
Information Security Training for Third Party Access Users



May 2015

Information Security and Privacy Overview

Module 1



Information Security ...

Plays a vital role in an organization's ability to achieve its stated business mission, while safeguarding its information assets.



What is Information Security?



Information security is the protection of information assets from unauthorized access, use, modification, theft, deletion, and disclosure.

Examples of Information Assets

- Word Processing documents
- Spreadsheets
- Meeting Requests
- Graphics & drawings
- Presentations
- Personal computer hard drives and records
- Computer printouts
- Letters, memos and reports
- Fax documents
- Diskettes, CDs, and USB portable drives
- Electronic mail

Information Privacy



Information Privacy is the prevention of revealing personal information to anyone that **does not** have permission to have access. In addition, access is only permitted when there is an impending business need.

Personal Information

Personal information is protected by law from unauthorized access and disclosure. Personal information is comprised of an individual's first name or first initial, and last name in combination with any one or more of the following data elements:

- Social security number
- Address
- California Driver's license number or California Identification Card number
- Bank account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Child Support Information

Module 2



Child Support Information

With regards to the Child Support Program, information security pertains to all personal and confidential child support information. This includes:

- Federal Tax Information (FTI),
- Department of Motor Vehicle (DMV) information,
- Information from the Medi-Cal Eligibility Determination System (MEDS), and
- Any other personally identifiable information generated, obtained or stored as part of the Child Support Program.



Confidential Information

Confidential Information is protected by law from unauthorized access and disclosure. Confidential information has value to the public, and as such access to that is jeopardized unless access is restricted to specific individuals or business functions. Examples:

- Child Support participant application for Child Support Program services.
- Records pertaining to pending litigation or claim.
- Medical or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy.
- Test questions, scoring keys, and other examination data used to administer a licensing examination or examination for employment.
- Documents protected by attorney-client privilege.
- System and network information, such as diagrams, IP addresses, etc.
- Employment data.

Federal Tax Information



Federal Tax Information (FTI) is Information received from the Internal Revenue Service which pertains to (1) a taxpayer's identity and (2) the nature, source, or amount of his or her income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments.

DCSS is responsible for...

Securing all information used in the Child Support Program. This information is confidential. You may be subject to disciplinary actions, including termination, as well as civil and/or criminal penalties if you unlawfully access or disclose Child Support Information. DCSS strictly enforces information security and privacy protection.



If you violate DCSS confidentiality policies...

You may be subject to administrative, civil and/or criminal action.

- Fines for confidentiality violations range from \$1,000 to \$20,000.
- Imprisonment for confidentiality violations ranges from 1 year to 5 years.
- You may be liable for damages to persons injured by your confidentiality violation.



Identifying Security Incidents



A security incident is defined as any act or failure to act, or an event that creates a threat to the confidentiality, integrity and/or availability of Child Support Information and IT Assets, or person(s) or property located at any Child Support facility.

Some examples:

- Hacking attempts
- Unauthorized disclosure of personal identifiable information
- Lost or stolen information/equipment
- Inappropriate activities
- Unauthorized/suspicious people or activity in facility

Reporting a Security Incident

If you identify a security incident, you must report it to your immediate supervisor and to the DCSS Information Security Office. You should:

- Email the Information Security Office, info.security@dcss.ca.gov
- Contact the Information Security Office via phone at 916-464-5045.



Summary of Module 2

- Federal Tax Information is tax return information received from the IRS.
- All Child Support Information should be treated as "confidential". This includes, but is not limited to the information received from the IRS, accessed through DMV and MEDS.
- You may be held personally responsible for unauthorized access or disclosure of child support information.
- If you identify a security incident you must report it immediately to your supervisor and the DCSS Information Security Office.

Access to Child Support Information

Module 3



Access to Child Support Information

Because of the confidential nature of the Child Support Information, access to the information must be controlled. The key issues to consider when granting access to Child Support Information are: (1) does the employee have a “business need” (2) does the employee have a relationship with one or more individuals involved in the case and (3) the time frame (days and hours) for accessing the information. Also important is safeguarding your password to the DCSS network and any DCSS system.

Business Need

You should only access child support information when you have a “business need” to do so. You should never access:

- Your own information
- Relatives’ information
- Former spouses’ information
- Neighbors’ information
- Information not directly related to current assigned cases.



