Department of Developmental Services

Data Exchange Security Questionnaire Form

STATE OF CALIFORNIA
DEPARTMENT OF DEVELOPMENTAL SERVICES
INFORMATION TECHNOLOGY DIVISION
INFORMATION SECURITY OFFICE
1600 9TH ST. ROOM 220 MS 2-7
SACRAMENTO CA 95814

Purpose

Departments or external entities requesting to exchange data with DDS are required to submit a *Data Exchange Security Form (DS 5305.8-F)* prior to approval of a data exchange/use agreement. This form allows DDS to develop a risk analysis of security controls of requesting entities to ensure that DDS information is properly protected.

Respond to all questions

Whenever possible, respond using the electronic format, which will allow for the evaluation of the unique computing environment (Local Area Network (LAN) and Wide Area Network (WAN)) of each entity.

Check the desired box to select a response:

1	**Confidentiality Statement**	
	Does your organization require its employees to sign a confidentiality statement prior to accessing confidential information?	**Yes** ☐ **No** ☐
2	**The following questions must be completed by your organization's responsible authority:**	
a.	Does your organization follow *National Institute of Standards and Technology (NIST) SP 800-53* security guidelines (for moderate level data) to protect your information processing systems?	**Yes** ☐ **No** ☐
	If no, provide the guidelines your organization follows to secure its information assets:	
b.	Does your organization allow remote access to its information?	**Yes** ☐ **No** ☐
	If Yes, is two-factor authentication required for remote access?	**Yes** ☐ **No** ☐
3	**Information Security Program**	
	Is an Information System Security Plan in place to protect confidential and sensitive information?	**Yes** ☐ **No** ☐
4	**Information Security Awareness and Training Program**	
	Is a training program established for employees and contractors that explains how to comply with information security policies, procedures, and guidelines?	**Yes** ☐ **No** ☐
5	**Access Management** The following requirements are designed to prohibit unauthorized access to our information. If you provide authentication services for another entity, please indicate how you control your client's access to our information or the session.	
a.	Is a warning banner displayed when a user accesses our information through a login screen?	**Yes** ☐ **No** ☐
	If Yes, provide the wording of your organization's warning banner:	
b.	Are all sessions that display our information terminated, and/or the screen obscured, after a predetermined period of inactivity on all workstations? For example, do all workstations have a password-protected screensaver?	**Yes** ☐ **No** ☐
c.	Are access controls in place to ensure the confidentiality and integrity of files and databases (classified as containing information obtained from DDS)?	**Yes** ☐ **No** ☐
d.	Is access to information resources revoked immediately for individuals who separate from your organization or no longer perform the authorized business function?	**Yes** ☐ **No** ☐
e.	Are user accounts disabled for a specified time period after several consecutive unsuccessful login attempts?	**Yes** ☐ **No** ☐
f.	When user accounts are unlocked, is user identification (ID) verification required?	**Yes** ☐ **No** ☐

	g. Are personally-owned devices allowed to access information resources that contain DDS information?	**Yes** ☐ **No** ☐
6	**Identification and Authentication**	
	a. Are there authentication controls that require each individual to have a **unique** user ID and a confidential password to log on to the DDS session or the system in which DDS data reside?	**Yes** ☐ **No** ☐
	b. Are all users **required** to manually enter a password to log on to DDS systems or when the systems that contain DDS data are accessed? (Applications cannot save passwords for future use or permit the use of programmed function (PF) keys)	**Yes** ☐ **No** ☐
	c. Are keyed passwords **prevented** from being displayed on the screen in plain text or a readable manner?	**Yes** ☐ **No** ☐
	d. Are system-level passwords changed at least on an annual basis? (For example, root, enable, network, application, local and enterprise-level administration, etc.)	**Yes** ☐ **No** ☐
7	**Incident Response** A security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.	
	a. Does your organization have an established incident response procedure for log collection, analysis, and reporting of unauthorized or unusual telecommunications, network, and host-based activities?	**Yes** ☐ **No** ☐
8		
	a. Is DDS information encrypted during **transmission** (including the legitimate transmission of DDS data by email)? **If No, explain how the personal information is protected in transit**:	**Yes** ☐ **No** ☐
	b. Do your organization's encryption requirements meet or exceed the Advanced Encryption Standard (AES) Federal Information Processing Standards *(FIPS) Publication 197*?	**Yes** ☐ **No** ☐
9	**Malicious Code Mitigation**	
	a. Is anti-virus software installed, enabled, centrally-managed, and configured to prevent deactivation on workstations and servers that access DDS information?	**Yes** ☐ **No** ☐
	b. Are the latest anti-virus definitions maintained on all servers used to access, update or store DDS information?	**Yes** ☐ **No** ☐
	c. Are periodic scans performed to search for malicious code and viruses on all servers and workstations that access, store, or process DDS data?	**Yes** ☐ **No** ☐
10	**Patch Management**	
	Are all security patches and upgrades installed on servers and workstations after proper testing? **If Yes, specify the timeframe to deploy those patches:**	**Yes** ☐ **No** ☐
11	**Security Controls**	
	a. Is there at least one firewall located between each external access point on your organization's LAN and any server that hosts applications, provides access to, or stores DDS information?	**Yes** ☐ **No** ☐
	b. Are your organization's firewalls configured to restrict traffic to specific hosts, ports, and services?	**Yes** ☐ **No** ☐

