REVISION CONTROL

Document Title:	VISC Third Party Guidelines
Author:	Andru Luvisi
File Reference:	CSU Information Security Managing Third Parties policy

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
09/16/2011	Andru Luvisi	Draft of VISC guideline	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
01/11/2011	VISC Docs Team	Recommended to VISC team
01/25/2011	VISC Group	Recommended to VISC Governance
02/07/2012	VISC Governance	Approved

1.0 INTRODUCTION

The University can choose to contract with software and service vendors. These arrangements can require the University to send protected data from its systems to those of the vendor. The University will need to take steps to ensure that these arrangements do not weaken its information security or place its data at risk of unauthorized disclosure. This guideline describes administrative controls for managing vendor's access to data from the University.

2.0 PURPOSE

This guideline provides sample contract language, checklists and a procedure that may be adopted by campuses with or without modification to assist in complying with the CSU Information Security Managing Third Parties Policy and the CSU Information Security Third Party Security Standard.

3.0 SCOPE

This guideline and its samples may be used any time CSU data is received, transmitted, stored, or processed by a third party, especially when level 1 or 2 data is involved.

4.0 GUIDELINE

Any University department entering into an agreement to use software operated by a Third Party servicer or to provide protected data to a vendor who will store it on its systems (outside the University) will need to ensure that security and audit controls employed by the vendor are evaluated before contracting with a vendor in all cases to ensure that the University is adequately protected against loss.

The University will need to ensure that when critical or protected information is shared with third parties, it is either specifically permitted or required by law and that a written agreement is executed between the parties that identifies the applicable laws, regulations, and CSU/campus policies, standards, procedures, and security controls that must be implemented and followed to adequately protect the information asset.

4.1 Sample Checklist

Below is a sample checklist which includes some basic guideline considerations for managing a third party relationship and dealing with University sensitive information. Some of these questions are included in the Sample Contract (Appendix A). If the question is included in the Sample Contract, then it is highlighted in 'Bold' and 'Italics' with the corresponding Sample Contract section at the end of the question. This checklist is provided to help ensure that all the important questions are asked when managing a third party.

☐	**1.** ***Is there a written agreement for the vendor to provide the data to the University upon contract termination? (Section 9.0)***
☐	***2.*** ***Is there a written agreement for the vendor to securely delete the University's data including backups, upon contract termination? (Section 9.0)***
☐	**3.** ***Is there a written agreement for the vendor to follow University and CSU security policies and standards? (Section 3.2)***

☐	**4.** ***Is there a written agreement for the vendor to maintain the privacy of protected personal information and be financially responsible, if and to the extent that any security breach relating to protected personal information results from acts or omissions of the vendor, or its personnel, for any notifications to affected persons (after proper consultation with the University), and to the extent requested by the University, administratively responsible for such notifications? (Section 5.6)***
☐	**5.** ***Is there a written agreement for the vendor to protect University data according to published information security policy and standards and no less rigorously than it protects its own confidential information, and in no case less than reasonable care? (Section 3.2)***
☐	**6.** ***Is there a written agreement for the vendor to require all employees, affiliates and subcontractors with access to university data, as a condition of their engagement, to participate in annual security awareness training? (Section 6.0)***
☐	**7.** ***Is there a written agreement for the vendor to comply and cause its representatives, affiliates and subcontractors to comply with all personnel, facility, safety and security rules and regulations and other instructions of the University, when performing work at a university facility, and to conduct its work at University facilities in such a manner as to avoid endangering the safety, or interfering with the convenience of, University representatives or customers? (Section 6.0)***
☐	**8.** ***Is there a written agreement for the vendor who must share University data to with a subcontractor to not disclose any Protected Data other than on a "need to know" basis with the subcontractor? (Section 2.0)***
☐	**9.** ***Is there a written agreement for the vendor in connection with this agreement that requires written consent from the University to prior work being performed in connection with this agreement by the vendor, its affiliates or subcontractors, outside of the United States, unless the prior written consent of the University is received to perform work outside the United States? (Section 2.0)***
☐	***10.*** ***Is there a clause in a written agreement where the vendor has agreed to promptly provide annual, or at the request of the University, current evidence of compliance with the PCI DSS or PA DSS (as appropriate)? (Section 5.3)*** ***a)*** ☐ ***Has the vendor supplied a copy of the most recent SAS 70 report from the vendor covering the subject matter relevant to the University? (Section 5.3)*** ***b)*** ☐ ***Has the vendor supplied documentation showing a recent PCI audit, or a statement indicating why this information is not available? (Section 5.3)***
☐	***11.*** ***Is there a written agreement for the vendor to fully comply with all applicable federal and state laws, including but not limited to, as appropriate, HIPAA, HITECH, GLBA, SB1386 and FERPA? (Section 2.0)***
☐	**12.** ***Is there a written agreement for the vendor to provide immediate notification to the University's primary contact and Information Security Officer whenever there is a breach of protected data, not later than 24 hours after discovery? (Section 4.1)***

