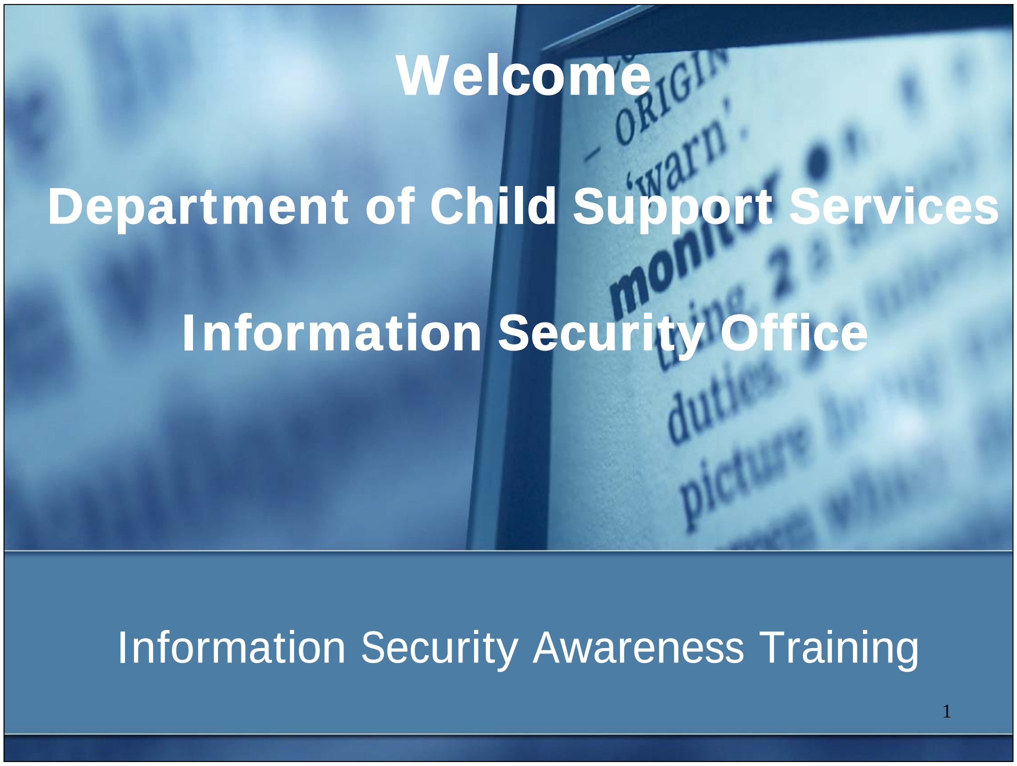


Welcome

Department of Child Support Services

Information Security Office

Information Security Awareness Training

1

Welcome to the Department of Child Support Services (DCSS) Information Security Office (ISO) Annual Security Awareness Training.

The term Child Support Employees for information security includes all employees, contractors, students and vendors that access, maintain or support Child Support information or information assets.

All Child Support Employees are <u>required</u> to receive information security awareness training upon hire and annually thereafter.

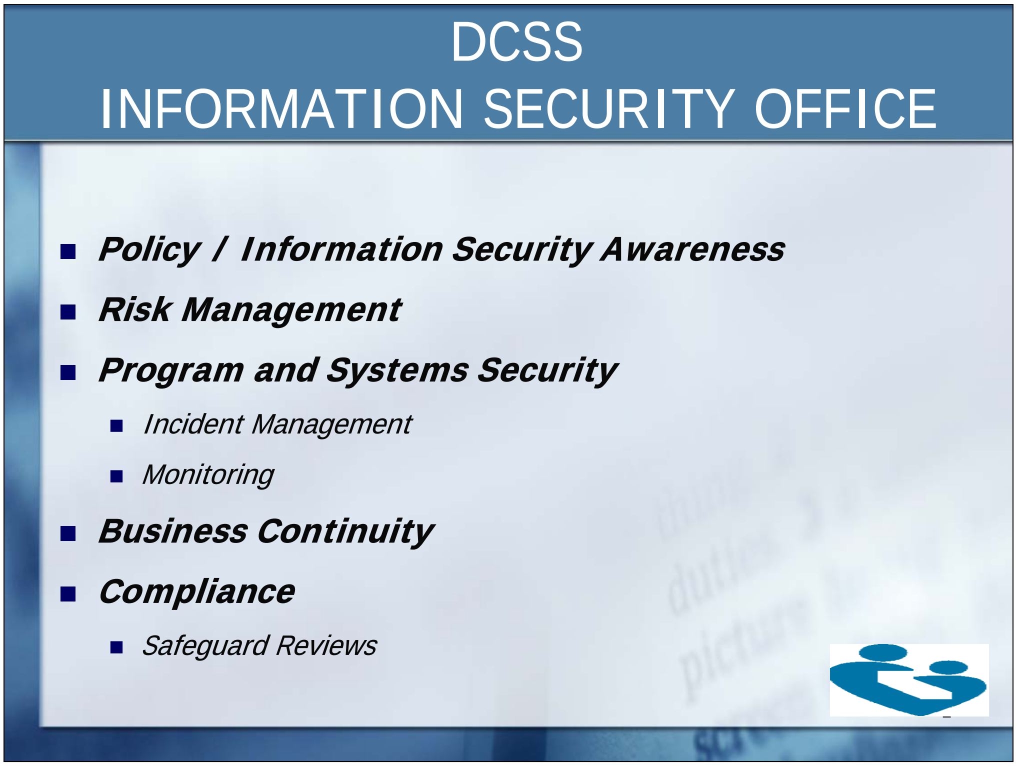
This presentation is provided as a tool to comply with the DCSS Information Security Manual (ISM). It is provided as a guide and may be adapted to meet your organization’s information security training needs. Additional tools such as the forms mentioned in the training are available from the ISO or at the DCSS ISO web page.

