**Data Sharing Agreement**

**between**

**Department of Public Safety of the State of Texas**

**and**

*Organization\_A*

**Table of Contents**

[1.0 Data Sharing Statement 4](#_Toc389031059)

[2.0 Security 4](#_Toc389031060)

[2.1 General Description of Information Sensitivity 4](#_Toc389031061)

[2.2 Trusted Behavior Expectations/Rules of Behavior 4](#_Toc389031062)

[2.3 Formal Security Policy 4](#_Toc389031063)

[2.4 Administrative Security 4](#_Toc389031064)

[2.5 Identification and Authentication 5](#_Toc389031065)

[2.6 Audit Trail and Review 5](#_Toc389031066)

[2.7 Logical Access Control 6](#_Toc389031067)

[2.8 Password Management 6](#_Toc389031068)

[2.9 Software Security 6](#_Toc389031069)

[2.10 Telecommunications Security 7](#_Toc389031070)

[2.11 Media Security 7](#_Toc389031071)

[2.12 Incident Response 7](#_Toc389031072)

[2.13 Training and Awareness 8](#_Toc389031073)

[3.0 Roles and Responsibilities 8](#_Toc389031074)

[3.1 EntityResponsibilities 8](#_Toc389031075)

[3.2 DPS Responsibilities 8](#_Toc389031076)

[4.0 Termination and Validation 10](#_Toc389031077)

# 1.0 Data Sharing Statement

The requirement for data sharing between the Department of Public Safety of the State of Texas (DPS)and *Organization\_A* (Entity)exists for the sole purpose to *[list services that are being provided or the reason for the data exchange]*.

# 2.0 Security

## 2.1 General Description of Information Sensitivity and Exhibits Incorporated by Reference

Confidentiality, integrity, and availability requirements and standards are derived from the Criminal Justice Information Services (CJIS) Security Policy (http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/); 1 Texas Administrative Code § 202.1 *et seq.*; and DPS General Manual Chapters 25, *Cyber Security*, and 26, *Information Resource Policy*. The DPS General Manual Chapters are incorporated by reference as Exhibit A.

## 2.2 Trusted Behavior Expectations/Rules of Behavior

Entity must protect DPS data in accordance with this DSA, CJIS, Department of Information Resources (DIR) Regulations, and DPS General Manual Chapters 25, Cyber Security, and 26, Information Resource Policy. Entity will provide a copy of this DSA to all authorized personnel with access to DPS’s data.

## 2.3 Formal Security Policy

DPS developed these requirements under this DSA to ensure the protection of DPS data when it is being provided to outside entities. Entitymust comply with the requirements found in this DSA. Failure to comply with these procedures may result in the termination of this agreement and in any necessary action that DPS must take to protect its data.

## 2.4 Administrative Security

Entity must comply with the following administrative security procedures:

1. Entity must use host systems that have an approved warning banner on the login screen that displays a message of consent to monitoring and that warns the user about unauthorized use being subject to criminal prosecution or criminal or civil penalties.
2. Entity must ensure that all DPS data are used for official purposes only.
3. Entitymust appropriately safeguard all DPS data, permitting only authorized individuals with access.
4. Entitymay not share DPS’s data with an entity that is not a party to this DSA prior to obtaining DPS’s written approval. This written approval may be through email, an amended agreement, or a new agreement, depending upon the circumstances and at DPS’s discretion upon discussion between the parties.

## 2.5 Identification and Authentication

The purpose of authentication is to provide reliable identification for access to data or information systems. Entity must maintain the identity of active users, linking actions to specific users, and all other identification and authentication requirements. Non-repudiation must be maintained for each user accessing DPS data.

