TEXAS DEPARTMENT OF CRIMINAL JUSTICE
PD-04 (rev. 7), "DATA USE AND NON-DISCLOSURE AGREEMENT"
MARCH 1, 2022

TABLE OF CONTENTS

EXECUTIVE DIRECTIVE

SUBJECT: **DATA USE AND NON-DISCLOSURE AGREEMENT**

AUTHORITY: 45 C.F.R. Parts 160, 164; Tex. Bus. & Com. Code § 521.002; Tex. Gov't Code §§ 493.001, 493.006(b), 552.021, 552.023, 559.004, 2054.003(7), 2054.134; Tex. Penal Code § 33.02; 1 Tex. Admin. Code §§ 202.1, 202.20–.26; BP-02.08, "Statement of Internal Controls"

APPLICABILITY: All users of Texas Department of Criminal Justice (TDCJ) information resources

EMPLOYMENT AT WILL CLAUSE:

This directive **does not** constitute an employment contract or a guarantee of continued employment. The TDCJ reserves the right to change the provisions of this directive at any time.

Nothing in this directive limits the executive director's authority to establish or revise human resources policy. This directive guides the operations of the TDCJ and **does not** create a legally enforceable interest for employees or limit the executive director's, deputy executive director's, or division directors' authority to terminate an employee at will.

POLICY:

All TDCJ employees, contract employees, consultants, vendors, interns, volunteers, and other individuals shall comply with the TDCJ's policy regarding the use of information resources and confidentiality of information and shall agree to abide by such policies.

DEFINITIONS:

The following terms are defined for the purpose of this policy and are not intended to be applicable to other policies or procedures.

"Consultant" is a professional advisor under contract with the TDCJ who performs consulting services for the TDCJ.

"Contract Employee" is an individual who performs services for the TDCJ on a contractual basis.

"Employee" is a person employed by the TDCJ on a full-time, part-time, or temporary basis.

"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.

"Intern" is an individual who performs work for the TDCJ on a temporary basis without pay, and whose work: (a) provides training or supplements training given in an educational environment; (b) provides experience for the benefit of the individual performing the work; and (c) is performed under the close supervision of TDCJ staff.

"Other Individual" is a person requiring a user account with the TDCJ; for example, Windham School District employees, Special Prosecutor's Office, Sheriff's Department, and Board of Pardons and Paroles employees.

"User" is an employee, contract employee, consultant, vendor, intern, volunteer, automated application, process, or other individual authorized to access the information resource by the information owner, in accordance with the owner's procedures and rules.

"Vendor" is any company or individual under contract to provide a service to the TDCJ, other than through a contract employee, when providing such service requires the vendor or the vendor's employee to: (a) have access to premises owned, leased, or contracted by the TDCJ; or (b) provide services to inmates at any location.

"Volunteer" is an individual who has been approved to perform volunteer services for the TDCJ.

PROCEDURES:

I. User Responsibilities

Each user is responsible for being aware of and understanding TDCJ rules regarding the use of information resources and the confidentiality of information. Access to information resources will be managed by the TDCJ Information Resources Security Program in accordance with ED-15.08, "TDCJ Information Resources Security."

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or under the custody and control of the TDCJ are the property of the TDCJ. Such files are not private and may be accessed by authorized TDCJ information security employees at any time without the knowledge or permission of the information resources user. The TDCJ reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

II. Confidentiality of Information

All users are required to conform to applicable laws and agency policies governing confidential and sensitive information, and shall maintain confidentiality of all records and information, both written and verbal, that pertain to employees, inmates, or releasees within the TDCJ. Confidential and sensitive information includes identifying information, federal tax information, personal health information, criminal justice information, or any information that is considered confidential or sensitive by federal or state law, by agency policy, or is defined as personal identifying information or sensitive personal information under Texas Business and Commerce Code § 521.002(a)(1)-(2). All users are required to safeguard and retain the confidentiality, integrity, and availability of confidential and sensitive information. Failure to comply with this agreement may result in loss of access privileges to TDCJ information resources or other disciplinary action up to and including dismissal for employees; termination or alteration of employment relations in the case of contract employees, consultants, vendors, or other individuals; or dismissal for interns and volunteers. Additionally, all users could be subject to civil liability or criminal charges, including "Breach of Computer Security" as defined by Texas Penal Code § 33.02.

All users shall take the necessary steps to prevent unauthorized access to confidential information. Users shall not share their TDCJ accounts, passwords, personal identification numbers, identification cards, credit cards, or similar information or devices used for identification and authorization purposes.

III. Data Use and Non-Disclosure Agreement Requirement

A. TDCJ Employees, Contract Employees, and Interns

All TDCJ employees shall attend Cybersecurity Awareness training provided by the TDCJ no later than 30 calendar days after most recent hire date, and every two years of employment thereafter. TDCJ contract employees and interns shall attend Cybersecurity Awareness training within 30 calendar days of reporting to the unit or department of assignment. All users shall complete the EMPL3, Data Use and Non-Disclosure Agreement (Attachment A), after viewing the Cybersecurity Awareness video in accordance with PD-97, "Training and Staff Development."

