brief statement of the reason for releasing PII/SPI to an external entity, approved by a member of the president’s cabinet or the President of the University.

   iii. Required Agreements. The following agreements (or agreements fundamentally similar in nature) between Colgate University and external entities handling PII/SPI data.

   iv. Other Agreements. Any contracts for products or services between Colgate University and the external entity handling PII/SPI data that are related to the specific use of the data.

2. An authorized representative of the external entity must review and sign the following documents, which outline the specific information-security related actions required of the entity with regard to PII/SPI data (attached to this policy for reference).

   i. Addendum for Data Security Compliance Requirements
   ii. Colgate University Confidentiality and Non-Disclosure Agreement

B. Information Security Guidance and Waivers - Case Specific Prior to Agreements Being Entered.

1. Colgate University ITS will evaluate external entities against then-current standards-based security frameworks and may, on a case-by-case basis, require additional documentation, data breach insurance or other assurances in an effort to fully safeguard institutional data.

2. At the discretion of the Vice President and Chief Information Officer or, in his or her absence, the Colgate Information Security Officer, additional information security documentation such as SOC 2 reports, current PCI audit reports or other documentation may be required prior to releasing institutional data.

3. At the discretion of the Vice President and Chief Information Officer, with the consent of the Provost and Dean of Faculty, Senior Vice President and Chief
Financial Officer, or President of the University, any of the requirements of this Policy may be waived with assurance that the spirit of the policy is otherwise being met.

Section 3. Audit and Risk of Non Compliance

A. Colgate University reserves the right to perform periodic audits of 3rd party entities holding institutional data to confirm compliance with the letter and spirit of this policy (or any waivers), and all associated agreements.

B. Those who share Colgate University data with external entities without proper guidance increase the risk for financial and reputational damage to the University, and to the individuals whose personally identifiable information is shared.

C. Failure to follow this policy can result in referral to the office of Human Resources, office of the Dean of the College, or office of the Dean of Faculty/Provost, as appropriate, for disciplinary action.

Appendix A -

Addendum for Data Security Compliance Requirements (“Requirements”)

Colgate University and its affiliates and ________________________ ("Company") have entered into an Agreement for services as of ______________, 20__ (the “Agreement”) which is incorporated herein by reference, and hereby agree to the following additional terms and conditions which shall be effective as of the _____ day of _____________, 20__.

1. Definitions

The following terms have the indicated definitions and meanings:

"Sensitive Data" means data or information provided by or on behalf of Colgate University or its affiliates, regardless of form or media, which is:

a. personally identifiable information, including, but not limited to, an individual’s: (i) Social Security number; (ii) date of birth; (iii) home address; (iv) user passwords or personal identification numbers (PIN); (v) driver’s license or other state or federal identification number; (vi) financial account information; (vii) health or medical information; (viii) insurance ID number; or (ix) biometric data;

b. Colgate University employee data, including, but not limited to; (i) human resources data (e.g., social security number, date of birth, performance reviews, medical information, health information, family information, etc.); or (ii) compensation data;

c. Colgate University corporate financial data, including, but not limited to, information on Colgate University sales, sales projections and corporate strategies, which have not been released to the public;

d. Colgate University application or system user ID and passwords;

e. data which is specifically identified by Colgate University as "Sensitive Data;"

f. Cardholder Data (as defined in Section 6 below); or,

g. any of the foregoing even when categorized under a different name (e.g. a person’s social security number used as an account number).
h. student education record information, or information Colgate University student’s have supplied to supplier

“Company” as used in these Requirements shall include the Company identified in the header above and, any contractors, subcontractors, consultants, temporary associates, or other third parties (“Third Party or Parties”) which Company utilizes to Process Sensitive Data.

"Process or Processing" means any action taken by Company in relation to Sensitive Data, to include access, collection, use, retention, storage, transfer, disclosure, destruction, and any other operation.

"Breach" means any (i) misuse, loss, destruction, compromise, or unauthorized access, collection, retention, storage, or transfer of Sensitive Data or (ii) any act or omission, that causes non-compliance with these Requirements.

"Card" means any credit card, debit card, charge card or declining balance card.

