TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS
TDHCA Governing Board Approved Draft of
10 TAC §1.25 ("Information Security and Privacy Requirements for Contractors")

Disclaimer

Attached is a draft of **10 TAC §1.25 ("Information Security and Privacy Requirements for Contractors")** that was approved by the TDHCA Governing Board on April 27, 2017. This draft incorporates changes made by the Board as a result of public comment at the meeting. This document, including its preamble, is scheduled to be published in the May 12, 2017 edition of the *Texas Register* and that published version will constitute the official version for purposes of public comment. The version herein is informational only and should not be relied upon as the basis for public comment.

Public Comment

Public Comment Period: Starts: 8:00 a.m. Austin local time on May 12, 2017; Ends: 5:00 p.m. Austin local time on June 12, 2017.

Comments received after 5:00 p.m. Austin local time on June 12, 2017 will not be accepted.

Written comments may be submitted in hard copy or by email to:

Texas Department of Housing and Community Affairs
Attn: Jeff Pender
P.O. Box 13941
Austin, Texas 78711-3941
Email: jeff.pender@tdhca.state.tx.us

Comments may be submitted only within the designated public comment period. Those making public comment are encouraged to reference the specific draft rule, policy, or plan related to their comment as well as a specific reference or cite associated with each comment.

Please be aware that all comments submitted to the TDHCA will be considered public information.

TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS
Street Address: 221 East 11th Street, Austin, TX 78701
Mailing Address: PO Box 13941, Austin, TX 78711-3941
Main Number: 512-475-3800 Toll Free: 1-800-525-0657
Email: info@tdhca.state.tx.us Web: www.tdhca.state.tx.us

Texas Administrative Code

TITLE 10	COMMUNITY DEVELOPMENT
PART 1	TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS
CHAPTER 1	ADMINISTRATION
SUBCHAPTER A	GENERAL POLICIES AND PROCEDURES
RULE §1.25	Information Security and Privacy Requirements for Contractors

The Texas Department of Housing and Community Affairs (the "Department") proposes new 10 TAC §1.25, concerning information security and privacy requirements for Contractors, and the repeal of 10 TAC §1.24, concerning Protected Health Information, and 10 TAC §5.18, concerning information technology security practices. The purpose of this proposed new section is to protect the privacy and security of protected information belonging to individual customers and beneficiaries of the department's programs by requiring contractors who deal with such information to meet certain requirements when communicating directly with the department's information systems, or when they store, create or otherwise possess such information on their own information systems. The purpose of the repeals is to remove largely redundant regulations that will no longer be needed because of the proposed new rule.

FISCAL NOTE. Timothy K. Irvine, Executive Director, has determined that, for each year of the first five years the new rule and repeals will be in effect, enforcing or administering the new rule and repeals will reduce the likelihood of having to bear costs associated with the loss or theft of protected information.

PUBLIC BENEFIT/COST NOTE. Mr. Irvine also has determined that, for each year of the first five years the new section and repeals will be in effect, the public benefit anticipated as a result of the new section will be greater security of the personal information of our customers and beneficiaries in the hands of contractors who have access to the department's protected information.

ADVERSE IMPACT ON SMALL OR MICRO-BUSINESSES. The Department estimates that there are less than twenty small or micro-businesses that do business with the Department directly, or as a subcontractor, that would meet the definition of a small or micro-business found in Tex. Gov't code §2006.001 of the Texas government Code, and that would be subject to this new rule.

The economic impact of this rule is projected to be minimal. The Department has two rules in effect that already require certain financial and health information protections; 10 TAC §1.24 concerning protected health information, and 10 TAC §5.18 concerning information technology security practices. These two rules already require many of the information security and privacy protections proposed in the new rule. The new rule simply states more completely and clearly the requirements mandated in the underlying state and federal information security and privacy laws.

The most likely additional costs to be incurred by regulated parties who are small and micro-businesses include maintaining written policies, responding to requests for documentation of the regulated entity's compliance with the rule, and documentation of compliance by subcontractors who access the Department's protected information. Regulated small and micro-businesses should already be complying with the other relevant requirements in the new rule.