☐	**13.** ***Is there a written agreement for the vendor to provide reasonable care and effort to detect fraudulent credit card activity in connection with credit card transactions processed for the University? (Section 5.2)***
	ADDITIONAL QUESTIONS THE UNIVERSITY WILL NEED TO CONSIDER
☐	What data elements will be shared with, or collected by, the vendor?
☐	Has the data been classified according to the CSU Data Classification Standard?
☐	Has the data owner been identified, and has this person explicitly approved access to the data by the vendor?
☐	Has the vendor made a commitment to providing a specific level of availability?
☐	Has the vendor identified any subcontractors used for the project?
☐	Does the contract include provisions for contract termination if security provisions are not met?
☐	Will level 1 or 2 data be involved? If so: ☐ Has a risk assessment been performed? ☐ Will encryption be used for all removable media? ☐ Will all data transfers be encrypted?
☐	Will the vendor store, process, or transmit credit card data? If so: ☐ Is the vendor compliant with the Payment Card Industry Data Security Standard? ☐ Are all applications used by the vendor compliant with the Payment ☐ Application Data Security Standard as appropriate?
☐	Have provisions been made for the University to have the ability to inspect and review vendor operations for potential risks to university operations or data?
☐	Will the service involve Protected Health Information? If so: ☐ Has the vendor agreed to use and disclose this information in compliance with HIPAA and HITECH?
☐	Has the vendor supplied a copy of the vendors existing information security and privacy policies? ☐ Do they address systems and application management, including change control, encryption, firewall management, remote access, vulnerability scanning, monitoring, patch management, incident management, system hardening, and intrusion detection and response?

	☐ Do they address redundancy in power, storage, networking, computers, Internet service, or other technical measures designed to eliminate single points of failure? ☐ Do they describe existing security procedures and practices to maintain a separation between data owned by different clients on production, test, and data backup environments? ☐ Do they describe established vendor data protection and recovery plans, and provide evidence that these plans have been recently tested?

4.2 Sample Contract Language

Sample contract language can be found in Appendix A.

4.3 Sample Procedure

Before the purchase of any third party service, the service should be evaluated against a standard security checklist. (Campuses may wish to adopt a version of the checklist supplied in this guideline.)

All University data that may be shared with third parties should be classified according to the CSU Data Classification Standard.

The University should insist that contracts include appropriate contract language, as determined by the kind of data being handled by the third party service provider.

If any CSU protected level 1 or 2 data is to be handled by the third party service, then the purchase should be subject to the approval of the Information Security Officer or their designee.

Prior to University data being stored or transferred to the third party, the appropriate data owner should approve.

Prior to University data being stored or transferred to the third party, the third party should provide the following documents at a minimum:

- Current Security Plan
- Current Security Audit Documentation (SAS 70)
- Incident Response / Breech Notification Procedure
- Signed Confidentiality agreement for each employee

Campuses should maintain a list of active contracts involving CSU Level 1 or CSU Level 2 data classification types.

Campuses should have documented mechanisms for periodic audit and risk assessment.

5.0 DEFINITIONS

All definitions from the Integrated CSU Administrative Manual glossary (http://www.calstate.edu/icsuam/glossary/) are incorporated here by reference.

6.0 REFERENCES

The CSU Information Security Managing Third Parties policy.
http://www.calstate.edu/icsuam/sections/8000/8040.0.shtml

The CSU Data Classification Standard.
http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf

The CSU Information Security Third Party Security standard.

8040_FINAL_DRAFT_IS_Standard_Third_Part

Appendix A

Proposed Contract Language for Third Party Service Providers Working with Level 1 and 2 Information Assets

Table of Contents

1.0 ACKNOWLEGEMENT

[This section is required if the product/service involves CSU Protected Data.]