"Cardholder" means the individual to whom the Card has been issued.

"Cardholder Data" means all information provided by or about a Cardholder in the course of a transaction or obtained through the use of a Card, including, but not limited to, name, address, PIN, security code, credit card account numbers, expiration dates, magnetic stripe data and any other information identifying the Cardholder or the related account.

“Secure Facility” means the physical location(s) where Sensitive Data can be stored or electronically processed. Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves and the facilities used to support their operation. For the purposes of this Addendum, the Secure Facility will be _________.

2. Rights and License in and to Sensitive Data

Company agrees that as between Colgate University and Company, all rights including any intellectual property rights in and to Sensitive Data shall remain the exclusive property of Colgate University, and Company has a limited, nonexclusive license to use this data as provided in the Agreement solely for the purpose of performing its obligations thereunder and solely for the term of the Agreement. Neither the Agreement nor these Requirements provide Company any rights, implied or otherwise, to Sensitive Data.

3. Sensitive Data Handling Requirements

When accessing, storing, processing, or transmitting Colgate University Sensitive Data or Systems, Company shall:

I. Prohibition of Unauthorized Use or Disclosure – Company agrees to hold Sensitive Data in strict confidence. Company shall not use or disclose Sensitive Data received from or on behalf of Colgate University except as permitted by the Agreement or this Addendum, as required by law, or otherwise authorized in writing by Colgate University.

II. General Security
a. process Sensitive Data only in accordance with the terms of the Agreement, including, without limitation, these Requirements.
b. maintain and utilize a reasonable privacy and security training program applicable to all Company resources providing Services to Colgate University under the Agreement.
c. Company will have in place, written confidentiality agreements or obligations with all of its employees, subcontractors and vendors who work with Colgate University Sensitive Data.
d. protect against any anticipated threats or hazards to the security or integrity of Sensitive Data, including, without limitation:
   i. reasonable efforts, through the use of industry standard virus and malware protection software and other customary procedures, to avoid introducing or permitting the introduction of any virus into the Colgate University IT environment.
   ii. reasonable efforts to regularly check for and delete viruses and malware in the Company systems used by Company to provide the Services by way of standard industry virus and malware detection tools.
e. protect against unauthorized access to or use of Sensitive Data which could result in substantial harm or inconvenience to Colgate University, including, without limitation:
   i. implementation of administrative, technical and physical security controls to limit access by Company personnel and Colgate University authorized subcontractors to only the Colgate University information they need to provide the Services in this Agreement
   ii. providing user identification and access controls designed to limit access to Colgate University systems and information to authorized users, using complex passwords
   iii. ensuring that access is revoked immediately for those Company personnel who no longer have a direct need to have access to Sensitive Data.
g. implement business continuity and disaster recovery plans necessary to ensure systems, services, and information are not unavailable for a period in excess of twenty-four (24) hours.
h. take prompt corrective action(s) to remedy a violation of (and to prevent future violation of) any of these Requirements.
i. any exception to these Requirements shall require specific, advance written approval by the Colgate University.

III. Security Incidents

a. contact Colgate University promptly (in less than one business day) after a Breach involving Colgate University Sensitive Data is confirmed.
b. take prompt corrective action(s) to remedy a Breach and to prevent future Breach.
c. take prompt corrective action(s) to remediate any vulnerabilities or security concerns in accordance with Company policies.
d. implement corrective action(s) in a timeframe commensurate with the risk or as agreed upon with Colgate University.
e. cooperate fully with Colgate University in facilitating investigation and remediation of a Breach.
f. not inform any third party of any Breach except as specifically required by applicable law, without first obtaining Colgate University’s prior written consent.
g. promptly notify Company’s primary Colgate University business contact of any complaint related to processing of Sensitive Data.