Conflict Recusal



Conflict recusal is a commitment from a Child Support employee that because he or she has a personal or business relationship with one or more individuals in a child support case he or she relinquishes access to any Child Support Information about that case.

Passwords



A password is a confidential series of characters used to authenticate an individual's identity, usually during the logon process. User IDs and passwords are given to enable authorized access to DCSS systems and resources.

You are accountable for all system activity associated with your ID and password.

Passwords (cont.)

All staff must take the necessary precautions to safeguard their passwords. The users must:

- Use a password no less than eight characters long.
- Not reveal their passwords to anyone, at anytime, for any reason.
- Not store their passwords in an unencrypted format for reference.
- Change their password if a compromise is suspected.
- Not select passwords that are easily guessed – name of spouse, children, pet, favorite sport, hobbies, common words, etc.
- Select complex passwords, – that is passwords that combine three of the following four elements: uppercase letters, lowercase letters, numeric digits, punctuations, and special characters such as @, #, \$, %.

Work Area



It is extremely important that you be alert to the sensitivity of the information you work with and be continually aware of who may have access to it. It is your responsibility to prevent unauthorized access to DCSS information from visitors, service personnel or anyone else to whom access has not been allowed.

Work Area (cont.)

Here are some things you can do to protect information in your work area:

- Lock doors, drawers, cabinets, etc., when not in your work area.
- Lock up sensitive documents and removable media.
- Secure all computing devices when left unattended by logging off or activating the password protected screensaver.
- Never share your logon ID or Password.
- Never allow another person to “piggyback” into the work area.
- Challenge unescorted people you do not know.
- Clear your desk and work area at the end of the day. This includes the proper disposal or storage of sensitive documents.

Summary of Module 3

- Staff should take the necessary precautions to safeguard their passwords.
- Never reveal your password to anyone, at anytime, for any reason.
- Always lock your workstation when you step away from your cubicle or office.
- You should recuse yourself from any case where you have a personal or business relationship with one or more parties involved in the case.

Summary of Module 3 (cont.)

- Always treat child support Information as confidential.
- Never access child support information unless you have a business need.
- Never disclose child support information to anyone who does not have a business need.

Use and Confidential Destruction of Child Support Information

Module 4



Use and confidential destruction of child support information

The level of security over Child Support Information is directly affected by the day-to-day activities of employees. This Module discusses the precautions you should take while using Child Support Information.



Handling of confidential documents

- You should safeguard confidential information no matter what form it takes (i.e., stored on the network, stored on a CD, printed on paper).
- File cabinets, storage areas, desks, paper, computers, microfilm, microfiche, diskettes, CDs and any other removable media must be secured from unauthorized access at the end of each workday.
- All confidential or personal information contained on paper documents, and computer monitors must be secured from observation by or disclosure to unauthorized persons at all times (i.e., store paper documents in locked drawers) whenever you're away from your work area, lock your computer screen (Ctrl/Alt/Del) .



Printing confidential information

Any printouts containing information that is personal, confidential, or sensitive should be picked up immediately after printing.



Faxing confidential information



Take extra precautions when sending or receiving confidential information via a fax. A fax cover sheet should accompany all faxes.

When sending, staff should *notify the recipient* when the fax is transmitted, and *immediately follow-up* with the recipient that the fax was received.

When receiving, staff should ask the sender to notify them when the fax is transmitted, staff should then *immediately pick up* the fax.

Confidential Destruction



Give careful thought before you toss confidential reports, memos, etc. Into the regular disposal bin. Often times social engineers will rummage through an organization's trash bins looking for information like names and acronyms for use in social engineering to gain access to systems.

Destroy or dispose of confidential or sensitive documents and files appropriately using either the secured confidential destruction bins or cross-cut shredders located within the county organizations.

Summary of Module 4

- Lock up confidential information when not being used.
- Dispose of reports or memos which contain confidential information and are no longer needed, in the secured confidential disposal boxes.
- Be sure confidential information is not accessible to those who don't have a business need to know.
- Log-off or lock your workstation (Alt-Ctrl-Del) when away from your desk for any length of time.

Thank You

“Information Security is Everyone’s Responsibility.”

If you have any questions regarding information security or privacy protection, please contact the Information Security Office at info.security@dcss.ca.gov or 916-464-5045.

This concludes the Information Security Training for Third Party Users.

