# Appendix G

**IT SECURITY CONTROLS**

If selected through this RFP process respondent shall provide an initial Security Controls Report in the form attached hereto prior to executing an agreement with LACERA. All subsequent Security Controls Reports that are required after this first report shall be performed and submitted annually. The questionnaires are to focus on security as it applies to the technologies impacting services provided in relation to the scope of work. If a control is found to be inadequate, respondent will develop a remediation plan within 30 days. Respondent will implement the plan and inform LACERA of the change within a mutually agreed upon and reasonable time.

The Security Controls Reports shall report in writing on the respondent’s system(s) and the suitability of the design and operating effectiveness of controls, information functions, and/or processes applicable to the environment in which the respondent receives and maintains LACERA records, including the security requirements.

Respondent shall provide to LACERA, within 30 calendar days of the issuance of each Security Controls Report, a documented corrective action plan that addresses each audit finding or exception contained therein. The corrective action plan shall show in detail the required remedial action by respondent along with the implementation date(s) for each remedial action.

If respondent does not obtain an annual Security Controls Report, LACERA shall have the right to retain an independent audit firm to perform such an audit engagement for such a report. The audit will include the controls, information functions, and processes used or provided by respondent. Respondent agrees to allow the independent audit firm to access its facilities for purposes of conducting this audit engagement. They will provide the necessary support and cooperation to the independent audit firm.

The independent audit firm will be engaged by LACERA’s legal department and subject to the same confidentiality requirements supported in this agreement, and any disclosure will be on a need-to-know basis only for the purpose of the Security Controls Report. LACERA will invoice respondent for the expense of the report(s) or deduct the cost from future payments to the respondent.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IT Security Controls - LACERA Environment** | | | | |
| **Control Section** | **Control Name** | **Control Description** | **Control Validation Test/ Review Performed** | **Control Validation Results** |
| **Access Control** | Access control policy | An access control policy shall be established, documented, and reviewed based on business and information security  requirements. |  |  |
| Access to networks and network services | Users shall only be provided  with access to the network and network services that they have been specifically  authorized to use. |  |  |
| User registration and de- registration | A formal user registration  and de-registration process shall be implemented to  enable assignment of access rights. |  |  |
| User access provisioning | A formal user access  provisioning process shall be implemented to assign or revoke access rights for all  user types to all systems and services. |  |  |
| Review of user access rights | Asset owners shall review  users’ access rights at regular intervals. |  |  |
| Removal or adjustment of access rights | The access rights of all  employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon  change. |  |  |
| Use of password information | Users shall be required to  follow consultant's practices in the use of password information. |  |  |
| Secure log-on procedures | Where required by the  access control policy, access to systems and applications shall be controlled by a  secure log-on procedure. |  |  |
| Password management | Password management systems shall be interactive and shall ensure quality passwords. |  |  |
|  | | | | |
| **Physical and Environmental Security** | Physical security perimeter | Security perimeters shall be defined and used to protect areas that contain either sensitive, critical information or information processing  facilities. |  |  |
| Physical entry controls | Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel  are allowed access. |  |  |
| Protecting against external and environmental threats | Physical protection against natural disasters, malicious  attacks, or accidents shall be designed and applied. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Supporting utilities | Equipment shall be protected from power failures and other disruptions caused by  failures in supporting utilities. |  |  |
| Equipment maintenance | Equipment shall be correctly maintained to ensure its continued availability and  integrity. |  |  |
| **Network Security Management** | Network controls | Networks shall be managed and controlled to protect information in systems and  applications. |  |  |
| Security of network services | Security mechanisms,  service levels, and management requirements of all network services shall be identified and included in network services agreements, whether these  services are provided in- house or outsourced. |  |  |
| Information transfer policies and procedures | Formal transfer policies,  procedures, and controls shall be in place to protect the transfer of information using all types of  communication facilities. |  |  |
| **Operational** | Documented operating procedures | Operating procedures shall be documented and made available to all users who  need them. |  |  |
| Change management | Changes to consultant, business processes, information processing facilities and systems that affect information security  shall be controlled. |  |  |
| Capacity management | The use of resources shall be monitored and tuned, and projections made of future capacity requirements to ensure the required system  performance. |  |  |
| Controls against malware | Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with  appropriate user awareness. |  |  |
| Information backup | Backup copies of information, software, and system images shall be taken and tested regularly in  accordance with an agreed backup policy. |  |  |
| Event logging | Event logs recording user activities, exceptions, faults, and information security events shall be produced,  kept, and regularly reviewed. |  |  |
| Protection of log information | Logging facilities and log information shall be protected against tampering  and unauthorized access. |  |  |
| Clock Synchronization | The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single  reference time source. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Management of technical vulnerabilities | Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, consultant's exposure to such vulnerabilities evaluated and appropriate measures taken to address  the associated risk. |  |  |
|  | | | | |
| **Information Security Incident Management** | Responsibilities and procedures | Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information  security incidents. |  |  |
| Reporting information security events | Information security events shall be reported through appropriate channels as  quickly as possible. |  |  |
|  | Reporting information security weaknesses | Employees and contractors using consultant's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or  services. |  |  |
|  | Response to information security incidents | Information security incidents shall be responded to in  accordance with the documented procedures. |  |  |
| Learning from information security incidents | Knowledge gained from  analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future  incidents. |  |  |