Contractor acknowledges that its contract/purchase order with the California State University ("CSU") may allow the Contractor access to CSU Protected Data including, but not limited to, personal information, student records, health care information, or financial information. This data may be transferred in various forms, notwithstanding the manner in which or from whom it is received by Contractor subject to state laws that restrict the use and disclosure of such information, including the California Information Practices Act (California Civil Code Section 1798 et seq.) and the California Constitution Article 1, Section 1. **Contractor represents and warrants that it will keep CSU Protected Data strictly confidential both during the Term and after the termination of the Agreement.**

2.0 DISCLOSURE REQUIREMENTS

[This section is required if the product/service involves CSU Protected Data.]

Contractor shall not use or disclose Protected Data except as permitted or required by the Agreement or as otherwise authorized in writing by University. Contractor shall maintain the privacy of, and shall not release, Protected Data without full compliance with all applicable state and federal laws, University policies, and the provisions of this Agreement.

Contractor agrees that it will include all of the terms and conditions contained in this agreement in all subcontractor or agency contracts providing services under this Agreement. Contractor further acknowledges the applicability to this Agreement of Federal privacy laws such as the Gramm-Leach-Bliley Act (Title 15, United States Code, Sections 6801(b) and 6805(b)(2)) applicable to financial transactions and the Family Educational Rights and Privacy Act (Title 20, United States Code, Section 1232g) applicable to student records and information from student records.

The contractor agrees that except as otherwise specifically provided for in this Agreement; CSU data will not be shared, sold, or licensed or otherwise disclosed with or to any third-party by the Contractor.

Contractor shall not disclose or use University Protected Data other than to carry out the purposes of this agreement. Contractor shall not disclose any Protected Data other than on a "need to know" basis and then only:

a. To its employees or officers, provided, however that each such employee or officer have entered into a confidentiality agreement, that is enforceable under the laws of each applicable jurisdiction, with terms no less restrictive than the terms hereof;
b. To affiliates of or subcontractors to Contractor, only if previously approved by University and provided that

    i. Use by such Affiliates shall be limited to the purpose of this agreement;
    ii. Affiliate is bound by contract and or confidentiality agreement to protect CSU data from unauthorized access.

If required by a court of competent jurisdiction or an administrative body to disclose Protected Data, Contractor will notify University in writing prior to any such disclosure in order to give University an opportunity to oppose any such disclosure. Prior to any disclosure of Confidential Information as required by legal process, the Contractor shall:

c. Notify the University of any, actual or threatened legal compulsion of disclosure, and any actual legal obligation of disclosure immediately upon becoming so obligated, and
d. Cooperate with the University reasonable, lawful efforts to resist, limit or delay disclosure.

Any access, transmission, or storage of Protected Data outside the United States is subject to prior written authorization by the University.

2.1 Exceptions to Obligations of Confidentiality

With the exception of the data classified as "Personally Identifiable Information", the obligations of confidentiality shall not apply to any information that

a. Contractor rightfully has in its possession when disclosed to it, free of obligation to University to maintain its confidentiality;
b. Contractor independently develops without access to University Protected Data;
c. is or becomes known to the public other than by breach of this contract;
d. University or its agent releases without restriction; or
e. Contractor rightfully receives from a third party without the obligation of confidentiality.

Any combination of Protected Data disclosed with information not so classified shall not be deemed to be within one of the foregoing exclusions merely because individual portions of such combination are free of any confidentiality obligation or are separately known in the public domain.

Failure by Contractor to comply with any provision of this Section shall constitute a breach of the Agreement.

3.0 INFORMATION SECURITY PLAN

[This section is required if the product/service involves CSU Protected Data. This section contains two sub-sections. The University will select one of the two sub-sections to use in their contract. The first sub-section is to be used for large vendors or high risk projects. The second sub- section is to be used for small vendors or low risk projects. The size of the vendor and level of risk will be determined by the University.]

3.1 Large Vendor High Risk Projects

[This clause is appropriate for large vendors or high risk projects]

Contractor acknowledges that University is required to comply with information security standards for the protection of Protected Data Information required by law, regulation and regulatory guidance, as well as University's internal security policy for information and systems protection.

