BOARD DIRECTIVE

SUBJECT: **TEXAS BOARD OF PARDONS AND PAROLES ELECTRONIC MAIL (EMAIL)**

PURPOSE: To establish guidelines for the administrative processing of electronic mail for Texas Board of Pardons and Paroles Board Members and employees who use any Texas Department of Criminal Justice Information Resources.

AUTHORITY: Texas Government Code Sections 508.035(d), 2054.003(7), 2054.051(a) and (b), 2054.052(a), and 2203.004
Texas Administrative Code Title 1, Part 10, Chapter 202, Sections 202.20(1), (2), (3), and (4).

DISCUSSION: The Texas Board of Pardons and Paroles (Board) requires utilization of electronic messages (email) in accordance with state law and ethical considerations.

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus, this directive is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;
- To create prudent and acceptable practices regarding the use of email; and
- To educate individuals using email with respect to their responsibilities associated with such use.

DEFINITIONS: Confidential Information – information maintained by the Texas Department of Criminal Justice that is exempt from disclosure under the provisions of the Texas Public Information Act or other state or federal law.

Electronic Mail System – any software application that allows electronic mail to be communicated between electronic devices.

Electronic Mail – any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Information Resources – 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.

Malware – software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Phishing – the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Sensitive Information – information maintained by the Texas Department of Criminal Justice that requires special precautions to assure its accuracy and integrity by utilizing error checking, verification procedures, and access control to protect it from unauthorized modification or deletion. Sensitive information may be confidential or it may be subject to disclosure under the Texas Public Information Act.

Spam – is an irrelevant, unwanted, intrusive, or inappropriate message sent on the internet to a large number of recipients.

Virus – a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting a system or destroying data.

PROCEDURE:

Email and the messages sent via the Texas Department of Criminal Justice (TDCJ) electronic mail systems are considered the same as all other office equipment and work produced. They are the property of TDCJ, whose management maintains the right to access. All user activity on TDCJ Information Resources (IR) assets is subject to logging and review. Consequently, there is no expectation of privacy in any email sent via TDCJ IR.

I. Utilization

A. Emails are to be used to conduct state business. When using email for these purposes, the messages should be directed to the specific users who have an interest in or need to know the information. The following information may be sent by email with the approval of the Presiding Officer:

1. Information about charitable or social activities of special interest to Board staff or social activities of special interest to the Board; and

2. Condolences and funeral announcements about employees, their relatives, or former employees.

B. All messages, files, and documents located on TDCJ IR are owned by TDCJ, may be subject to open records requests, and may be accessed in accordance with this directive. The Board reserves the right to request that TDCJ audit networks and systems on a periodic basis to ensure compliance with this directive.

C. Email users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Board unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the Board. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer".

D. Individuals shall not send, forward, or request to receive confidential or sensitive Board or TDCJ information through non-TDCJ email accounts. Examples of non-TDCJ email accounts include, but are not limited to, Microsoft Outlook, Hotmail, Google Mail, Yahoo Mail, iCloud.mail and email provided by other Internet Service Providers (ISPs). Confidential data shall be protected at all times from unauthorized disclosure. Encryption is an acceptable method of data protection.

E. Individuals shall not send, forward, request to receive, or store confidential, restricted, or sensitive Board or TDCJ information utilizing non-TDCJ accredited mobile devices. Examples of mobile devices include, but are not limited to, PDAs, two-way pagers, tablets, smart-phones, and cell phones.

F. Email users who elect to display a photo with their email profile shall only display a photo of the agency seal or a professional photo in business/professional attire of the head and shoulders. The employee's immediate supervisor has the discretion to determine the appropriateness of the photo.

G. Email users are cautioned to beware of suspicious email, especially email received from unknown senders, with misspellings and with unexpected attachments and/or links, as these may be spam or phishing emails that could result in the release of confidential, restricted, or sensitive TDCJ information or contain a virus or other malware that could present a security issue. If users notice a suspicious email, they are advised to notify the TDCJ Information Technology Division (TDCJ ITD), Office of the Information Security Officer (OISO). The OISO can be reached by phone at 936-437-1800 or 936-437-1821, or by email at iso@tdcj.texas.gov.

II. Prohibited Activities

A. The following activities are prohibited by policy:

1. Sending email that is intimidating or harassing;

2. Using email to transmit or receive material that may be offensive, indecent, or obscene;

3. Using email for personal benefit or non-Board or non-TDCJ personal solicitations;

4. Sending email for purposes of political lobbying or campaigning;

5. Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role; and

6. The use of unauthorized email software. Authorized software is listed in the TDCJ ITD Enterprise Technology Architecture (ETA) document. Use of language that violates TDCJ PD-22 General Rules of Conduct and Disciplinary Action Guidelines for Employees (Attachment A, Rules 14, 21, or 22), or usage that violates BPP-DIR 141.309 Ethics Policy will result in disciplinary action in accordance with TDCJ PD-22. All email messages are subject to review and approval by supervisors, whether or not they contain information deemed confidential by the Board or TDCJ.

B. The following activities are prohibited, as they impede the functioning of network communications and the efficient operations of email systems:

1. Sending or forwarding chain letters; and

2. Sending unsolicited messages to large groups except as required to conduct Board business.

C. All email activities and internet sites accessed as a result of using email must comply with TDCJ Information Resource Security Program Acceptable Use Policy.

III. Enforcement

A. In accordance with TDCJ PD-22, violation of this directive may result in disciplinary action, which may include termination for employees and temporaries, a termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of TDCJ IR access privileges as well as civil and criminal prosecution.

B. Any violations of state or federal law regarding this policy shall be reported to the Board's General Counsel's Office for further investigation.

SIGNED THIS, THE 14TH DAY OF OCTOBER, 2022.

DAVID GUTIÉRREZ, PRESIDING OFFICER (CHAIR)
**Signature on file.*