In preparing this rule, the Department considered alternative methods for achieving the purposes of the rule. As originally drafted all provisions applied to all regulated entities regardless of size or capacity. The rule was rewritten to make clear that only certain requirements applied to all regulated entities, while others applied only to organizations with more complicated computing

networks. The rule also includes a provision that would allow a contractor to work with the Department in minimizing the protected information the entity would need to access for the purpose of minimizing labor/professional costs associated with meeting the requirements under the new rule. In general, the Department believes it has minimized the rule requirements, and restricted their applicability to minimize impact to regulated entities, without jeopardizing the statutory goals of protecting the economic welfare of the Department's customers.

REQUEST FOR PUBLIC COMMENT. Written comments may be submitted to the Texas Department of Housing and Community Affairs, Jeffrey T. Pender, Rule Comments, P.O. Box 13941, Austin, Texas 78711-3941, or by email to: jeff.pender@tdhca.state.tx.us. **ALL COMMENTS MUST BE RECEIVED BY 5:00P.M. on June 12, 2017.**

STATUTORY AUTHORITY. The new section and repeals are proposed pursuant to Tex. Gov't Code §2306.053 which authorizes the Department to obtain, retain and disseminate records and other documents in electronic form and to adopt and enforce rules. More specifically, 10 TAC §202.24 requires state agencies to develop an information security program. The proposed repeals and new section affects no other code, article, or statute.

§1.25. Information Security and Privacy Requirements for Contractors

(a) Statement of Purpose

In order to assure the security and privacy of information submitted to the Department by persons seeking financial or other assistance, the Department must not only implement its own information security and privacy measures, but make sure those Contractors of the Department that may gain access to Protected Information under contracts, or otherwise, with the Department, adopt and implement appropriate strategies. The purpose of this rule is to identify measures that may be required by Department Contractors accessing Protected Information on behalf of the Department. Although all requirements in this rule generally apply to every Contractor possessing Protected Information on behalf of the Department, the scope and complexity of each Contractor's specific security and privacy measures will vary depending on the size of the organization and risks presented by Contractor's operations.

(b) Definitions

The following capitalized words and terms have the meaning given below unless the context clearly indicates otherwise.

(1) Computing Device means any personal computer, laptop, server, smart phone, or any other data processing device that is used to connect to the Department's network.

(2) Contractor means a third party, including but not limited to, auditors, outside counsel, funding agencies, Vendors or Subrecipients, including any and all of its Representatives, that may gain access to Protected Information on account of its relationship with the Department.

(3) Department means the Texas Department of Housing and Community Affairs.

(4) Financial Statements of a Tax Credit Applicant means a formal statement of the financial activities of a Low Income Housing Tax Credit Applicant, submitted to the Department as part of a Low Income Housing Tax Credit Application, including but not limited to, the balance sheet, income statement, cash flow statement or changes in equity. (Tex. Gov't. Code §2306.6717(d)(Public Information and Hearings)).

(5) Information Resources means the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

