

STANFORD UNIVERSITY
Outsourced Application Development
Information Security Requirements

1. OVERVIEW

This document defines the minimum information security criteria that the Outsourced Provider (OSP or the Vendor) of Application Development or Application Support Services must meet in order to be in compliance with Stanford's Information Security Policies, Standards and Guidelines.

These Standards are subject to additions and modification. Stanford will provide reasonable notice of any revisions to the Vendor to allow adequate time to make any necessary changes in infrastructure, practices or processes.

2. GENERAL INFORMATION SECURITY REQUIREMENTS

- a. Stanford University reserves the right to periodically audit the Vendor's global network and development center infrastructures to ensure compliance with the Stanford Information Security Policies and Standards. Non-intrusive network audits (basic port scans, etc.) may be performed randomly and without prior notice. Stanford University, or its agents, may conduct more intrusive network and on-site physical audits with, as little as, 24 hours notice.
- b. The Vendor must provide architecture documents that includes full network diagrams of current, and proposed, the Stanford University Application Environments, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where Stanford University data resides, the applications that manipulate it, and the security thereof.
- c. The Vendor must be able to immediately disable all or part of the functionality of the application should a security issue be identified. Vendor must provide Stanford the functionality to disable process for emergency, critical and normal security issues.
- d. Active Intrusion Detection Systems, (IDS) for both Host Systems and the Network. Vendor shall provide Stanford with lists of hardware and software used along with the maintenance process. The Vendor will not use home grown or freeware products unless Stanford is provided with as much as technical data necessary. The Intrusion Detection Response processes must include the Stanford notification processes. Stanford reserves the right to reject the usage of any Product or processes which Stanford feels does not meet their requirements.
- e. Information security incident response processes must be clearly defined and documented. Stanford requires a copy of the documented incident response processes be available on-site for inspection. Please ensure the processes cover policy, procedures and guidelines on security incident response; and details on incident classification (types-critical, emergency and normal). Please provide us with your Information Security Incident Response Guidelines or Polices. Historical statistics on incident events and responses for the last year shall also be available to Stanford.

3. INSPECTIONS & AUDITS

- a. Vendor shall maintain performance, accounting and related records resulting from or arising in connection with the terms and conditions of the Agreement during the Term and for six (6) years (or such longer period as may be required by law) after the expiration or termination of the Agreement.
- b. 2.11.2 During the Term and for six (6) years after the expiration or termination of the Agreement (or such longer period as may be required by law), Stanford, its auditors (including internal audit staff and external auditors), inspectors, regulators and other representatives as Stanford designate from time to time in writing, shall be entitled to enter to any Facility, and to view, copy and remove data and records relating to the Services and other duties and obligations of Vendor under the Agreement, for the purpose of performing audits, examinations and inspections of Vendor and any of its Third Party Vendors, including any audit or examination necessary to enable Stanford to meet applicable regulatory requirements, and for any other reasonable purpose, including without limitation: (i) to verify the accuracy of the Charges, and the invoices from Vendor to Stanford, hereunder; (ii) to verify the integrity and security of Stanford's or Vendor's (whichever applicable) data and the systems (including without limitation Facilities) that process, store, support and transmit that data; (iii) to examine Vendor's performance of the applicable Services; and/or (iv) to verify Vendor's compliance with the terms of the Agreement. Stanford shall use commercially reasonable efforts to conduct its audit activities so as not to materially disrupt Vendor's business operations or ability to perform the Agreement.
- c. Vendor shall conduct, at Stanford's request and expense and at time(s) agreed to by Stanford, a SAS 70 Type II audit by an independent accounting firm acceptable to Stanford of the operations of Vendor in relation to the Services and Vendor's compliance with this Agreement, including but not limited to Vendor's compliance with Section 4.1 and the Information Security Measures. The audit shall cover all Facilities and operations of Vendor involved in the provision of Services. The results of such audit shall be provided to Stanford, and shall be in a form acceptable to Stanford. At least once each calendar quarter, Vendor shall certify to Stanford in writing that Vendor maintains an adequate internal control structure and procedures for financial reporting that in all events are in compliance with US Laws.
- d. Does the OSP meet any certified standards? (Please list the certification standard met, e.g. BSO, ISO, CMM, VISA, PCI and who performed the certification.) The OSP shall provide Stanford copies of current and subsequent certifications. During the contract period, the OSP shall disclose to Stanford any material weaknesses, or deficiencies identified during audits on the Vendor facilities hosting, or data pathways, supporting Stanford projects.
- e. Vendor shall promptly correct at its expense any deficiency or other problem applicable to the Services or this Agreement found by any process, security, financial or other audit, examination or inspection conducted by Stanford or by Vendor. If any financial audit, examination or inspection reveals that Vendor's invoices for the audited period are not correct, Vendor shall promptly reimburse Stanford for the amount of any overcharges, with interest accrued from the date the incorrect payment was made until reimbursement, at the lesser of: (i) one and one-half percent (1.5%) per month or (ii) the maximum rate of interest allowed by applicable Law.