## 2.6 Audit Trail and Review

An audit trail is a chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the final output. Entity must comply with the following audit trail procedures:

1. Entity information systems that process DPS data must produce an audit trail that records, for all users, the following at a minimum:
	1. The identity of each person and device that accesses or attempts to access the system or application.
	2. Start-up and shutdown of the audit functions.
	3. Successful use of the user security attribute administration functions.
	4. All attempted uses of the user security attribute administration functions.
	5. Identification of which user security attributes have been modified.
	6. Successful and unsuccessful logons and logoffs.
	7. Unsuccessful access to security relevant files including creating, opening, closing, modifying, and deleting those files.
	8. Changes in user authenticators.
	9. Blocking or blacklisting user IDs, terminals, or access ports.
	10. Denial of access for excessive logon attempts.
	11. System access by privileged users (privileged activities at the system, either physical or logical consoles) and other system-level access by privileged users). Users may not have administrative privileges to local systems, unless the systems are standalone.
	12. Starting and ending times for each access to the system.
2. For analysis purposes, Entity must retain audit trails for at least one year or in accordance with Entity security policy, whichever is longer.
3. All audit trails must be protected from actions such as unauthorized access, modification, and destruction that would negate their forensic value.
4. DPS may modify these requirements in its discretion, in accordance with its cyber security policies.

2.7 Logical Access Control

Logical access controls provide a technical means to control user access to information and system resources. They control what information users can access, the programs they can run, and the modifications they can make. Entity must comply with the following logical access controls:

1. The identity of the user must be established before access to DPS data is granted.
2. Users will have access only to data to which they are entitled (the principle of least privilege will be enforced).
3. Entityinformation systems processing DPS data will automatically disconnect or otherwise deny access to a user after three failed logon attempts.
4. DPS may modify these requirements in its discretion, in accordance with its cyber security policies.

2.8 Password Management

Password management includes the generation, issuance, and control of the passwords that support authentication. Entity must comply with the following password management for access to DPS information:

1. Password management must meet the requirements of DPS security policy at minimum; however, Entity is authorized to implement password requirements that exceed DPS security policy requirements.
2. Passwords considered re-usable must be encrypted during transmission.
3. Passwords must be stored in an encrypted form in a protected password file to ensure confidentiality.
4. DPS may modify these requirements in its discretion, in accordance with its cyber security policies.

## 2.9 Software Security

Entity must use anti-virus protection software. Entitymust manage the anti-virus protection software to include upgrades, updates, modifications, corrections, patches, plugins, etc., that may be required to keep the software current and effective.

## 2.10 Telecommunications Security

Telecommunications security is concerned with the protection of data during transmission. Entity must comply with the following telecommunication security requirements:

1. All data must be protected during transmission in compliance with Federal Information Processing Standard (FIPS) 140-2 or 140-3 approved cryptographic modules and 1 Texas Administrative Code § 202.1 *et seq*.
2. All passwords must be protected during transmission using a mechanism that is compliant with FIPS 140-2 or 140-3 approved cryptographic modules and 1 Texas Administrative Code § 202.1 *et seq*.

## 2.11 Media Security

Entity must apply the following policies for marking and disposition of tapes, flash drives, hard drives, printouts, or any other media containing non-public or confidential data:

1. Media containing non-public or confidential data must be labeled with the appropriate information classification (e.g., Confidential).
2. Prior to release or disposal, electronic media containing sensitive or confidential data must be completely erased or destroyed usingDPS authorized methods.

## 2.12 Incident Response

An information system incident is an unexpected, unplanned event that could have a negative effect on information technology resources. A security incident is an event that violates security policies or circumvents security mechanisms (e.g., hostile probes, intrusions, malicious software), and may lead to the unauthorized exposure, access, disclosure, compromise, or loss of DPS information. Entity must comply with the following incident response policy:

1. In the event of a confirmed security incident, Entity must notify the DPS Chief Information Security Officer (CISO) in writing within four hours of discovering the incident or being notified of an incident that involves any DPS data.
2. If a security incident is suspected, but not yet confirmed, Entitymust notify the DPS Chief Information Security Officer (CISO) in writing within 24 hours of discovering the potential incident or being notified of a potential incident that involves any DPS data.
3. In the event of a security incident where Entity has detected or confirmed an intrusion, the DPS CISO, or the CISO’s designated agent, will have authority to suspend the transmission of any DPS data to Entity until it has proven recovery to a secure state that can ensure the confidentiality of DPS data. In addition, Entity must also promptly provide DPS with a copy of any incident reports involving DPS data.