(6) ISP Agreement means an agreement between the Department and Contractor implementing information security and privacy requirements.
(7) Non-Public Personal Information means personally identifiable financial information provided by an individual in connection with applying for or receiving a financial product or service, unless the information is otherwise publically available. (Graham-Leach-Bliley Act (15 USC §§6801-6809 and 6821-6827)).
(8) Personal Identifying Information means information that alone or in conjunction with other information identifies an individual, including an individual's name, Social Security number, date of birth, or government-issued identification number, mother's maiden name, unique biometric data including fingerprint, voice print, retina or iris image, unique electronic identification number, address, or routing code, and telecommunication access devices as defined by Tex. Penal Code §32.51. (Tex. Bus. & Com. Code Chapter 521 (Unauthorized Use of Identifying Information)).
(9) Personal or Business Financial Information means any personal or business financial information including, but not limited to, Social Security numbers, tax payer identification numbers, or bank account numbers submitted to the Department to receive a loan, grant, or other housing assistance by a housing sponsor, individual or family. (Tex. Gov't. Code §2306.039 (Open Meetings and Open Records)).
(10) Protected Health Information means any information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. (45 CFR §160.103).
(11) Protected Information means Protected Health Information, Personal Identifying Information, Sensitive Personal Information, Personal or Business Financial Information, Non-Public Personal Information, Financial Statement of a Tax Credit Applicant, or WAP Applications and Participation Information
(12) Representative means any officer, employee, contractor, subcontractor, member, director, advisor, partner, or agent of Contractor, or any person serving in such a role, however titled or designated.
(13) Sensitive Personal Information means an individual's first name or first initial and last name in combination with any one or more of the following items if the name and items are not encrypted: (1) social Security number, (2) driver's license or government-issued identification number, (3) account or credit/debit card number in combination with any required security code, access code, or password that would permit access, or (4) information that identifies or reveals an individual and the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual. The term does not include publicly available information that is lawfully made publicly available. (TEX. BUS. & COM. CODE Chapter 521 (Unauthorized Use of Identifying Information)).
(14) Subrecipient means an organization with whom the Department contracts, and entrusts to administer federal or state program funds, including but not limited to, units of local government, nonprofit and for-profit corporations, administrators, community action agencies, collaborative applications, sub-grantees, developers, land banks, participating mortgage lenders and non-profit owner-builder housing providers.
(15) Vendor means a person or organization that supplies goods or services, properly procured under relevant laws, to the Department.
(16) WAP Applications and Participation Information means any specifically identifying information related to an individual's eligibility application for WAP or the individual's participation in WAP, such as name, address, or income information. (Weatherization Program Notice 10-08, U.S. Department of Energy, issued February 1, 2010).

(c) General Requirements

(1) Contractors that have entered into agreements with the Department that may result in Contractor having access to Protected Information shall enter into an ISP Agreement with the Department. The ISP Agreement shall be in a form provided by the Department, and shall be effective with respect to all current and future contracts that Contractor has with the Department for as long as the Contractor has access to Protected Information under those contracts. No new contract with the Department that may result in access to Protected Information may be implemented until there is an ISP Agreement in effect with the Department.

(2) Contractors that currently have access to Protected Information shall enter into an ISP Agreement with the Department as soon as is practical, but no later than 30 days after notification by the Department that an ISP Agreement is necessary.

(3) Department staff may work with Contractor to identify and reduce the number of classes of Protected Information implicated under a contract, and the related security and privacy protections required.

(4) The ISP Agreement shall include, among other requirements:

(A) security measures for devices that connect to the Department network, and

(B) security measures for maintenance of Department information external to the Department network, including, but not limited to:

(i) maintaining an inventory of all information technology ("IT") assets,
(ii) implementing and maintaining a risk management program,
(iii) ensuring information is recoverable in accordance with risk management decisions,
(iv) adhering to monitoring techniques for detecting, reporting, and investigating security incidents,
(v) providing IT security training to employees,
(vi) conducting criminal background checks on employees with access to department information,
(vii) separating development and production environments,
(viii) following a software change control process,
(ix) maintaining and following an IT security policy that has been approved by the department, and
(x) implementing other requirements reasonably necessary to ensure the security and privacy of Protected Information in the Contractor's possession or control

(5) Contractor shall ensure that all Representatives execute a separate acknowledgement, to be supplied by the Department in an addendum to the ISP Agreement, wherein a Representative acknowledges the ISP Agreement between Contractor and the Department, and accepts its responsibility to safeguard Protected Information in accordance with applicable federal and state laws, and the terms and conditions set forth in the ISP Agreement. For new contracts, all such acknowledgements shall be executed before work may begin. For existing contracts, acknowledgements shall be executed at the time the ISP

Agreement is executed with the Department. All such acknowledgements shall be made available to the Department upon request.

(6) Contractor shall permit Department to conduct periodic IT general controls audits, Internet security scans, and internal network vulnerability assessments, and contract monitoring audits at reasonable times, and upon reasonable notice. Such reviews may be conducted by the Department, the Texas State Auditor's Office, the Texas Department of Information Resources, or any third parties under contract with one of these agencies.

(7) The Department may, in its sole discretion, amend any ISP Agreement in order to conform to state and federal law.