The human resources representative shall forward the EMPL3 for all employees to Employee Services, Human Resources Headquarters, for imaging into the employee's master human resources file, and retain a copy pending confirmation of imaging completion.

The human resources representative shall maintain the EMPL3 for contract employees and interns in a separate unit or department file.

B. Consultants and Vendors

Consultants and vendors requiring a user account with the TDCJ shall complete the EMPL3 prior to providing services for the TDCJ and prior to accessing TDCJ data. The appropriate TDCJ department or division shall maintain the original EMPL3.

C. Volunteers

Volunteers shall attend a Volunteer Training and Orientation Session before being allowed to begin their volunteer service in accordance with the TDCJ *Volunteer Services Plan*. Volunteers shall complete the EMPL3 at the conclusion of training, and all forms shall be forwarded to the Volunteer Services department for maintenance.

D. Other Individuals

All other individuals shall have cleared a Criminal Justice Information Services (CJIS) background check before an account is granted. Upon clearance, these individuals shall complete the EMPL3 and the appropriate department or division shall maintain the original and forward a copy to the Information Technology Division, Information Security Office. These individuals must have a TDCJ sponsor to request access via a data services request (RQ00) to any TDCJ information.

Bryan Collier
Executive Director

TEXAS DEPARTMENT OF CRIMINAL JUSTICE

DATA USE AND NON-DISCLOSURE AGREEMENT

NAME: _____ SSN: _____

ORGANIZATION: _____ DEPT: _____

POSITION: _____

PLEASE READ THE FOLLOWING AGREEMENT CAREFULLY AND COMPLETELY BEFORE SIGNING.

This Agreement applies to employees, contract employees, consultants, vendors, interns, volunteers, and other individuals of the Texas Department of Criminal Justice (hereafter referred to as "TDCJ") who handle confidential and sensitive information, including financial, medical, personnel, criminal justice, or student data and pertains to all state-owned or controlled information resources. The purpose of this Agreement is to inform you of your principal obligations concerning the use of TDCJ information resources and to document your Agreement to abide by these obligations.

"Information Resources" has the meaning defined in Texas Government Code § 2054.003(7) as ". . .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." Additionally, data impacted by the aforementioned is included as information resources.

Under 1 Texas Administrative Code § 202.22(3), "the user of an information resource has the responsibility to:

(A) use the resource only for the purpose specified by the agency or information-owner;

(B) comply with information security controls and agency policies to prevent unauthorized or accidental disclosure, modification, or destruction; and

(C) formally acknowledge that they will comply with the security policies and procedures in a method determined by the agency head or his or her designated representative."

CONFIDENTIAL AND SENSITIVE INFORMATION:

As an employee, contract employee, consultant, vendor, intern, volunteer, or other individual of the TDCJ, you may have access to confidential or sensitive information through use of TDCJ information resources or through your associated activities with TDCJ information systems. Confidential and sensitive information includes identifying information, federal tax information, personal health information, criminal justice information, or any information that is classified as confidential or sensitive by federal or state law, by TDCJ policy, or is defined as "Personal Identifying Information" or "Sensitive Personal Information" under Texas Business and Commerce Code § 521.002(a)(1)-(2). Under 1 Texas Administrative Code § 202.1(22), an information system includes an interconnected set of information resources under the same direct management control that shares common functionality. An information system normally includes hardware, software, network infrastructure, information, applications, communications, and people.

As a user of TDCJ information systems, you are required to conform to applicable laws and TDCJ policies governing confidential and sensitive information.

Your principal obligations in this area are outlined below. You are required to read and to abide by these obligations.

I UNDERSTAND THAT:

I may have access to confidential and sensitive information related to:

- Inmates, customers, employees, users, contractors, and volunteers. This may include records, conversations, applications, or financial information by which the identity of a person can be determined, either directly OR indirectly.
- TDCJ functions, such as information protected by the attorney-client and attorney work product privilege, financial information, employment records, contracts, federal tax information, internal reports, memos, and communications.
- Third parties to include vendor and customer information and contracts.

Name: _____ SSN: _____

I AGREE THAT:

- I will, at all times, safeguard and retain the confidentiality, integrity, and availability of confidential and sensitive information.
- I will only access confidential and sensitive information for business needs.
- I will not in any way divulge, copy, release, sell, loan, review, alter, or destroy any confidential or sensitive information, except as authorized.
- I will not misuse or carelessly handle confidential and sensitive information.
- I will encrypt confidential and sensitive information when appropriate, including when emailing such information outside the TDCJ and when storing such information on portable electronic devices and portable storage devices.
- I will safeguard and not disclose my password or other authorization I have that allows me to access confidential and sensitive information, except as permitted by law.
- I will report activities by any other individual or entity that I suspect may compromise the confidentiality, integrity, or availability of confidential and sensitive information.
- My privileges hereunder are subject to periodic review, revision, and if appropriate, renewal.
- I have no right or ownership interest in any confidential or sensitive information referred to in this Agreement. The TDCJ may revoke my access to confidential and sensitive information at any time and without notice.