4. PHYSICAL SECURITY REQUIREMENTS

- a. The equipment hosting and supporting the Outsourced Development Center, (ODC), environments for Stanford University must be located in a physically secure facility, which requires badge access at a minimum.

- Production systems, including servers, firewalls, hubs, routers, and voicemail systems, shall be located within a physically secured area.
 - Information systems and communications equipment that require additional security shall be physically isolated to enhance the general level of protection.
 - To assure the continual service of critical production systems, management shall provide security controls that alert, monitor, and log intrusions, fires, explosives, smoke, water, dust, vibrations, chemical and electrical effects, electrical supply interferences, and electromagnetic radiation.
- b. The infrastructure (hosts, network equipment, etc.) hosting the Stanford University environments must be located in a locked cage-type environment.
 - c. Stanford University shall have final say on who is authorized to enter any locked physical environment, as well as access the Stanford University Application or Development Infrastructure.
 - d. The Vendor must disclose who amongst their personnel will have access to the environments hosting Stanford University's application and data.
 - e. Stanford University requires that the Vendor disclose their employee/contractor background check procedures and results prior to Stanford University granting approval for use of a Vendor.
 - f. Entry controls shall identify, authenticate and monitor all access attempts to restricted information processing areas within Vendor facilities.
 - g. Facility Identification – Access to any Vendor data center, network operations center, telecommunications or other similar information processing facility supporting Stanford University shall be restricted. Every person authorized to enter the facility, including visitors, shall be issued a facility identification badge that contains identifying information (such as name, photograph, and job position) and their level of building access. Badge color or some other bold identifier may be used to represent the level of access.
 - h. Badge Review - All badges shall be checked prior to entry. A receptionist, desk attendant, security guard or electronic card reader that logs the identity, time, date, and access privileges of each entry attempt may do such checking.
 - i. Physical Access to Sensitive Areas – Access to any office, computer room, or work area that contains sensitive information shall be physically restricted. Management responsible for the staff working in these areas shall consult with security administration to determine the appropriate access control method (receptionists, metal key locks, magnetic card door locks, etc.).
 - j. Securing Sensitive Information in Unattended Locations – Sensitive information, either in paper or electronic form, shall be protected from unauthorized access and disclosure. When such information is left in unattended locations, it shall be stored in safes, file cabinets, or other appropriate containers and locked away. During non-working hours, desks shall be cleared to prevent unauthorized access and disclosure of information.
 - k. Inspection of Luggage and Packages – Based on the nature and confidentiality of the information processed, users shall be advised that all luggage (e.g., briefcases and backpacks) and packages are subject to inspection before entry is permitted.
 - l. Access Accountability - All entry logs shall be secured and maintained. Users shall challenge anyone not wearing an identification badge. Access rights to secure areas shall be reviewed and updated regularly.