Within thirty (30) days of the Effective Date of the Agreement and subject to the review and approval of University, Contractor shall establish, maintain and comply with an information security plan ("Information Security Plan"), which shall contain such elements that University may require after consultation with Contractor. On at least an annual basis, Contractor shall review, update and revise its Information Security Plan, subject to University's review and approval. At University's request, Contractor shall make modifications to its Information Security Plan or to the procedures and practices thereunder to conform to University's security requirements as they exist from time to time.

Contractor's Information Security Plan shall be designed to:

- Ensure the security, integrity and confidentiality of CSU Protected Data;
- Protect against any anticipated threats or hazards to the security or integrity of such information;
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the person that is the subject of such information;
- Protect against unauthorized changes to or use of CSU Protected Data; and
- Comply with all applicable CSU policies legal and regulatory requirements for data protection.
- Include business continuity and disaster recovery plans.

Contractor's Information Security Plan shall include a written response program addressing the appropriate remedial measures it shall undertake in the event that there is an information security breach.

Contractor shall cause all Subcontractors and other persons and entities whose services are part of the Services which Contractor delivers to University or who hold University Protected Data, to implement an information security program and plan substantially equivalent to Contractor's.

The parties expressly agree that Contractor's security procedures shall require that any Protected Level 1 Data transmitted or stored by Contractor only be transmitted or stored in an encrypted form approved by University.

In addition, Contractor represents and warrants that in performing the Services, it will comply with all applicable privacy and data protection laws and regulations of the United States including, as applicable, the provisions in the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6801 et seq., the Family Education Rights and Privacy Act ("FERPA"), 20 USC Section 1232(g) et seq., and of any other applicable non-U.S. jurisdiction, including the European Union Directives, and that it will use best efforts, consistent with Federal Trade Commission and other applicable guidance, to protect University's Personally Identifiable Information from identity theft, fraud and unauthorized use.

3.2 Small Vendor Low Risk Projects

[This clause is appropriate for small vendors or low risk projects]

Contractor agrees that it will protect CSU Protected Data according to published information security policy and standards and no less rigorously than it protects its own confidential information but in no case less than reasonable care.

Contractor shall develop, implement, maintain and use appropriate administrative, technical and physical security measures, which may include but not be limited to encryption techniques, to preserve the confidentiality, integrity and availability of all such Protected Data.

In addition, Contractor represents and warrants that in performing the Services, it will comply with all applicable privacy and data protection laws and regulations of the United States including, as applicable, the provisions in the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6801 et seq., the Family Education Rights and Privacy Act ("FERPA"), 20 USC Section 1232(g) et seq., and of any other applicable non-U.S. jurisdiction, including the European Union Directives, and that it will use best efforts, consistent with Federal Trade Commission and other applicable guidance, to protect University's Personally Identifiable Information from identity theft, fraud and unauthorized use.

Failure by Contractor to comply with any provision of this Section shall constitute a breach of the Agreement.

4.0 INCIDENT RESPONSE MANAGEMENT

[This section is required if the product/service involves CSU Protected Data.]

4.1 Notification of a Security Incident

Contractor shall report, in writing, to University any use or disclosure of CSU Protected Data not authorized by this Agreement or authorized in writing by University, including any reasonable belief that an unauthorized individual has accessed CSU Protected Data. This report shall be made to University's [primary contact] and its designated information security officer. It shall include details relating to any known or suspected security breach of Contractor's system or facilities which contain University Protected Data or any other breach of Protected Data relating to this Agreement. This report shall be made immediately - not later than within twenty-four (24) hours after discovery, if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

4.2 Reporting a Security Incident

Contractor's report shall identify:

- the nature of the unauthorized use or disclosure,
- time and date of incident,
- description of the University Protected Data used or disclosed,
- who made the unauthorized use or received the unauthorized disclosure,

- what Contractor has done or shall do to mitigate any harmful effect of the unauthorized use or disclosure, and
- what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

Contractor shall provide such other information, including a written report, as reasonably requested by University.

Contractor agrees to fully cooperate with the University for the preparation and transmittal of any notice, which University may deem appropriate or required by law, to be sent to affected parties regarding the known or suspected security breach, and to further take appropriate remedial action with respect to the integrity of its security systems and processes.

