# **INFORMATION SECURITY REQUIREMENTS**

Each Proposal must include detailed information that clearly describes how Company will meet the following Information and Security requirements.

In fulfilling its obligations, Company may be granted temporary access to networks, systems, and/or data of the District and be entrusted with the security and confidentiality of the District’s systems, records, and information. When such access is granted, Company (and any subcontracted personnel and agents) are to adhere to the following requirements:

1. Unauthorized use or access to the District’s system records and information is prohibited.
2. Access granted under this request is only for fulfillment of obligations under this Agreement.
3. Access will be only for the term of the Agreement. Thereafter, all accounts, passwords, and access associated with this Agreement will be revoked immediately.
4. If system administrator rights are granted, they will apply only to the specific actions authorized. Performance of any unrelated and/or unauthorized actions may, at the District’s sole discretion, result in the immediate termination of access and termination of this Agreement.
5. To maintain account and password security, disclosure of any account information and passwords is prohibited.
6. Exhibiting or divulging the contents of any record or report to any person, or otherwise, is prohibited except in the performance of authorized duties and responsibilities.
7. Using any information accessed under any given request for gender and/or ethnicity-based recruiting/selections, unauthorized fund raising, or other barred activities are prohibited.
8. Personally benefiting or allowing others to benefit from any confidential information or other information gained by virtue of network or system access is prohibited.
9. Directly or indirectly causing the inclusion of any false, inaccurate, or misleading entries into any records or reports is prohibited.
10. Except as specifically authorized under this Agreement, no record or report or copy thereof, whether paper or electronic, may be removed from the office where it is maintained without written authorization from the District’s authorized personnel.
11. All systems must be completely exited before leaving a computer or server unattended.
12. Industry-accepted security standards for access, use, retention, and disposal of information must be maintained.
13. Company will protect any accessed confidential information no less rigorously than it protects its own/customers’ confidential information.
14. Company will hold confidential information in strict confidence, and will access information only for the explicit business purposes outlined this Agreement.
15. Company will ensure compliance with the protective conditions outlined in this Agreement.
16. Company will return or securely destroy all confidential information upon expiration or termination of this Agreement.
17. Company agrees and understands that violation of security precautions to protect confidential information may be a crime and subject to appropriate legal action and/or criminal prosecution.
18. Company will notify the District immediately upon the termination of any individual involved in providing Services so that account access, passwords, remote diagnostic access, or other forms of access can be revoked.
19. Company will not aid, or act in conspiracy with, anyone to violate any of the requirements listed above.
20. Contractor may (1) create, (2) receive from or on behalf of District, or (3) have access to, records or record systems (collectively, "District Records·). Among other things, District Records may contain social security numbers, credit card numbers, or data protected or made confidential or sensitive by applicable federal, state and local, laws, regulations, and ordinances, including the Gramm Leach Bliley Act (Public Law No: 106-102), the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA”). If DISTRICT Records are subject to FERPA, (1) District designates Contractor as a District official with a legitimate educational interest in District Records, and (2) Contractor acknowledges that its improper disclosure or re-disclosure of personally identifiable information from District Records will result in Contractor's exclusion from eligibility to contract with District for at least five (5) years. Contractor represents, warrants, and agrees that it will: (1) hold District Records in strict confidence and will not use or disclose District Records except as (a) permitted or required by a signed contract, (b) required by law, or (c) otherwise authorized by District In writing; (2) safeguard District Records according to commercially reasonable, administrative, physical and technical standards such as standards established by (i) the National Institute of Standards and Technology and (ii) the Center for Internet Security, the Gramm-Leach­ Bliley Act, as well as the Payment Card Industry Data Security Standards that are no less rigorous than best practices in the data security industry; (3) continually monitor its operations and take any action necessary to assure that District Records are safeguarded and the confidentiality of District Records is maintained in accordance with all applicable federal, state and local, laws, regulations, and ordinances, including FERPA and the Gramm-Leach Bliley Act, and the terms of a signed contract; and (4) comply with the District's rules, policies, and procedures regarding access to and use of District's computer systems. Contractor represents, warrants and certifies that it complies with District's Policies on lnformation Security, including, without limitation, the following Board Policies:

<http://pol.tasb.org/Policy/Download/358?filename=CR(LOCAL).pdf>

<http://pol.tasb.org/Policy/Download/358?filename=CR(REGULATION).pdf>

<http://pol.tasb.org/Policy/Download/358?filename=CS(LOCAL).pdf>

<http://pol.tasb.org/Policy/Download/358?filename=CS(REGULATION).pdf>

1. At the request of District, Contractor agrees to provide District with a written summary of the procedures Contractor uses to safeguard and maintain the confidentiality of District Records.
2. Contractor agrees to provide District a copy of the Contractor’s Payment Card Industry – Data Security Standard (PCI-DSS) Attestation of Compliance and Statement of Scope.
3. Contractor must provide insurance coverage for IT Professional and/or Cyber Liability.  Coverage shall be sufficiently broad to respond to the duties and obligations undertaken in an agreement and shall include, but not limited to, claims involving infringement of intellectual property, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security.  The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.
4. **Notice of Impermissible Use**. If an impermissible use or disclosure of any District Records occurs, Contractor will provide written notice to District within one (1) business day after Contractor's discovery of that use or disclosure. Contractor will promptly provide District with all information requested by District regarding the impermissible use or disclosure.
5. **Return of District Records**. Within thirty (30) days after the expiration or termination of a signed contract, Contractor will make commercially reasonable efforts, for District Records created or received from or on behalf of District, will be (1) returned to District, with no copies retained by Contractor; or (2) if return is not feasible, destroyed. Twenty (20) days before destruction of any District Records, Contractor will provide District with written notice of Contractor's intent to destroy District Records. Within five (5) business days after destruction, Contractor will confirm to District in writing the destruction of District Records.
6. **Disclosure.** If Contractor discloses any District Records to a permitted subcontractor or agent, Contractor will require the permitted subcontractor or agent to comply with the same restrictions and obligations as are imposed on Contractor by this Section.
7. **Press Releases.** Except when defined as part of the Services, Contractor will not make any press releases, public statements, or advertisement referring to the Project or the engagement of Contractor as an independent contractor of District in connection with the Project, or release any information relative to the Project for publication, advertisement or any other purpose without the prior written approval of District.
8. **Public Information.** District strictly adheres to all statutes, court decisions and the opinions of the Texas Attorney General with respect to disclosure of public information under the Texas Public Information Act ("TPIA"), Chapter 552, Texas Government Code. In accordance with Section 552.002 of TPIA and Section 2252.907, Texas Government Code, and at no additional charge to District, Contractor will make any information created or exchanged with District pursuant to a contract (and not otherwise exempt from disclosure under TPIA) available in a format reasonably requested by District that is accessible by the public.