5. NETWORK SECURITY REQUIREMENTS

- a. Stanford University requires that the network hosting the application and development environments be segregated from any other corporate or customer network that the Vendor may have. Network segregation for the ODC shall be accomplished by implementation of a VLAN. This means the Stanford University ODC environments use separate hosts and separate infrastructure. Any shared technical infrastructure elements must be negotiated and approved by Stanford.
- b. Stanford University requires access to any security, traffic or authentication logs relating to the access and connectivity to the University's application and development environments.
- c. Data Path & Connectivity between Stanford University and the Vendor.
 - If Stanford University will be connecting to the Vendor via a private circuit (such as frame relay, etc.), then that circuit must terminate on the Stanford University extranet, and the operation of that circuit will come under the University's computing procedures, standards and policies.
 - If, on the other hand, the data between Stanford University and the Vendor will go over a public network such as the Internet, the Vendor must deploy appropriate firewall technology, and the traffic between Stanford University and the Vendor must be protected and authenticated by cryptographic technology (See Cryptography §3.8 below). Stanford University requires administrative access to any firewalls and/or routers on the University's side of the firewall infrastructure.
 - No "split-tunneling" of any secure connection between the Vendor and Stanford University application development environments.

6. HOST SECURITY REQUIREMENTS

- a. Stanford requires host systems (UNIX, Linux, Windows, etc.) comprising the ODC infrastructure that supports Stanford University be hardened against attack. This includes resetting default passwords and eliminating the running of unnecessary services on the servers. Stanford requires documentation of the hardening standards for all systems in the ODC.
- b. Vendor systems that are classified as "production-level" in the ODC are required to follow industry standard change management control processes. These processes include:
 - Approvals are required for system changes at the Operating System level, and this includes changes regarding security administration.
 - The services provided at the Operating System level shall be restricted to the minimum necessary services required for the purpose the systems are designed to perform.
 - The host systems must be reviewed for authenticity and proper directory structure before being placed in service in, or supporting, the ODC.
 - File systems of a production system that are application specific will contain some level of dynamic data. Periodic auditing dynamic data areas shall be performed for plausibility, e.g. the directory structures contain only the expected files with typical permissions.
 - Static application data areas (e.g. the static information used to populate a website outside of any dynamic data available) of the file system shall be governed by change management approval processes that involve the application owners.

- c. Stanford requires current listings of current patch levels on hosts, including host OS patches, web servers, databases, and any other material application used in the ODC.
- d. Stanford requires that the Vendor have documented policies and procedures for applying security patches on hosts and systems in, or supporting, the ODC. The change control processes shall include roll-back plans or strategies.
- e. An audit log shall be maintained of all updates to operational system files.
- f. Stanford requires that the Vendor document their processes for monitoring the integrity and availability of those hosts and systems in, or supporting, the ODC.
- g. Stanford requires documentation of the Vendor's password policies for the ODC systems and infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.
- h. Stanford University will not provide internal usernames/passwords for account generation, as Stanford is not comfortable with internal user/system passwords being in the hands of third parties. With that restriction, describe your process to authenticate users (e.g., LDAP, Netegrity, Client certificates) to the Stanford development environments and infrastructure.
- i. The Vendor must provide documentation regarding account generation, maintenance and termination process, for both maintenance as well as user accounts in the ODC. The documentation shall include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.
- j. Previous software versions shall be retained for contingency purposes.

7. DESKTOP SECURITY REQUIREMENTS – OPERATIONAL SOFTWARE CONTROLS

- a. Stanford requires desktop systems (UNIX, Linux, Windows, etc.) within the ODC infrastructure supporting Stanford University be hardened against attack. This includes resetting default passwords and eliminating the running of unnecessary services on the servers. Stanford requires documentation of the hardening standards for all systems in the ODC.
- b. Vendor desktop systems that are classified as "production-level" in the ODC are required to follow industry standard change management control processes. These processes include:
 - Approvals are required for system changes at the Operating System level, and this includes changes regarding security administration.
 - The services provided at the Operating System level shall be restricted to the minimum necessary services required for the purpose the systems are designed to perform.
 - The host systems must be reviewed for authenticity and proper directory structure before being placed in service in, or supporting, the ODC.
 - File systems of a production system that are application specific will contain some level of dynamic data. Periodic auditing dynamic data areas shall be performed for plausibility, e.g. the directory structures contain only the expected files with typical permissions.
 - Static application data areas (e.g. the static information used to populate a website outside of any dynamic data available) of the file system shall be governed by change management approval processes that involve the application owners.