5.0 COMPLIANCE WITH LAWS

Contractor shall comply with all applicable CSU policies, United States federal, state and local laws, regulations and ordinances, and rules of self-regulatory organizations, as well as all national, state and local laws, regulations and ordinances, and rules of self-regulatory organizations of any other non-U.S. jurisdiction to which Contractor, University or the Services are subject. If a charge of non-compliance with such laws, regulations and rules is brought against Contractor in connection with this Agreement or the Services, Contractor shall promptly notify University of the charge in writing.

Where a federal, state or local law, ordinance, rule or regulation is required to be made applicable to this Agreement, it shall be deemed to be incorporated herein without amendment to this Agreement.

5.1 ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

Contractor shall make itself, and any employees, subcontractors, or agents assisting Contractor in the performance of its obligations under the Agreement, available to University at no cost to University to testify as witnesses, provide information or otherwise assist in the event of litigation or administrative proceedings against University, its directors, officers, agents or employees based upon claimed violation of laws relating to security and privacy and arising out of this agreement.

5.2 PCI-DSS REQUIREMENTS

[This section is required if Contractor provides a service that involves credit card Data. This section is to be used for services involving the storage, transmission, and processing of credit card data]

Contractor represents and warrants that it shall implement and maintain certification of Payment Card Industry ("PCI") compliance standards regarding data security and that it shall undergo independent third party quarterly system scans that audit for all known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (i.e., viruses and worms) to gain access to or disrupt the network devices. If during the term of the Agreement, Contractor undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI DSS standards and/or other material payment card industry standards, it will promptly notify the University of such circumstances.

Contractor agrees promptly to provide annual, or at the request of the University, current evidence, in form and substance reasonably satisfactory to University, of compliance with PCI-DSS security standards which has been properly certified by an authority recognized by the payment card industry for that purpose.

Contractor shall maintain and protect in accordance with all applicable laws and PCI regulations the security of all cardholder data when performing the contracted Services on behalf of the University.

Contractor will provide reasonable care and efforts to detect fraudulent credit card activity in connection with credit card transactions processed for University,

Contractor shall not be held responsible for any such loss of data if it is shown that the loss occurred as a result of the sole negligence of the University.

5.3 PA DSS REQUIREMENTS

[Team Comment – This section is required if the software application provided by Contractor involves the storage, transmission, and processing of credit card data]

Contractor represents and warrants that software applications it provides for the purpose of processing payments, particularly credit card payments, are developed in accordance with and are in compliance with the standards known as Payment Application Data Security Standards (PA-DSS). As verification of this, the Contractor agrees to provide evidence that any such application it provides is certified as complying with these standards and agrees to continue to maintain that certification. The evidence may be provided in the form of the PA DSS form if the contractor self certified, or a copy of the PA QSA if the Contractor was certified by an external party. If the vendor is unable to provide a copy of the PA DSS form of the PA QSA letter, the vendor must provide the CSU with proof of bonded insurance listing the CSU as the beneficiary in the case of a security breach.

If during the term of the Agreement, Contractor undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PA DSS standards and/or other material payment card industry standards, it will promptly notify the University of such circumstances.

Contractor agrees promptly to provide, annual or at the request of the University, current evidence, in form and substance reasonably satisfactory to University, of compliance with PA-DSS security standards which has been properly certified by an authority recognized by the payment card industry for that purpose.

5.4 NACHA REQUIREMENTS

[This section is required if the goods or services involves ACH payments.]

Contractor agrees to assist the University in documenting compliance with NACHA-The Electronic Payment Association provisions.

5.5 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

[This section is required if the goods or services involves protected health information.]

Contractor shall agree to use and disclose Protected Health Information in compliance with the security standards for the protection of electronic protected health information as per (45 C.F.R. Parts 160 and 164).

5.6 INDEMNIFICATION FOR INFORMATION SECURITY BREACH

Contractor shall indemnify, defend, protect and hold University harmless from and against any and all claims, losses, damages, notices and expenses, including, without limitation, any fines which University maybe required to pay, which result from Contractor's breach of the provisions of this Section.

Without limiting the generality of the foregoing, it is expressly agreed that if the University pays any fine in connection with a breach by Contractor of the provisions of this Section, the foregoing indemnity obligation shall require Contractor to reimburse University the full amount of such fine within thirty (30) days of University delivering written notice to Contractor of University's payment of such fine.

Contractor shall fully cooperate with any investigation of any data loss or other breach of Contractor's obligations under this agreement. Such investigation may instituted by University or any other entity with jurisdiction to conduct such investigation.

