Data Security for Contractors

EXHIBIT A Training

Original Date: October 14, 2019 | Revised Date:
Information Technology Division, Information Security | Approved for distribution by Pablo Matute, DCYF IT Security Administrator

www.dcyf.wa.gov

Washington State Department of CHILDREN, YOUTH & FAMILIES

Data Security for Contractors
Exhibit A Training

DCYF has created and uses within all their contracts, Exhibit A – Data Security Requirements. The contract exhibit outlines Contractor requirements regarding DCYF Data in all forms. This PowerPoint will go over the highlights of Exhibit A and clarify some of the requirements. This training **is not** to take the place of reading and understanding **all** of the requirements within Exhibit A. It is your responsibility to know and understand the entirety of Exhibit A.

There is additional information on the DCYF website at https://www.dcyf.wa.gov/services/child-welfare-providers. If you have additional questions, please contact the Contract Manager listed on the first page of your contract.

Data Security for Contractors
Exhibit A Training

Training Outline:

Data Categories – General
Data Categories – Examples
Administrative Controls
Data Security training requirements
Password – General
Password Minimum requirements
Passwords – Complex Passwords
Email security
Physical security – removable Devices
Physical Security – Laptops/Mobile Devices
Protection of data – General requirements
Protection of Data – paper Documents
Cloud Storage
Confidentiality – General
Confidentiality
Data Disposition
Data Breach – general
Data Breach – Upon Notice of breach
Closing
Contacts
Certificate of Completion

Data Security for Contractors
Exhibit A Training

Data Categories: General

All DCYF owned data falls into one of four categories:

Category 1 – Public information can be released to the public.

Category 2 – Sensitive information is not specifically protected by law but should be limited to official use and protected from unauthorized access.

Category 3 – Confidential information is protected from disclosure by law.

Category 4 – Confidential information requiring "special handling" is also protected from disclosure by law, regulation, or agreement. There are serious consequences could arise from unauthorized disclosure, ranging from life threatening situations to legal sanctions.

DCYF Data is always Category 3 and above

Data Security for Contractors
Exhibit A Training

Data Categories: Examples

Below are some examples of Category 3 and 4 data:

Category 3 – Confidential information: Includes personal information about individual DCYF clients, department employee personnel records, source code fro computer applications, and any other documents or information that could potentially jeopardize the integrity of the Department, enable fraud, or trigger action by law enforcement or regulatory group. Personal information includes things like name, birthdate, social Security Number, and address.

Category 4 – Confidential information, special handling: Includes information with especially strict handling requirements such as a client's Federal Tax Information (FTI), their Protected Health Information (PHI), a location of an abused spouse or other potentially life-threatening data.

Data Security for Contractors
Exhibit A Training

Administrative Controls

Contractor is required to have a documented security policy governing the secure use of all computer networks, mobile devices, portable devices, and paper/hard copy documents. The policy must define sanctions that may be applied to Contractor staff for violating the policy.

It is every Contractor staff responsibility to read and understand this policy, as well as, all of the requirements within Exhibit A. Ask for and read both of these documents.

Data Security for Contractors
Exhibit A Training

Data Security Training Requirements

Every Contractor staff member must complete, on an annual bases, the following required training:

- Contactor staff responsibilities under the Contractors security policy;
- Contractor staff responsibilities as outlined under contract Exhibit A;
- Compete the DCYF Information Security Awareness Training (Link provided in Exhibit A).

Data Security for Contractors
Exhibit A Training

Password Security: General Rules

Passwords are the Contractors first and sometimes last line of defense against unauthorized access to sensitive systems and information.

As Contractor staff it is **your responsibility to use strong passwords**, to protect them from disclosure and to report any breaches *immediately*.

You can protect your passwords by following these basic guidelines:

- Use complex passwords that cannot be easily guessed;
- *Never* write your password down;
- *Never* share your password with *anyone* – verbally or in writing;
- *Never* allow a coworker to assume control over a computer while you are logged in on your account;
- Change passwords often, **required** after a breach occurs.