- c. Stanford requires current listings of current patch levels on desktop systems, including host OS patches, web servers, databases, and any other material application used in the ODC.
- d. Stanford requires that the Vendor have documented policies and procedures for applying security patches on desktop systems in, or supporting, the ODC. The change control processes shall include roll-back plans or strategies.
- e. Stanford requires that the Vendor document their processes for monitoring the integrity and availability of the desktop systems contained in the ODC.
- f. Desktop systems in the ODC shall only hold operationally relevant applications and information.
- g. Previous software versions shall be retained for contingency purposes.

8. DISASTER RECOVERY AND BUSINESS CONTINUITY REQUIREMENTS

Vendor will comply with, and assist in the performance of any information technology aspects of, Stanford's disaster recovery and business continuity plans, as applicable to Vendor, with respect to any Disaster affecting Stanford's operations or Facilities.

- a. Vendor shall provide disaster recovery, business resumption, and business continuity services in the event of a Disaster as specified by Stanford and the OSP, as well as any applicable provisions of any Statements Of Work, and all applicable regulatory guidelines and requirements and Stanford's business recovery guidelines and requirements. Each Disaster Recovery Plan must be satisfactory to Stanford and must contain, among other things, a time frame for restoring Service, which shall not exceed a mutually agreed upon time-frame determined from the inception of a Disaster, or other outage, by Stanford and Vendor representatives as part of their initial incident response activities.
- b. Off-Site Facilities – The OSP shall maintain, and continue to maintain throughout the Term, off-site Disaster recovery capabilities that permit Vendor to implement its Vendor Disaster Recovery Plans and provide such Disaster services and to promptly recover from a Disaster and continue, after any Disaster or other comparable outage, to continue providing Services in accordance with the Agreement, including all Service Levels. Such capabilities shall include redundant systems and the use of geographically diverse backup and Facilities. Vendor also shall provide, as a component of its Vendor Disaster Recovery Plans, uninterrupted backup power supply to guard against electrical outages at the Vendor Facilities from which the Services are rendered and backup telecommunications lines to such Facilities, on independent circuits, to guard against telecommunications outages.
- c. Risk Assessments – Risk assessments shall be conducted and formally documented to assess the risks and their potential impacts to the organization. With each risk, an analysis of the likelihood of an event shall be determined and prioritized in such a manner so that methods of mitigation can be explored. Risk assessments shall include both technical and environmental threats to software (data and applications), hardware (including operating systems) and procedures. Risk assessments shall be reviewed annually and updated as required
- d. Impact Analysis - An impact analysis provides an understanding of the effect that an interruption will have on the organization. These shall include both long and short-term interruptions of minor and major incidents.
- e. Alignment to Business Strategy - Business continuity plans shall be created to support the organizations business objectives and priorities. This shall be reflected in procedures supporting application and data back-up requirements and procedures required for system restoration. Specific considerations to include in data back-up and testing shall include:

- Consistent implementation of data back-up for critical systems.
 - Standard back-up schedules.
 - Consistent data vaulting procedures.
 - Regular, formal back-up data integrity checks and test restorations, including data and related applications.
 - Service level agreements (SLAs) that identify responsibility for data, application and operating system back-up, restoration and testing.
 - Development of redundant technical infrastructures to eliminate single points of failure for data communications between systems and the ODC and Stanford.
 - Determination and selection of an alternative ODC, or processing facility.
- f. Testing and Updating Plan - Business continuity plans shall be tested annually to determine effectiveness. Schedules and times shall be based upon changes to the environment and training needs for the staff involved. Updates to the plans are necessary to keep information and processes accurate. Consideration shall be given to digitizing or duplicating irreplaceable Agency physical documentation for off-site archival.
- g. Management of the Plan - Business continuity must be supported at the appropriate level in the organization. Responsibilities for the plan will be distributed across the organization and therefore require senior level support. Management shall ensure that the organization's processes are incorporated into the structure of the plan.