IV. Storing/Transmitting Colgate University Sensitive Information
a. provide evidence of a current SOC2 audit, or evidence of compliance with ISO 27002 or PCI DSS 3.2.
b. provide for daily back-up of Colgate University information and archival of such Colgate University data at a secure facility.
c. encrypt all Company storage devices and networks utilizing industry standard encryption techniques
d. require all Company personnel to use Company owned and managed devices to store Colgate University information, prohibiting all Company personnel from using personal computer equipment for such purposes.
e. prohibit storage to a portable computing devices, e.g., USB drives, cameras and camera phones, and any other portable device that would allow the capturing, printing or storing of Colgate University data or confidential information to be transported outside the secure facilities
f. establish written procedures for the disposal of electronic storage devices and information, which include the destruction and sanitization of all Colgate University information, compliant with NIST 800-88, or a NAID certified 4th party.
g. at the conclusion of the engagement, or upon request, Company will certify that all Colgate University data have been erased from Company, and all subcontractor and downstream recipient's, equipment; or it has removed the storage device(s) from Company, and all subcontractor and downstream recipient's, equipment and provided all storage device(s) to Colgate University.
h. provide industry standard firewalls, both network and device based, that regulate all data entering Company's internal data network from any external source, and which will enforce secure connections between internal and external systems and will permit only specific types of data to pass through.
i. prohibit the use of Colgate University information in Company non-production environments.
j. implement audit controls that record and monitor systems activity continuously, including logging of who has accessed Colgate University information

V. Company Provided Software
a. not knowingly insert or knowingly allow the insertion into the Software of any code which would have the effect of wrongfully disabling or otherwise wrongfully shutting down all or any portion of the Services.
b. train Company personnel in proper techniques for developing secure application
c. upon discovery of software and system vulnerabilities, provide software patches to remediate vulnerabilities, based on a severity rating mutually agreed upon, within seven (7) calendar days for High vulnerabilities, fifteen (15) days for Medium vulnerabilities, and thirty (30) days for Low vulnerabilities.
perform application security analysis and testing (also called "verification") according to the verification requirements of an agreed-upon standard (such as the OWASP Application Security Verification Standard (ASVS)). Company shall document verification findings according to the reporting requirements of the standard. The Company shall provide the verification findings to Colgate University, at a minimum, annually.

4. Company Personnel Requirements

Company shall ensure that a background check is performed on all personnel prior to hiring such personnel if they will have access to Sensitive Data that includes:

a. verification of legal authority to work in the United States as applicable,

b. review of an individual’s record of criminal conviction history in all counties in which the individual resided or worked for more than 30 days within the past seven years to ensure personnel have not been convicted of (i) a felony offense within the past seven (7) years related to violent crimes, property offense, substance abuse, or fraud; or (ii) any misdemeanor related to violent crimes, property offense, substance abuse, or fraud. Criminal conviction history checks include a review of all federal, state and local criminal conviction records; and

c. verification that no personnel are listed on the Office of Inspector General (OIG) sanction and disqualification list.

For purposes of these guidelines, the term “Criminal Conviction” includes probation, deferred adjudication and no contest pleas.

5. Connectivity Requirements

Where Company is permitted to access any internal Colgate University systems, applications, or networks (collectively "Colgate University Systems"), Company shall:

a. only connect to Colgate University Systems through the manner and means authorized by Colgate University.

b. not connect to, access, attempt to access, or use any Colgate University Systems without the prior authorization of Colgate University.

c. notify Colgate University when a Company employee with access to Colgate University Systems has left the company, or no longer has need to access Colgate University Systems.

d. not use any Colgate University System in any way that is illegal, abusive or creates a security risk or vulnerability.

6. Cardholder Data Security

Where Company has any access to or will use any Cardholder Data, Company shall comply with the following, which shall be in addition to, and without limiting other Requirements:

I. Cardholder Data Protection

Company shall implement, maintain and use such proper security controls and measures as is necessary to ensure the secure Processing of Cardholder Data and to protect Cardholder Data from unauthorized Processing or other compromise. In all events, Company shall comply with
the Payment Card Industry ("PCI") Data Security Standard v. 3.0, ("PCI DSS") or such later version or replacement standard.

II. Cardholder Data Breach

In the event any Breach affecting, directly or indirectly, Cardholder Data is suspected or confirmed (an "Event"), Company will notify Colgate University, via email and phone, promptly (in all events, within twenty-four (24) hours) of such Event. Within the next forty-eight hours, Company shall conduct an internal investigation to determine whether unauthorized Processing of Cardholder Data may have occurred and shall report the results of such investigation to Colgate University. Company will provide to Colgate University all information related to Company's investigation or audits related to any unauthorized Processing of Cardholder Data, to include any information received from the issuer of the Card.