Failure by Contractor to comply with any provision of this Section shall constitute a breach of the Agreement.

6.0 PERSONNEL SECURITY REQUIREMENTS

Contractor shall require all Affiliates and Subcontractors, as a condition to their engagement, to agree to be bound by provisions substantially the same as those included in this Agreement.

Any work to be performed in connection with this Agreement by Contractor, its Affiliates or Subcontractors must be performed in the United States, unless the prior written consent of the University is received to perform work outside the United States. Further, University Protected Data may not be transmitted or stored outside the United States without the prior written consent of University.

Contractor shall require all employees, Affiliates and Subcontractors with access to University's protected information as a condition of their engagement, to participate in annual security awareness training.

Contractor shall comply and shall cause its Representatives, Affiliates and Subcontractors to comply with all personnel, facility, safety and security rules and regulations and other instructions of University, when performing work at a University facility, and shall conduct its work at University facilities in such a manner as to avoid endangering the safety, or interfering with the convenience of, University Representatives or customers.

Contractor shall not knowingly permit a Representative or Subcontractor to have access to the records, data or premises of University when such Representative or Subcontractor:

a. has been convicted of a crime;
b. has engaged in a dishonest act or a breach of trust; or
c. use of illegal drugs.

Contractor agrees that under no circumstances shall any of Contractor's employees, officers, Affiliates or Subcontractors, whether full-time or part-time, connect to any University system or access any University data, for purposes of downloading, extracting, storing or transmitting information through personally owned, rented or borrowed equipment including, but not limited to mobile devices (e.g., laptops, PDAs, cell phones, etc.,)

Contractor represents that it maintains comprehensive hiring policies and procedures which include, among other things, a background check for criminal convictions, and pre-employment drug testing, all to the extent permitted by law. Contractor shall conduct thorough background checks and obtain references for all its Representatives and Subcontractors who have access to University's protected information.

Any exceptions are at variance with University policy and must be approved in advance according to University policy guidelines.

7.0 RECORD RETENTION REQUIREMENTS

[The records and residual data retention periods should be specified by the University in accordance with the CSU's records retention policy and schedule(s)]

Contractor shall maintain all records pertaining to the Services provided to University under this Agreement for a period consistent with the records retention policy of the University or longer after termination of the Agreement, if required by applicable law or regulation. Contractor further agrees to provide to University, at its request, a full copy of all such records for University to maintain at a U.S. location which University shall designate.

Any residual data that exists on backups must be destroyed or purged in agreement with the Universities records retention policy. Backup data may not be archived.

8.0 CSU RIGHT TO CONDUCT AND/OR REVIEW RISK ASSESSMENTS OR AUDITS

Contractors with access to University protected data shall conduct risk assessments and/or audits of University protected data at least annually. The Contractor shall provide University with copies of its latest information security risk assessments and/or audits upon request.

During regular business hours, University may, at its sole expense and on a mutually agreed upon date (which shall be no more than fourteen (14) days after written notice), time, location and duration perform or arrange for a site visit and/or

confidential audit of Contractor's operations, facilities, financial records, and security and business continuity systems which pertain specifically to the Services.

If Contractor is not in substantial compliance with the requirements of the performance requirements set forth in this Agreement, University shall be entitled, at Contractor's expense, to perform additional such assessments and/or audits. University will provide to Contractor a copy of each report prepared in connection with any such audit within thirty (30) calendar days after it prepares or receives such report. Contractor agrees to promptly take action at its expense to correct those matters or items that require correction as mutually agreed.

If any assessment and/or audit disclose material variances from the performance requirements set forth in this Agreement or a breach by Contractor of the provisions of this Agreement, Contractor shall be deemed in breach of this Agreement.

9.0 TERMINATING OR EXPIRING THE AGREEMENT

Upon the termination or expiration of this Agreement, or at any time upon the request of University, Contractor and its subcontractors shall return all University Protected Data (and all copies and derivative works thereof made by or for Contractor). Further, Contractor and all subcontractors shall delete or erase such Protected Data, copies and derivative works thereof, from their computer systems.

University shall have the right to require Contractor to verify, to University's satisfaction, that all University Protected Data has been returned, deleted or erased. Contractor agrees to fully cooperate with University's requests for verification.