9. DEVELOPMENT TOOLS REQUIREMENTS

- a. Stanford requires that the Vendor disclose any development and change management tools used in the ODC, and their version numbers.

10. QUALITY ASSURANCE & CODE REVIEW REQUIREMENTS

- a. Stanford requires that the Vendor provide documentation regarding their processes for performing security Quality Assurance testing. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.
- b. If the Vendor has external code reviews performed, including CGI, Java, etc, for the explicit purposes of location and remediation of security vulnerabilities, then Stanford requires information concerning the results of said review, including – who performed the review, the results, and what remediation activity has taken place. Stanford requires reasonable advance notice of any external code reviews on Stanford systems.

11. CRYPTOGRAPHY REQUIREMENTS

- a. Stanford will not accept the use of any “homegrown” cryptography. Any symmetric, asymmetric or hashing algorithm utilized by the Stanford University application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.
- b. Encryption algorithms must be of sufficient strength to equate to either, 168-bit Triple DES or 128-bit AES.
- c. Connections to the OSP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP.

12. STANFORD'S DEVELOPMENT ENVIRONMENT REQUIREMENTS

- a. Stanford's development environments will be locally hosted by Stanford.
- b. All development will be performed in Stanford's development environments.
- c. No data will be transferred to external development locations or centers.
- d. All development efforts will be performed in the same development environment. (i.e. Stanford's former practice of separate development environments for on-site vs. off-shore developers shall be halted).
- e. Distinct Environments shall be established for every development project. The development environments and architectures for each application shall be distinct from one another and mirror the production environment.

13. DATA SCRAMBLING IN NON-PRODUCTION ENVIRONMENTS

- a. Stanford can continue its traditional practice of utilizing copies of Production data in Development and Testing environments, provided that data privacy requirements can be met. Stanford currently scrambles sensitive data elements, data that Stanford is required to protect for legal and regulatory purposes. This data is classified as Category A, as defined in Stanford's Administrative Guide Memo #63.
 - PeopleSoft and Oracle Financials currently obfuscate sensitive data in the development environments.
 - Unit and initial functional testing are conducted in scrambled data, test environments.
 - User Acceptance and Fix/Patch environments contain unscrambled data.

14. OUTSOURCED DEVELOPMENT CENTER (ODC) INFRASTRUCTURE

- a. Stanford requires a distinct ODC maintained by the vendor. All development activity is performed inside the ODC, (no remote access to the ODC). This environment shall be isolated from the vendor's corporate network.
 - Physical access controls – Proximity card access required, limited to Stanford project team. Initial phase of project shall require restricting access to Stanford's ODC to Vendor personnel with building level access. The Stanford ODC proximity card restriction will be established after approval from Stanford. Vendor will share the cost impact of such an infrastructure based on Stanford's requirements.
 - Visitor Sign-in Log – to document access to Stanford's ODC by non-project members.
 - Access control and visitor logs available to Stanford.
 - Upon commencement of initial projects, the ODC network shall be separated from the Vendor's corporate network by a single firewall. The Vendor shall provide Stanford a list of desktop applications installed on ODC computers that require access to the corporate network, (typically Anti-Virus, Operating System patching or project administration applications) along with the firewall rule set necessary for proper functionality of these applications. These desktop applications and firewall rules shall be implemented upon approval by Stanford. No other external connections shall be allowed to/from the ODC network.
 - Upon request by Stanford, the ODC network shall be separated from the corporate network by a pair of firewalls. Stanford will control the firewall facing the vendor's corporate network and the vendor will control the firewall facing the ODC. The Vendor shall provide Stanford a list of

desktop applications installed on ODC computers that require access to the corporate network, (typically Anti-Virus, Operating System patching or project administration applications) along with the firewall rule set necessary for proper functionality of these applications. These desktop applications and firewall rules shall be implemented upon approval by Stanford. No other external connections shall be allowed to/from the ODC network.