III. Compliance with PCI DSS.

During any period of time that Company has Cardholder Data, they shall remain in compliance with PCI DSS, and shall, at Colgate University request, provide proof of compliance to PCI DSS. If, at any time, Company becomes non-compliant with PCI DSS, they must notify Colgate University and shall provide a corrective action plan to identify how they will restore compliance.

7. Off-Shore Processing

No Colgate University data or information, including PHI and PII, may be transmitted or stored outside of the United States, including storage via server storage, backup, printing, photography, copy, paste or similar functions.

Company shall not use a third party subcontractor (other than its affiliates) to provide the Services under the Agreement, without Colgate University’s prior written consent.

Company shall promptly notify Colgate University of any intent to allow processing of Sensitive Data outside of the United States, by either Company itself, or any Third Party. Upon request, Company shall provide reasonable information regarding the Processing of Sensitive Data outside of the United States by Company, its affiliates or its third party subcontractors.

8. Certification and Compliance Requirements

These Requirements shall apply to all Sensitive Data which is: (i) Processed by Company, (ii) provided to Company by or on behalf of Colgate University, (iii) learned or otherwise used by Company during or in connection with the performance of services under the Agreement, or (iv) retained by Company.

Further, Company shall provide documentary evidence to Colgate University to show compliance with the applicable Requirements, upon request of Colgate University. Documentary evidence may include summaries of the Company’s applicable security policies and standards, and/or written certifications of Sensitive Data destruction.

9. Third Party Compliance
Company shall be solely responsible and liable for ensuring that any third party subcontractor who Process Colgate University Sensitive Data as part of Company’s performance under the Agreement fully comply with this Agreement, to include Audit Rights.

10. Non-Compliance

Company's failure to comply with any Requirement shall be a breach of the Agreement(s) with Colgate University. Without limiting any other right or remedy that Colgate University may have, Colgate University reserves the right to terminate, for default or breach, the Agreement as a result of such noncompliance in accordance with the terms of the Agreement.

11. Audit Rights

To the extent that Company stores or maintains Sensitive Data, Company shall, upon reasonable notice, allow its data processing facilities, systems, procedures and documentation to be inspected by Colgate University or designee(s) thereof, to assess compliance with these Requirements, any applicable law, and the Agreement between Colgate University and Company. Company shall reasonably cooperate with such audit requests by providing access to personnel, physical premises, documentation, and infrastructure which Company uses to perform its obligations under the Agreement.

In the event that any Colgate University Sensitive Data is processed or available through a Company website, Company shall conduct annual penetration tests and vulnerability scans. Company must provide the results of such testing and where deficiencies have been identified corrective action plans to Colgate University upon request.

12. Delegation by Colgate University

Colgate University may delegate any right granted to Colgate University under these Requirements. Company shall provide such access, information, data, and cooperation to such designee as Company is required to provide Colgate University under these Requirements.

13. Survival of Requirements

These Requirements shall remain in effect so long as Company has any Colgate University Sensitive Data, regardless of any termination, amendment or executions of other agreements, and further shall remain in effect until Company has certified that they have destroyed or returned all Sensitive Data. Where retention of Sensitive Data is required by law, these Requirements shall remain in effect for the period required by applicable law, after which time, Company shall destroy or return all Sensitive Data, in accordance with these Requirements.

14. Indemnity

Company shall defend and hold Colgate University harmless from all claims, liabilities, damages, or judgements involving a third party, including Colgate University’s costs and attorney fees, which arise as a result of Company’s failure to meet any of its obligations under this Agreement.
IN WITNESS WHEREOF, the Parties have each caused these Requirements to be signed and delivered by its duly authorized officer, all as of the date first set forth above. Company acknowledges that the Agreement allows access to Colgate University Sensitive Data.