Data Security for Contractors
Exhibit A Training

Password Security: Minimum Requirements

Minimum password requirements per Exhibit A:

- Must be a minimum length of eight (8) characters containing at least three (3) of the following character classes:
  - Uppercase letters
  - Lowercase letters
  - Numerals
  - Special characters (asterisk, ampersand, exclamation point, ect.)
- Does not contain a user's name, login ID or any form of their full name;
- Does not consist of a single dictionary word; maybe a passphrase which consists of multiple dictionary words;
- Must be significantly different from previous four (4) passwords. Increment by simply adding a number are not significantly different

Data Security for Contractors
Exhibit A Training

Password Security: Complex Passwords

Complex passwords meet the following criteria and are best practice:

- It is at least fifteen (15) characters long;
- It is not derived from the username – in whole or in part;
- It combines upper and lower-case letters, numbers and symbols;
- It does not include dictionary words, names, birthdays, telephone numbers or any personal identification numbers;
- The stronger your password, the less likely it will be that unauthorized use or breach of your account will occur.

REMEMBER: You are responsible for ensuring the integrity of your account(s).

Data Security for Contractors
Exhibit A Training

Email Security

- Email is the primary method through which most DCYF employees and Contractors communicate with each other, clients and partners.
- Unfortunately, email is also the primary method through which people with malicious or criminal intent attempt to breach the DCYF or Contractors network.
- Identifying a malicious message can be challenging. Here are some quick tips to help you avoid falling victim to one:
  - **Think Before You Click!**
  - Be *extremely* cautious about how you handle unsolicited emails.
  - **Never** click on links or open attachments in unsolicited emails.
  - **Never** respond to emails asking for your username, password or an personal or agency information.

If you have any doubts about the authenticity of an email, do not open it and notify your agency IT staff, follow your agency IT policy and if needed contract contact immediately.

Data Security for Contractors
Exhibit A Training

Email security

- When communicating by email with DCYF, always use the DCYF secure email system
- DCYF employees are required to use the secure email system when sending confidential data to Contractors and their staff
- Response from Contractor staff and data sent by Contractor staff will use the same method
- How to know if the DCYF secure email system was used:
  - Subject [secure]

Data Security for Contractors
Exhibit A Training

Physical Security: Removable Media

- Removable Media such as USB drives, external hard drives, memory cards/sticks, CD's/DVD's and voice recorders are very easy to lose and they are a prime target for thieves because they are small and valuable.
- It is extremely important that you keep these assets secure. Sensitive data on removable media should always be encrypted and you should never leave it somewhere that it can be easily lost or stolen.
  - Lock it Up
  - Keep it out of sight
  - Never leave in a motor vehicle

You must report lost or stolen removable media to your supervisor and follow the data breach protocol

Data Security for Contractors
Exhibit A Training

Physical Security: Laptops and Mobile Devices

- Many Contractors use laptops, mobile phones, tablets, voice recorders and cameras to perform some or all of their duties.
- Laptops and mobile devices are very easy to lose and they are a prime target for thieves because they are small and valuable. It is extremely important that you keep your assets secure at all times.
  - Laptops should always be encrypted;
  - Never leave them unsecured;
  - Never leave in a motor vehicle.

You must report lost or stolen laptops and mobile devices to your supervisor and follow the data breach protocol. You must also contact police and file a report.

Data Security for Contractors
Exhibit A Training

Protection of Data: General Requirements

It is everyone's responsibility to protect DCYF data. Aside from the specific system requirements outlined within Exhibit A, Section 7, the following common sense requirements are to be followed:

- **Do not** leave computers unattended and logged into when not physically present at the workstation;
- **Do not** leave mobile devices or paper documents unsecured in a motor vehicle. Take them with you when you exit your vehicle for any period of time;
- **Do not** allow unauthorized people access to your computer, mobile devices and/or paper documents;
- Data is only shared on a need to know bases. Not every coworker has a need to know.
- Be aware of your surroundings and who is around. Data can be compromised by listening to phone calls, employees talking and documents left on desks.