## 2.13 Training and Awareness

Entity must ensure that all Entityend users receive initial and annual DIR-certified security awareness training. In addition, Entity must ensure all users (persons and entities) sign the Rules of Behavior Agreement, Exhibit B, prior to those users having access to any DPS data.

# 3.0 Roles and Responsibilities

## 3.1 EntityResponsibilities

Entity must:

1. Protect all Personal Identifying Information and Sensitive Personal Information in accordance with Texas Business and Commerce Code § 521.001 and 1 Texas Administrative Code § 202.1 *et seq*.
2. Provide proof of compliance with security documents when requested to do so by DPS.
3. Ensure appropriate protection of all security documents.
4. Maintain copies of signed Rules of Behavior (Exhibit B) for every authorized user.
5. Have complete responsibility for all cyber security controls.
6. Have complete responsibility for encryption of all system components in accordance with FIPS 140-2 or 140-3.
7. Maintain all logical access controls and password management.
8. Maintain all system software, anti-virus protection, encryption, and operating systems to include all upgrades, updates, patches, plugins, etc. in alignment with current and best cybersecurity practices.
9. Only grant users access to data they need to perform their official functions.
10. Not share DPS’s data outside Entitywithout DPS’s written approval.
11. Ensure that it, and any entity that it shares DPS’s data with, complies with the requirements in this data agreement if Entity shares or sells DPS’s data.
12. Report any security breaches involving Entity (or shared entity or users) to the DPS CISO.
13. Implement the necessary procedures to ensure that Entity is secure from any unauthorized use.
14. Ensure that any individual requesting access to DPS data is authorized to receive it. Unauthorized request or receipt of data could result in criminal proceedings brought against the Entity and the individuals or entities involved.
15. Ensure all users have completed any required training prior to access and that annual security awareness training is performed.
16. Disseminate user manuals and other related publications as required.
17. In relation to DPS’s data, conduct investigations relating to possible fraud, waste, and abuse arising from Entity’s or one if its users’ access to the data.
18. Review this DSA on an annual basis (or more frequently if needed) and coordinate any recommended changes with DPS.
19. Ensure that a user’s access to any DPS data is terminated no later than 24 hours after the user is no longer authorized to have access.

## 3.2 DPS Responsibilities

 DPS will:

1. Protect all DPS Personal Identifying Information and Sensitive Personal Information in accordance with Texas Business and Commerce Code §521.001 and 1 Texas Administrative Code § 202.1 *et seq*.
2. Ensure appropriate protection of all security documents.
3. Maintain communication with Entity to ensure operational needs are being met.
4. Manage security incident assessment and response.
5. Review this DSA on an annual basis (or more frequently if needed) and coordinate any recommended changes with Entity.

4.0 Termination and Validation

Either party may terminate this agreement upon 30 calendar days’ advanced written notice or immediately without notice in the event of a security exception that cannot be timely resolved between the parties. On an annual basis (or more frequently if needed), DPS and Entity will review, update if necessary, and revalidate this DSA.

|  |  |  |
| --- | --- | --- |
| ***Organization\_A*****Authorized Representative** |  | **Department of Public Safety****Authorized Representative** |
| *Insert name and title here.* |  | *Insert name and title here.* |
|  |  |  |
|  |  |  |
|  |  |  |
| **Signature of Authorized Representative** |  | **Signature of Authorized Representative** |
| **Date:** |  | **Date:** |

|  |  |  |
| --- | --- | --- |
| ***Organization\_A*****Chief Information Officer** |  | **Department of Public Safety****Chief Information Officer** |
| *Insert name here.* |  | *Insert name and title here.* |
|  |  |  |
|  |  |  |
|  |  |  |
| **Signature of Chief Information Officer****Date:** |  | **Signature of Chief Information Officer****Date:** |

|  |  |  |
| --- | --- | --- |
| ***Organization\_A*****Chief Information Security Officer** |  | **Department of Public Safety****Chief Information Security Officer** |
| *Insert name here.* |  | *Insert name and title here.* |
|  |  |  |
|  |  |  |
|  |  |  |
| **Signature of Chief Information Security Officer****Date:** |  | **Signature of Chief Information Security Officer****Date:** |