If you have any questions or need additional assistance call the DCSS Information Security Office at:

(916) 464-5045

Or

DCSS.InformationSecurityOffice@DCSS.CA.GOV



DCSS
INFORMATION SECURITY OFFICE

- ***Policy / Information Security Awareness***
- ***Risk Management***
- ***Program and Systems Security***
  - *Incident Management*
  - *Monitoring*
- ***Business Continuity***
- ***Compliance***
  - *Safeguard Reviews*

The DCSS ISO Program includes these functions to support the DCSS and LCSAs comply with State and Federal requirements.

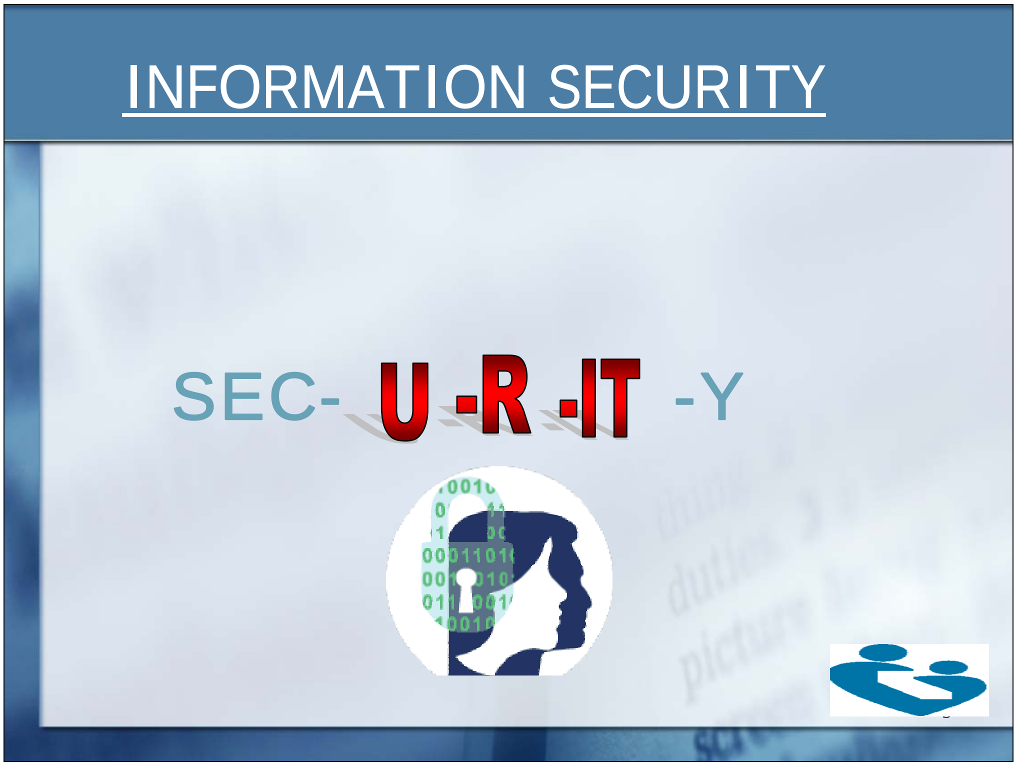
Policy / Information Security Awareness is responsible for developing Information Security policies, standards, guidelines and implementation tools to assist DCSS and LCSA implementation. This also involves the distribution and education/awareness of the policies for DCSS and LCSA.

Risk Management provides the methodology and support to assess program / technology processes and projects in identification of risks and mitigation plans to ensure acceptable security measures are implemented.