Data Security for Contractors
Exhibit A Training

Protection of Data: Paper Documents

- All paper documents must be stored in a secure area with access controlled through use of a key, card key, combination lock or comparable mechanism, accessible only to authorized personnel
- Paper documents transported outside the secure area must be under the physical control of Contractor staff with authorization to access the data
- Paper documents will not be secured or stored in a motor vehicle anytime a staff member is away from the motor vehicle
- Paper documents will be retained in a secure area per Washington state records retention requirements

Data Security for Contractors
Exhibit A Training

Cloud Storage

- DCYF does allow for data to be stored within the Cloud
- Follow all Cloud Storage requirements as outlined in Exhibit A under Section 7.h

Data Security for Contractors
Exhibit A Training

Confidentiality: General

Confidentiality of DCYF data is an essential part of all Contactor staff and subcontractors duties. Remember “Lose Lips, Sink Ships” from World War Two? This goes the same for protecting the data that you may have access to during your work day.

- Use data for the sole purpose of accomplishing the services set forth in this contract.
- Be mindful of your phone conservation, talking to other staff and especially talking to clients. Things can be overheard.
- Do not leave paper documents unattended, especially in unsecured locations.
- Do not leave computers unattended without locking the screen or logging out so that information cannot be seen.

Data Security for Contractors
Exhibit A Training

Confidentiality

- All Contractor staff and subcontractors who have access to DCYF data must sign a Statement of Confidentiality and Non-Disclosure (DCYF Form 03-374B).
- Form can be found at https://www.dcyf.wa.gov/forms

Data Security for Contractors
Exhibit A Training

Data Disposition

- Contactors and their staff are not authorized to dispose of or destroy any DCYF data without written authorization from DCYF.
- All DCYF data in any form must follow the Washington state records retention standards as set forth by law.
- Generally, all DCYF data has a retention of 6 years. However, there may be items that have a longer retention standard.
- Follow the data disposition requirements in Exhibit A to ensure proper records retention and disposition requirements.

DO NOT DISPOSE OF DCYF DATA WITHOUT DCYF WRITTEN AUTHORIZATION

Data Security for Contractors
Exhibit A Training

Data Breach Requirements: General

In the event of a data breach, including loss of paper documents, you are required to take the following steps:

- Immediately follow your Contractors notification process, informing the Contractor of the breach or possible breach of data.
  - Note day, time, location and how you believe data was lost
  - Report to police if items lost were stolen, a break-in occurred or other criminal activity lead to the breach/possible breach. **Police report is required in these instances.**
- **Contractor is required to notify DCYF through the Contracts and Procurement Office at dcyf.contractdatabreach@dcyf.wa.gov within one (1) business day after potential, suspected, attempted or actual breach of data.**
- Contractor will take steps to mitigate harmful effects of data breach.

Data Security for Contractors
Exhibit A Training

Data Breach: Upon Notice of breach

- Go to https://www.dcyf.wa.gov/services/child-welfare-providers and complete the Security Breach Report. Provide as much detail as possible.
  - Complete sections 1-8 and description on second page
  - When, where and how did incident occur, who was involved, date, time and location
  - How many people's information may have been compromised.
  - Type of information compromised (examples: reports, personal identifiable information, health records, names, addresses).
- **Contact by email the Contract and Procurement Office at dcyf.contractdatabreach@dcyf.wa.gov. Attach copy of the Data Security Breach form, police report (if applicable) and any other supporting documents.**
- **Contact the Contract Manager listed on the front page of your contract.**
- You will be notified by DCYF as to next steps and any additional requirements.

Data Security for Contractors
Exhibit A Training

Thank you for reviewing this training material. It is very important to DCYF that our data is protected when in your hands. By following these requirements, as well as, your agency data security policy, and staying aware of data security threats, you will be able to help protect our data.

You are the first line of defense!

Remember, that this training PowerPoint is not all encompassing. You still need to read and review Exhibit A and your agency specific data security policies on a yearly bases.

Print your Certificate of Competition (last slide) and place in your Personnel File.

Thank you!

DCYF IT Security Administrator

Pablo Matute

Email: Pablo.matute@dcyf.wa.gov

Phone: 360-688-4169

DCYF Contract Compliance Officer

Rick Morgan

Email: Richard.Morgan@dcyf.wa.gov

Phone: 360-902-7522

Certificate of Completion

THIS ACKNOWLEDGES THAT

HAS SUCCESSFULLY COMPLETED
DATA SECURITY FOR CONTRACTORS – EXHIBIT A

_____ _____

Contractor Date