

TESRS System Security Policy 2020

January 1, 2020

TESRS is required by state law to protect the confidentiality of information about members, retirees, and beneficiaries.

Local Boards must take steps to maintain the confidentiality of member information.

1. Read Government Code 865.019 (Confidentiality of Information about Members, Retirees, and Beneficiaries) to learn about your responsibilities to protect the confidentiality of member information. (see page 2)
2. Ensure that security and privacy controls are implemented and functioning to meet the obligations of Government Code 865.019.
3. Develop internal and physical controls to limit unauthorized access to personal forms and other records.
4. Refer public information requests about the pension system to the TESRS executive director upon receipt.

Local Board must take steps to prevent unauthorized access to pension information and other systems containing confidential information.

1. Develop internal controls restricting access to computer systems containing confidential information.
2. Conduct an annual review of TESRS security policies and other best-practices to prevent data breaches. Read TAC §310.12 (. Access to Information about Members, Retirees, and Beneficiaries) to learn about your local board's responsibilities to protect member information residing in the TESRS Online Database (TOL), the pension system's online database. (see page 3)
3. Ensure that security and privacy controls are implemented and functioning to satisfy the obligations of TAC § 310.12.
4. Annually appoint at least two trusted individuals to serve as authorized users of TOL.
5. Request TESRS to revoke the access of authorized users no longer associated with your department.
6. Keep your computer systems secure by keeping your operating systems and applications up-to-date and by installing anti-virus and anti-spyware software.
7. Encourage administrative personnel to complete annual cybersecurity training.

Notify TESRS within 24 hours when you have a security breach.

TESRS System Security Policy 2020

January 1, 2020

GOVERNMENT CODE

TITLE 8. PUBLIC RETIREMENT SYSTEMS

SUBTITLE H. TEXAS EMERGENCY SERVICES RETIREMENT SYSTEM

CHAPTER 865. ADMINISTRATION

Sec. 865.019. CONFIDENTIALITY OF INFORMATION ABOUT MEMBERS, RETIREES, AND BENEFICIARIES.

(a) Information contained in records that are in the custody of the pension system concerning an individual member, retiree, or beneficiary is confidential under Section [552.101](#) and may not be disclosed in a form identifiable with a specific individual unless:

- (1) the information is disclosed to:
 - (A) the individual or the individual's attorney, guardian, executor, administrator, conservator, or other person who the executive director determines is acting in the interest of the individual or the individual's estate;
 - (B) a spouse or former spouse of the individual after the executive director determines that the information is relevant to the spouse's or former spouse's interest in member accounts, benefits, or other amounts payable by the pension system;
 - (C) a governmental official or employee after the executive director determines that disclosure of the information requested is reasonably necessary to the performance of the duties of the official or employee; or
 - (D) a person authorized by the individual in writing to receive the information; or
 - (2) the information is disclosed under a subpoena and the executive director determines that the individual will have a reasonable opportunity to contest the subpoena.
- (b) This section does not prevent the disclosure of the status or identity of an individual as a member, former member, retiree, deceased member or retiree, or beneficiary of the pension system.
- (c) The executive director may designate other employees of the pension system to make the necessary determinations under Subsection (a).
- (d) A determination and disclosure under Subsection (a) may be made without notice to the individual member, retiree, or beneficiary.

Added by Acts 2005, 79th Leg., Ch. 803 (S.B. [522](#)), Sec. 1, eff. September 1, 2005.

Amended by:

Acts 2013, 83rd Leg., R.S., Ch. 1316 (S.B. [220](#)), Sec. 1.21, eff. June 14, 2013.

Acts 2019, 86th Leg., R.S., Ch. 1165 (H.B. [3247](#)), Sec. 36, eff. September 1, 2019.

Acts 2019, 86th Leg., R.S., Ch. 1165 (H.B. [3247](#)), Sec. 37, eff. September 1, 2019.

TESRS System Security Policy 2020

January 1, 2020

TITLE 34	PUBLIC FINANCE
PART 11	TEXAS EMERGENCY SERVICES RETIREMENT SYSTEM
CHAPTER 310	ADMINISTRATION OF THE TEXAS EMERGENCY SERVICES RETIREMENT SYSTEM
RULE §310.12	ACCESS TO INFORMATION ABOUT MEMBERS, ANNUITANTS, AND BENEFICIARIES

(a) The Executive Director shall develop a pension system security policy to protect member information, including electronic data.

(b) The local board annually shall review the pension system security policy and implement processes with respect to accessing the participating department's information in the pension system's online database which protect member information, including electronic data.

(c) At a meeting of the local board, the local board shall designate at least two (2) users who are approved by the local board to have access to the participating department's information in the pension system's online database. Using forms provided by the pension system and certified by signature of the local board chair, the local board shall report to the Executive Director the required information for each of the local board's approved users. At a meeting of the local board no later than the last day of February of each calendar year, the local board shall designate and approve two (or more) users and report the approved user information to the Executive Director in the manner prescribed by the Executive Director.

(d) The Executive Director shall authorize access to the pension system's online database only to users who complete a confidentiality agreement.

(e) Authorized users' confidentiality agreements under this section remain in effect until the last day of February of each calendar year or until the local board chair provides the Executive Director a written revocation of an authorized user's local board approval to maintain member records through access to the pension system's online database.

(f) If an authorized user's local board approval is revoked, the local board shall fill the vacancy for the remainder of the calendar year by the procedure in which the user was originally approved.

(g) All user access to the pension system's online database is subject to the Executive Director's approval and may be terminated at any time.