AUTHORIZED USE – I AGREE THAT:

- I will use information resources only for official state-approved business.
- I will not use information resources for personal reasons unless there are specific limited use exceptions permitted by the TDCJ division to which I am assigned.
- I have no right to expect privacy in my use of TDCJ information resources or in the content of my communications sent or stored in TDCJ information resources. All user activity is subject to monitoring, logging, and review.
- I will NOT attempt to circumvent the computer security system by using or attempting to use any transaction, software, files, or resources I am not authorized to use.

PERSONAL SECURITY IDENTIFICATION CODES (USER IDS AND PASSWORDS) - I AGREE THAT:

- I will receive and be required to use a personal security identification code (user ID and password) to gain access to and to utilize information resources.
- My user ID and password are security measures that must be used only by me and I will not disclose my password to anyone. The only exception is in the event an information technology specialist requires the password to resolve an access problem. Once the problem has been corrected, I will immediately change my password.
- I will be held personally responsible for any transactions initiated, actions taken, or for any harm, loss, or adverse consequences arising from the use of my user ID and password, including any unauthorized use by a third party if such party gains access to my user ID and password due to my misconduct or failure to abide by TDCJ policy.

COPYRIGHTED MATERIAL - I AGREE THAT:

- Any copyrighted material, including but not limited to commercial computer software, which may be made available, is protected by copyright laws and is NOT to be copied for any reason without permission from the copyright holder.
- I will only install or use software on TDCJ computers that has been properly licensed and approved for my use in accordance with TDCJ policies and procedures.
- If installing or authorizing the installation of software on TDCJ computers, I will be responsible for ensuring that such software is only used in a manner that complies with the terms of the applicable software license agreement and all applicable TDCJ policies and procedures.

ACCESS TO DATA - I AGREE THAT:

- Proper authorization is required for access to all data owned by the TDCJ, except data that has been authorized by the TDCJ for public access.
- I will not attempt to access or alter any data that I am not authorized to access in the performance of my job duties.

Name: _____ SSN: _____

- I will not use TDCJ information resources to review, alter, or otherwise act to obtain access to information about myself, or any relative, friend, or business associate.
- I will use appropriate measures to prevent others from obtaining access to TDCJ data, such as securing my workstation either by logging off or using a password-protected screen saver.
  - I will log off or activate a password-protected screen saver before leaving a workstation with access to files containing confidential or sensitive information.
  - I will follow TDCJ policies and procedures for the release of information if I receive a request for the release of TDCJ information or data.

SECURITY OF EQUIPMENT - I AGREE THAT:

- I will not remove information resources from TDCJ property without prior authorization and approval from the appropriate authority.
- I will immediately report all security incidents, including the loss or theft of any information resources or data, to agency management and to the TDCJ information security officer.

I AGREE THAT:

- I am required to be aware of, read, and comply with the information in the TDCJ Information Security Policy found at http://itd.tdcj.texas.gov/irsp.html.
- I must comply with the policies concerning information resources set out in the TDCJ policies and procedures manual, as well as any changes to those policies.
- I must comply with the information security policies, standards, and guidelines of the TDCJ division that employs me, including any changes to those policies, standards, and guidelines.
- My failure to comply with this Agreement may result in loss of access privileges to TDCJ information resources or other disciplinary action up to and including dismissal for employees; termination or alteration of employment relations in the case of contract employees, consultants, vendors, or other individuals; or dismissal for interns and volunteers. Additionally, I could also be subject to civil liability or criminal charges, including "Breach of Computer Security" as defined by Texas Penal Code § 33.02.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT:

As an employee, contract employee, consultant, vendor, intern, volunteer, or other individual of the TDCJ, you may have access to protected health information (PHI), including demographic data, that relates to an individual's past, present, or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

I AGREE THAT:

- In accordance with the *Health Insurance Portability and Accountability Act* (HIPAA) Privacy Rule, 45 C.F.R. Part 160 and Part 164, and ED-02.01, "TDCJ Ethics Policy," I shall ensure the confidentiality and security of PHI when it is transferred, received, handled, or shared. This applies to all forms of protected health information, including electronic, oral, and paper.

Signature: _____ Date: _____

Note to Employee, Contract Employee, Consultant, Vendor, Intern, Volunteer, or Other Individual: With few exceptions, you are entitled upon request: (1) to be informed about the information the TDCJ collects about you; and (2) under Texas Government Code §§ 552.021 and 552.023, to receive and review the collected information. Under Texas Government Code § 559.004, you are also entitled to request, in accordance with TDCJ procedures, that incorrect information the TDCJ has collected about you be corrected.

Distribution of Original Form:
Employee: Master human resources file
Contract Employee or Intern: Separate unit or department file
Consultant or Vendor: Appropriate department or division
Volunteer: Volunteer Services department
Other Individual: Appropriate department or division