- No email or Web servers are housed on the development network.
- Physical and network access to the ODC is managed by the Engagement and Project Managers. Stanford must be notified of all changes in personnel and/or responsibilities in a timely manner.

15. STANFORD-TO-ODC CONNECTIVITY REQUIREMENTS

- a. Stanford requires a secure means of connectivity between the Development environments located on the Stanford campus and the Vendor's ODC. The ranking of connectivity preferences are as follows (in descending order):
 - Direct, distinct connectivity between the Stanford and outsourced development centers. The off-shore developers will only have access to the Stanford network, and in essence will reside on a virtual extension of Stanford's network, (and are separately cabled). The ODC workstations would not have any other connectivity to the vendor's corporate network. Any external connectivity would be through Stanford. Developers with vendor corporate connectivity requirements would require separate network or connectivity.
 - MPLS (with redundant routing) would be the second choice for full-scale, off-shore efforts. This "transparent virtual LAN service" would enable large numbers of connections with high bandwidth requirements, and possible VOIP connectivity. Off-shore developers would have access to their corporate intranet and network project management tools. External connectivity to the public Internet could be discussed.
 - Site-to-Site VPN would be the preferred initial configuration. The initial stages of the off-shore effort will not require high-bandwidth, nor require large numbers of developer connections to Stanford. Off-shore developers shall have access to their corporate intranet and network project management tools. External connectivity to the public Internet could be discussed. This VPN could remain after migration to MPLS or direct networking as a back-up, or redundant connection.
 - Client-based VPN, either through the leased line, or the public Internet could also be used as a back-up connectivity method. Off-shore developers will not have simultaneous access to their corporate intranet and network project management tools. External connectivity to the public Internet would not be available while connected. This VPN would also be used by vendor personnel with privileged access.

16. PHASING-IN OF VPN REQUIREMENTS

- a. The outsourcing contract has a phased transition/implementation plan; the VPN requirements can migrate to meet the data throughput demands of each phase:
 - Initial Phase of off-shoring will utilize the site-to-site VPN. There are not sufficient connections or throughput requirements to justify MPLS or direct connections.

- Prior to Phase II, the connectivity requirement shall be reevaluated to determine if an MPLS or direct connection solution be implemented.

17. ROLE DEFINITIONS

- a. Stanford requires that there be clearly defined roles and responsibilities of all team members, both on-site and off-site project team members. (e.g. Business Analysts, Designers, Developers, Support Analysts, Testers and User Testers.)

18. PERSONNEL SECURITY REQUIREMENTS

- a. Employee/Contractor Screening – Stanford requires that background and employment verification checks be conducted as part of the employment/engagement process for both full- and part-time employees and contractors. Such checks shall be repeated periodically in cases of job change, role change, or promotion. (Please see Section 4.2 of the Master Service Agreement.)

Personnel screening checks must include one or more of the following, depending on the particular job duties, responsibilities, and access privileges of the position:

- Character references (business and personal, as appropriate).
- Training background.
- Academic and professional experience.
- Identity and background checks.
- Credit checks, when appropriate.

The sourcing Agency for contractors, consultants, and third-party vendors shall use similar criteria in screening processes, to include:

- Initial screening.
- Job-specific screening, if sensitive areas are to be accessed.
- Notification of re-screening, as required.

- b. Employee/Contractor Supervision - Managers and supervisors shall evaluate the procedures required for personnel that may be accessing sensitive information. These procedures shall be reviewed and updated by senior management or staff, as necessary.
- c. Confidentiality Agreements – Confidentiality and non-disclosure agreements must indicate that certain information is private or secret. Employees who need to access such information shall be required to sign these agreements when initially employed. Third-party users who are not already covered by an existing agreement shall also sign such agreements prior to being given access to the information. (Please see Section 8 of the Master Service Agreement).
 - Confidentiality and non-disclosure agreements shall be reviewed regularly, especially when employees leave the organization or when contracts expire.
- d. Terms and Conditions of Employment - Terms and conditions of employment shall clearly state the employee's responsibilities for information security. They shall include a defined period of time after employment and the actions that will be taken in the event of non-compliance to the agreement.