☐ All requirements in this document apply
☐ All of the requirements in this document apply, with the exception of:

Section 3, Sensitive Data Handling Requirements
☐ Storing/Transmitting Colgate University Sensitive Information
☐ Provided Software

☐ Section 5, Connectivity Requirements
☐ Section 6, Cardholder Data Security
☐ Section 7, Off-Shore Processing

Colgate University

By: ____________________________
Name: __________________________
Title: ____________________________
Date: ____________________________

COMPANY

By: ____________________________
Name: __________________________
Title: ____________________________
Date: ____________________________

Appendix B

COLGATE UNIVERSITY CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

Colgate University and its affiliates (“Client Name”) and ______________________ ("[Company/Employee]") have entered into an Agreement for services as of ______________, 20__ (the “Agreement”) which is incorporated herein by reference, and hereby agree to the following additional terms and conditions which shall be effective as of the _____ day of ______________, 20__.

RECITALS
A. Colgate University desires to protect from disclosure to third parties Confidential Information which has or will inevitably be revealed during the course of the parties’ interaction;

B. The parties acknowledge that disclosure of Confidential Information to competitors or other third parties, may cause severe damage to them, their sales, and their ability to compete; and

C. The parties desire to avoid such disclosure.

AGREEMENT

Therefore, the parties agree as follows:

1. Term. This Agreement may be terminated by Colgate University at any time upon thirty (30) days prior written notice to [Company / Employee]; provided, however, all Sections of this Agreement relating to the rights and obligations of the parties concerning Confidential Information as defined in Section 2 shall survive termination of the Agreement.

2. Confidential Information. [Company / Employee] acknowledges that they may obtain or may have obtained, from Colgate University, information Colgate University considers to be confidential, including, but not limited to, personal data, Social Security numbers, dates of birth, earnings, benefits and retirement data, ideas, methods, design concepts, inventions, internet implementation, operation processes and policies, products, technology, business plans, business partners, potential or pending acquisitions, roll-out dates, timelines, any customer information, location information, advertising and marketing plans and strategies, formulas, patterns, devices, usernames, systems, applications, specifications and data, software (including, without limitation, its architecture, features, functions, structure and code), customer and supplier lists, financial information, and compilations of information (“Confidential Information”). Further, [Company / Employee] acknowledges that Confidential Information may be transmitted orally, in writing, photocopying, photographs, computer files, notes, memos, faxes, letters, e-mails, files, reports, surveys, presentations, business plans, financial documents, analyses, video and audio tapes, and any other method of transmitting information whether prepared by the [Company / Employee] or by a third-party on the [Company / Employee]’s behalf.

4. Protection of Confidential Information. Except as provided herein, [Company / Employee] shall take all reasonable affirmative steps to prevent disclosure of Colgate University’s Confidential Information and maintain all Confidential Information, whether obtained either directly or incidentally and regardless of its form, confidential and safe from accidental or purposeful disclosure to any third party. [Company / Employee] will disclose Colgate University’s Confidential Information only to those of its employees, agents, attorneys, consultants, and contractors who have a need to receive the Confidential Information to further the purposes of this Agreement, provided the party has advised such employees, agents, attorneys, consultants, and contractors of the obligations under this Agreement and provided that such employees, agents, attorneys, consultants, and contractors are bound to protect such Confidential Information under terms comparable to the restrictions in this Agreement. Notwithstanding the foregoing, the [Company / Employee] disclosing Confidential Information shall be responsible and liable for any
unauthorized disclosure by its agents, attorneys, consultants and contractors. [Company / Employee] shall make all reasonable efforts (including the design and implementation or use of an existing procedure for handling Confidential Information) to safeguard Colgate University’s Confidential Information from disclosure to unauthorized individuals and for as long as the information disclosed remains Confidential Information as provided in Section 2.

5. Unauthorized Disclosure. Promptly upon discovery of any unauthorized intentional, unintentional or accidental disclosure of Confidential Information, [Company / Employee] shall notify Colgate University in writing of such disclosure. The notice shall contain a description of the Confidential Information disclosed, the approximate date of disclosure, to whom the Confidential Information was disclosed and the circumstances surrounding the disclosure.