Program and Systems Security assists DCSS and LCSAs by providing advise and monitoring implementation of information security policy requirements. This includes incident management to ensure mitigation, tracking and reporting compliance.

Business Continuity provides the methodology and support to ensure planning and preparedness for continued availability of resources and services.

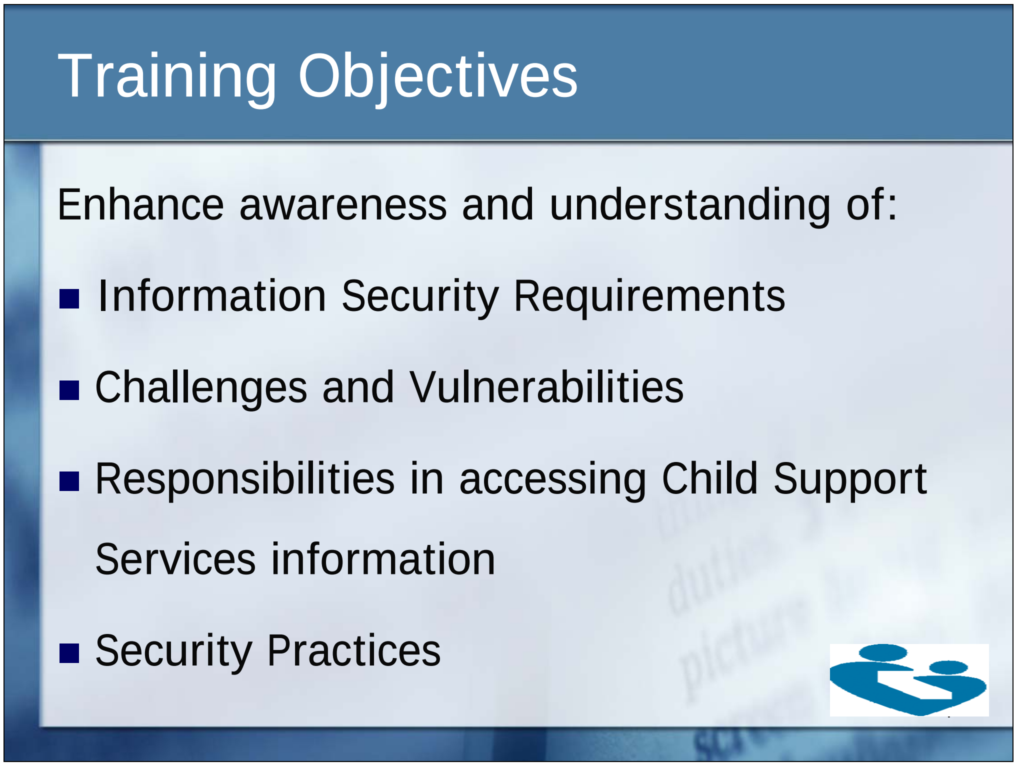
Compliance includes review of implemented policy for adherence to DCSS, State and Federal requirements.



INFORMATION SECURITY

SEC- U -R -IT -Y

The key to security awareness is embedded in the word security and “You” “Are” “it . The key to information security is: everyone taking responsibility to learn, understand and apply appropriate information security practices.