19. VIRUSES

- a. Each Party shall take commercially reasonable measures to prevent the introduction of Viruses into the Software, network, computer systems or operating environments used by

it. Both Parties shall continue to perform and maintain at least the Virus protection and correction procedures and processes in place at the Facilities prior to the Execution Date of each SOW, and continue to review, analyze and implement improvements to and upgrades of such Virus prevention and correction programs and processes that are commercially reasonable and consistent with information technology industry standards. If OSP introduces a Virus into the Software, network, computer systems or operating environments used by Stanford, Stanford may take any and all steps and actions that it deems reasonable and appropriate to locate and stop propagation of the Virus; cleanse or otherwise entirely remove the Virus from the Software, network, computer systems or operating environments used by Stanford and its Affiliates; and to counteract and eliminate the effects of the Virus on Stanford and its Affiliates and end users, at OSP's expense.

20. INFORMATION BACK-UP REQUIREMENTS

- a. Stanford requires that back-up copies of essential electronically-stored business data are routinely created and properly stored and that procedures and facilities for restoring such data are prepared and tested.
- b. Back-ups of all essential business data must be routinely created and properly stored to ensure prompt restoration. Specific considerations to include in data back-up and testing shall include:
 - Consistent implementation of data back-up for critical systems.
 - Standard back-up schedules, with at least 3 cycles of back-ups retained for critical business systems.
 - The retention period for essential data and special requirements for permanent archives shall be defined as required.
 - Consistent data vaulting procedures for both, on-site (ODC) and off-site storage of back-ups in appropriately physically and environmentally protected sites.
 - Regular, formal back-up data integrity checks and test restorations, including data and related applications.
 - Back-up media must be regularly tested to ensure that they can be reliably restored.
 - Service level agreements (SLAs) that identify responsibility for data, application and operating system back-up, restoration and testing.
 - Determination and selection of an alternative ODC, or processing facility.

21. MEDIA HANDLING REQUIREMENTS – DISPOSAL OF MEDIA

- a. Stanford requires that the Vendor have documented policies and procedures governing the secure disposal of media. When media is worn, damaged or otherwise no longer required, it must be disposed of in a secure manner to prevent the compromise of sensitive information through careless or inadequate media disposal processes. The following considerations shall be included in the documented media disposal procedures:
 - Items which may require secure disposal include paper documents, recordings, output reports, magnetic tapes, printers, faxes, copiers, removable disks or cassettes, optical storage media, program listings, test data, and system documentation.
 - Media containing sensitive information shall be disposed of by secure incineration or shredding.
 - If the magnetic or optical media is to be reused, it shall be completely emptied of data and prepared by special software designed to securely erase and/or reformat the media.

- Care shall be taken when selecting a media disposal contractor to ensure adequate security control and experience.
- A log shall be maintained of the disposal of all sensitive items so as to provide an audit trail.
- Consideration shall be given to the extra risks associated with accumulating a large volume of media prior to disposal. In large quantities, it may be more difficult to detect missing items.