6. Compelled Disclosure. In the event that [Company / Employee] is requested or required to disclose any Confidential Information via subpoena, discovery request, court order or any other request, the [Company / Employee] subject to such request or requirement will provide Colgate University with prompt, written notice of such request so that Colgate University may seek an appropriate protective order or agree in writing to waive the prohibition on disclosure of said Confidential Information. Failure to notify Colgate University in accordance with the requirements of this Section shall be considered a material breach of this Agreement and Colgate University may, in its sole discretion, elect to proceed with any or all remedies set forth in Section 7, below.

7. Remedies for Unauthorized Disclosure. In the event that [Company / Employee] discloses Colgate University’s Confidential Information for any reason, except as permitted in Section 4 or Section 6 above, Colgate University may, in its sole discretion, discontinue its relationship with the Employee / Vendor, terminate this Agreement, and seek whatever remedies may be available to it at law or equity. The foregoing notwithstanding, all the confidentiality provisions of this Agreement shall survive the cancellation or cessation of the relationship between the [Company / Employee] and Colgate University hereof for as long as the information disclosed remains Confidential Information as provided in Section 2. It is understood and agreed that money damages alone may not be a sufficient remedy for any breach of this Agreement and that Colgate University shall be entitled to seek injunctive relief, specific performance or other appropriate legal and equitable remedies for any such breach. These remedies shall not be deemed to be the exclusive remedy for any breach but shall be in addition to all other remedies available to Colgate University at law or in equity.

8. Copies. [Company / Employee] may make or cause to be made copies or other reproductions of Colgate University’s Confidential Information in its possession as necessary to accomplish the intent of this Agreement; provided, however, that all such copies shall remain the property of Colgate University and shall be returned or destroyed upon request of Colgate University.

9. Return or Destruction of Confidential Information. If, for any reason, the relationship between the parties is discontinued (including termination of this Agreement) or upon demand by Colgate University, [Company / Employee] shall return all Confidential Information
to Colgate University within ten (10) days. Alternatively, within the same period, Colgate University may request that the Employee / Vendor destroy all of Colgate University’s Confidential Information in its possession. Within ten (10) business days after receipt of a request for the return or destruction of all Confidential Information, [Company / Employee] shall certify in writing that all such Confidential Information was returned or destroyed, as applicable.

10. **Applicable Law.** This Agreement shall be governed by the laws of the State of New York without reference to choice of law or conflict of law principles.

11. **Notices.** Any notice required hereunder shall be in writing and shall be deemed to have been duly given (i) the same day if personally delivered, (ii) the next day if sent by an overnight courier service, or (iii) after five (5) business days if sent by certified mail, return receipt requested, postage prepaid, to the parties at their respective addresses. Either party may change the address to which written notices shall be given at any time upon prior written notice to the other party.

Notice: All notices regarding this Agreement are to be submitted in writing and shall be personally delivered, sent via overnight courier service, or sent via registered mail, return receipt requested to:

If to Colgate University, to: Colgate University
Attn: ____________________________

[CLIENT STREET ADDRESS]
[APT. / SUITE NUMBER], if applicable

[CLIENT CITY, STATE, ZIP CODE]

If to _______________, to: ______
Attn: ______

________

12. **No License.** This Agreement does not grant and shall not be construed as granting to [Company / Employee] a license or any rights under any patent, trademark, copyright, or trade secret of Colgate University beyond that which is necessary for the purposes of this Agreement.

13. **Entire Agreement.** This Agreement constitutes the entire agreement between the parties hereto with respect to its subject matter. This Agreement supersedes any and all prior agreements, discussions, negotiations, arrangements, or understandings, whether written, oral or implied, with respect to the subject matter of this Agreement. This Agreement may not be modified or amended without the prior written consent of each party.

14. **Attorney Fees.** In the event of any claim, dispute, or legal proceeding arising out of or relating to this Agreement, Colgate University shall be entitled to recover, and the [Company / Employee] shall pay, all fees and expenses (including, without limitation, costs of investigation, reasonable attorneys’ fees and litigation expenses) incurred in connection therewith.
IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives.

Colgate University  [COMPANY / EMPLOYEE]

By:  
Name:  Name: 
Title:  