c. Are passwords changed for all firewalls that protect DDS information from the default settings prior before production deployment? **Yes** ☐ **No** ☐

Is **administrative access** to firewall devices (that protect DDS information) limited to specific internal network IP addresses and users? ☐ ☐

Do all computers that access DDS information from remote locations have a centrally-managed personal firewall? ☐ ☐

If wireless technology is in use to access DDS information, are all required *NIST SP 800-53* moderate security controls (at a minimum) for wireless access in place? ☐ ☐

12 Intrusion Detection/Prevention

What methods are used to monitor network-based intrusions? This can be a combination of hardware and software controls that can detect all failed and successful attempts to penetrate firewalls and other computer access barriers.

Check all that apply:

a. Review firewall and system logs daily. ☐

b. Intrusion detection and prevention. ☐

c. Integrity checking software. ☐

(Specify:)

a. Is all audit log information securely stored? **Yes** ☐ **No** ☐

Specify the length of time the audit logs are stored:

Are the data elements recommended by *NIST SP 800-53* (moderate) included in all security audit log files? ☐ ☐

Are security audit log files reviewed on a regular basis? ☐ ☐

Is access to security audit logs limited only to authorized security and network personnel, law enforcement, and DDS? ☐ ☐

14 Physical Security Access Controls

Are systems containing DDS information physically protected from unauthorized access, theft, and malicious activity? **Yes** ☐ **No** ☐

15 Record, Documentation, and Equipment Disposal

DDS may store and maintain records for as long as there is a legitimate business need. The Department's Interagency Agreement (or Data Use Agreement) states the purpose for which your organization's approval was granted. All temporary files that contain DDS data must be processed and deleted within 24 hours of creation.

Equipment or Media Cleansing and Destruction

Reference *NIST SP 800-88, Guidelines for Media Sanitation*, from the Department of Defense 5220.22-M, *Clearing and Sanitation Matrix*, for approved methods of meeting this requirement.

a. What is your organization's data retention schedule for DDS data? **Response:**

b. Describe the method(s) used to destroy DDS data. **Check all that apply:**

☐ Paper – **Response:**
☐ CD – **Response:**
☐ Electronic Data – **Response:**

☐ Other (Specify) – **Response:**

I certify that the above information is true and correct and accurately reflects the administration of our security program as we originate participation in the Department of Developmental Services Data Exchange Program.

Printed Name: _____

Signature: _____

Title: _____

Date: _____

- Organization:
- Organization's physical address
- Respondent's Organizational Role:
- Phone Number:
- Email Address:

17	**Return the Completed Package via US Postal service or Email**

DEPARTMENT OF DEVELOPMENTAL SERVICES
INFORMATION TECHNOLOGY DIVISION
INFORMATION SECURITY OFFICE

1600 9TH ST. ROOM 220 MS 2-7
SACRAMENTO, CA 95814

datarequests@dds.ca.gov

18	**Review and Approval**

This should be reviewed and approved by the Information Security Officer

Name: _____

Signature: _____

Title: _____

Date: _____

19. Review Schedule and Revision History

Date	Description of Change	Reviewer
02/13/2016	Original Form Release	ISO
07/23/2018	Review by Managers and approve	CIO
10/07/2019	Add signature/date lines for ISO review/approval	ISO (v2r1)
10/16/2020	Change email submission address to datarequests@dds.ca.gov	CISO (v2r2)