22. SYSTEM MONITORING REQUIREMENTS

- a. Stanford requires that the Vendor have a formal, documented monitoring process to facilitate the discovery of attempts at unauthorized access or activity. Stanford requires that these logs be kept and reviewed in sufficient detail to detect activity atypical to the local environment.
- b. System Monitoring Risk Assessment – Stanford requires a risk assessment be performed to determine the types of monitoring needed to provide reasonable assurance of the systems’ integrity. The following criteria shall be assessed:
 - Authorized access including –
 - User ID
 - Date and time of key events
 - Types of events
 - Files or resources accessed
 - Programs, utilities and applications
 - Privileged Operations –
 - Use of supervisor (or administrator) accounts
 - System start-up and shutdown
 - I/O device attachment or detachment
 - Unauthorized access attempts –
 - Failed attempts
 - Access policy violations and notifications of network, gateways and firewalls
 - Alerts from proprietary intrusion detection systems
 - System alerts or failures, such as –
 - Console alerts or messages
 - System log exceptions
 - Network management alerts
- c. Stanford requires following types of events to be monitored and logged:
 - Logon Monitoring – A user event logging system shall be utilized and, at a minimum, contain the following information:
 - User ID
 - Dates and times of user logon and logoff
 - Logon method, location, terminal identity (if possible) and network address
 - Records of successful and unsuccessful system access attempts
 - Records of successful and rejected data access, and other resource access attempts.
 - Data Access Events - Where specific applications produce access event logs in addition to the system access logs the two logs shall be archived in such a way as to make cross correlation possible.
- d. Review of Monitoring Logs – Stanford requires that the log files produced by the monitoring systems shall be reviewed on a periodic basis to determine if illicit activity has occurred. The log files shall be secured in such a manner as to prevent unauthorized alterations of the log files.

- e. Log Archiving – Stanford requires that the Vendor have documented policies for the retention of logs. The length of retention shall reflect the availability of resources and the need to track historical information. The retention of logs shall also reflect the possibility of providing evidence in future investigations. The storage and access to the logs shall be sufficient to meet the requirements of evidence collection.

23. PASSWORD MANAGEMENT SYSTEM REQUIREMENTS

- a. Stanford requires that the Vendor have sufficient capabilities for password management to provide sufficient password security for computing resources for all Stanford projects.
- b. Password Testing – The Vendor’s Information Security Officer shall ensure that all password files used within the Stanford ODC undergo periodic reviews to determine password vulnerability. The results of these password reviews, and any remediation activities, must be communicated to Stanford’s Information Security Office in a timely manner.
- c. Physical Password Security – Within the Stanford ODC, the ability of general users to access the files containing passwords shall be limited. Password file access shall be monitored for unauthorized activity.
- d. Password Management Best Practices –
 - User passwords shall be unique to the individual and accessible for accountability.
 - Provide for creating high quality passwords.
 - Allow users to create their own passwords and include a confirmation method for possible input errors.
 - Where users maintain their own passwords, enforce password change schedules and password policies.

24. INFORMATION SECURITY DRIVERS

- a. Many of the applications and systems considered for this contract contain sensitive and private information which the University is required to protect. Stanford must maintain its ability to ensure tight controls over the development environments and the information contained the development databases.
- b. Information Security Drivers — Stanford University is committed to protecting its information resources from accidental or intentional intrusion or damage and is equally committed to preserving and nurturing the open, information-sharing requirements of its academic culture. Protecting information assets is driven by a variety of considerations including legal, academic, financial and other business requirements.
 - Legal — There are laws, both federal (e.g., HIPAA, FERPA) and state (e.g., social security number use, credit card exposure), that affect the level of protection Stanford is required to provide. Stanford also has many contractual relationships around the protection of data that is licensed from other sources.
 - Academic — Stanford both produces and owns intellectual capital, which must be protected against premature disclosure, or unauthorized tampering.
 - Financial — there are costs directly related to the protection of information assets. Similarly, there are costs directly related to the control and repair of damage to information resources that have been compromised.
 - Other business requirements — While Stanford, as a part of its fundamental mission, wants to make sure that many information resources are widely

available it also wants to keep private things private. Moreover, in addition to the direct costs related to damage control, Stanford's reputation as a world class institution is something that, if damaged, can have both direct and indirect negative effects.

c. Additional information can be obtained from:

- Stanford University Administrative Guide Memos (Policies) on Computing — <http://adminguide.stanford.edu/ch6contents.html>
- Data Classification – Matrix regarding Stanford University's Data Classification Schema described in Administrative Guide Memo No. 63, Information Security and in Appendix A of the RFP — http://securecomputing.stanford.edu/data_classification.pdf
- Information Security: Guidelines for Applications — [https://docushare.stanford.edu/Get/File-21682/General Recommendations for Application Security.pdf](https://docushare.stanford.edu/Get/File-21682/General_Recommendations_for_Application_Security.pdf)