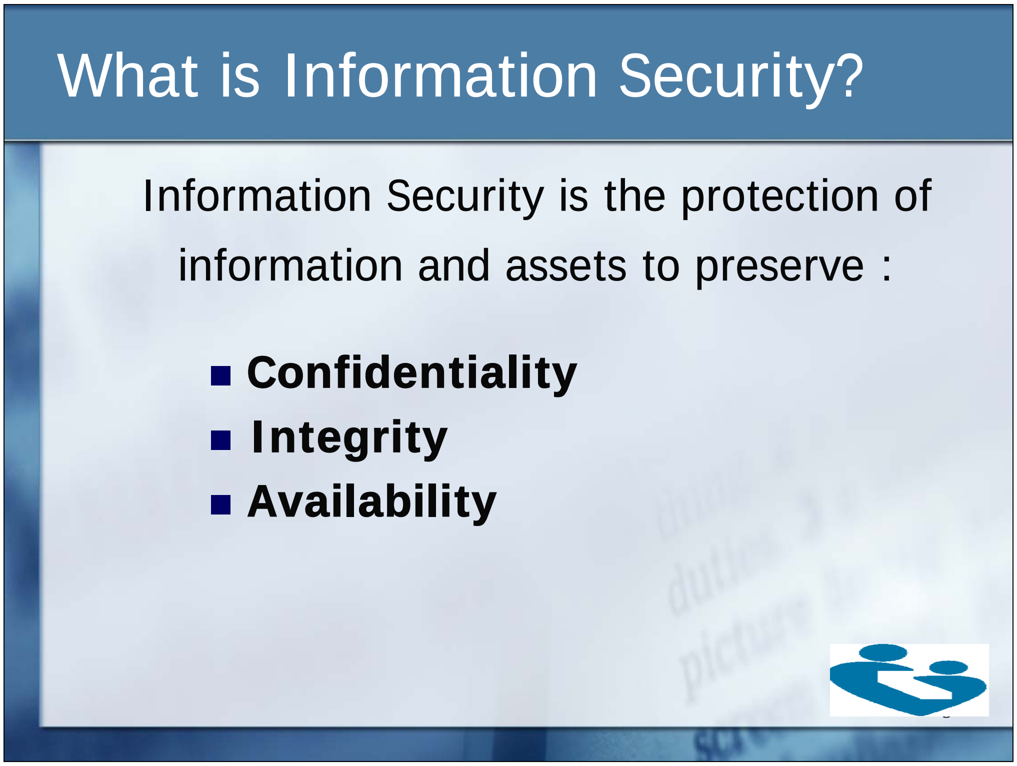
Training Objectives

Enhance awareness and understanding of:

- Information Security Requirements
- Challenges and Vulnerabilities
- Responsibilities in accessing Child Support Services information
- Security Practices

The enhanced awareness and understanding of :

- Why we must develop and implement information security.
- Compliance requirements and non-compliance consequences
- Security challenges and risks faced daily in the course of performing our work
- Your responsibilities in handling and protecting Child Support Services information
- What is defined as Information Assets, and
- The DCSS Information Security Policies and practices developed to help comply with Federal and State requirements



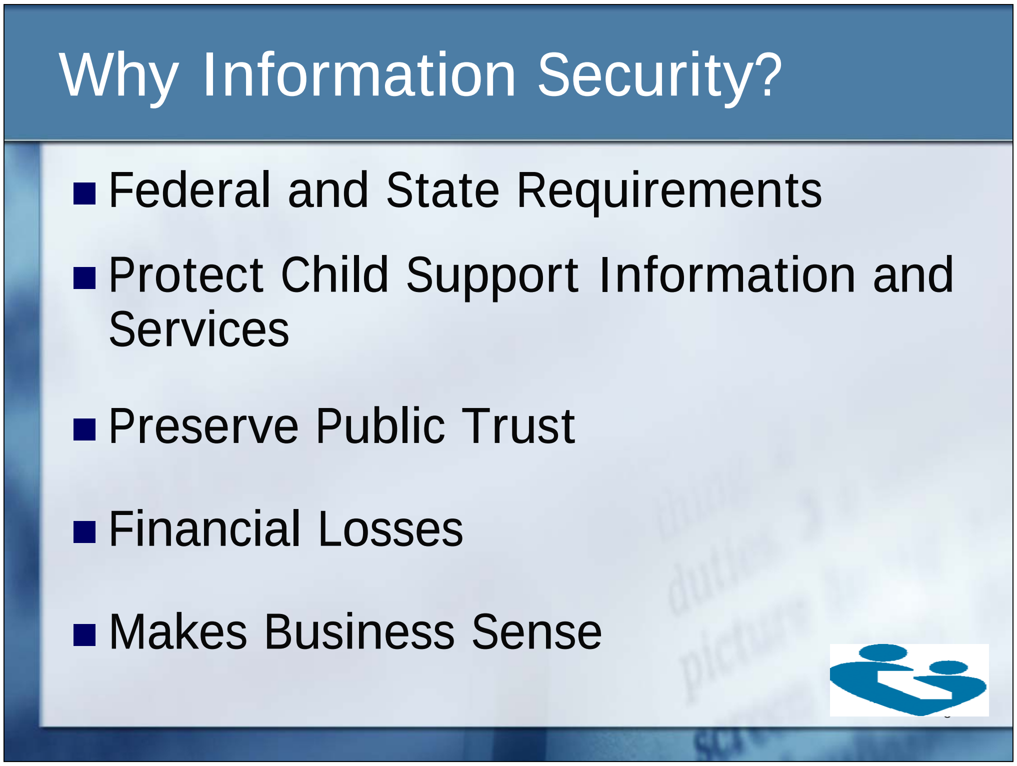
What is Information Security?

Information Security is the protection of information and assets to preserve :

- **Confidentiality**
- **Integrity**
- **Availability**

Information Security is

- Identifying and defining the value of information, data, systems, facilities, and other organizational resources
- Classifying those items to determine how to handle and protect them. These are the key protective elements:
  - Confidentiality: protecting information from inappropriate disclosure. Individually identifying information that if released could result in harm to a person or organization
  - Integrity: Keeping information correct and reliable by protecting it from unauthorized changes or manipulation
  - Availability: Protecting Child Support Information and Assets to ensure they are available when needed to perform work functions.

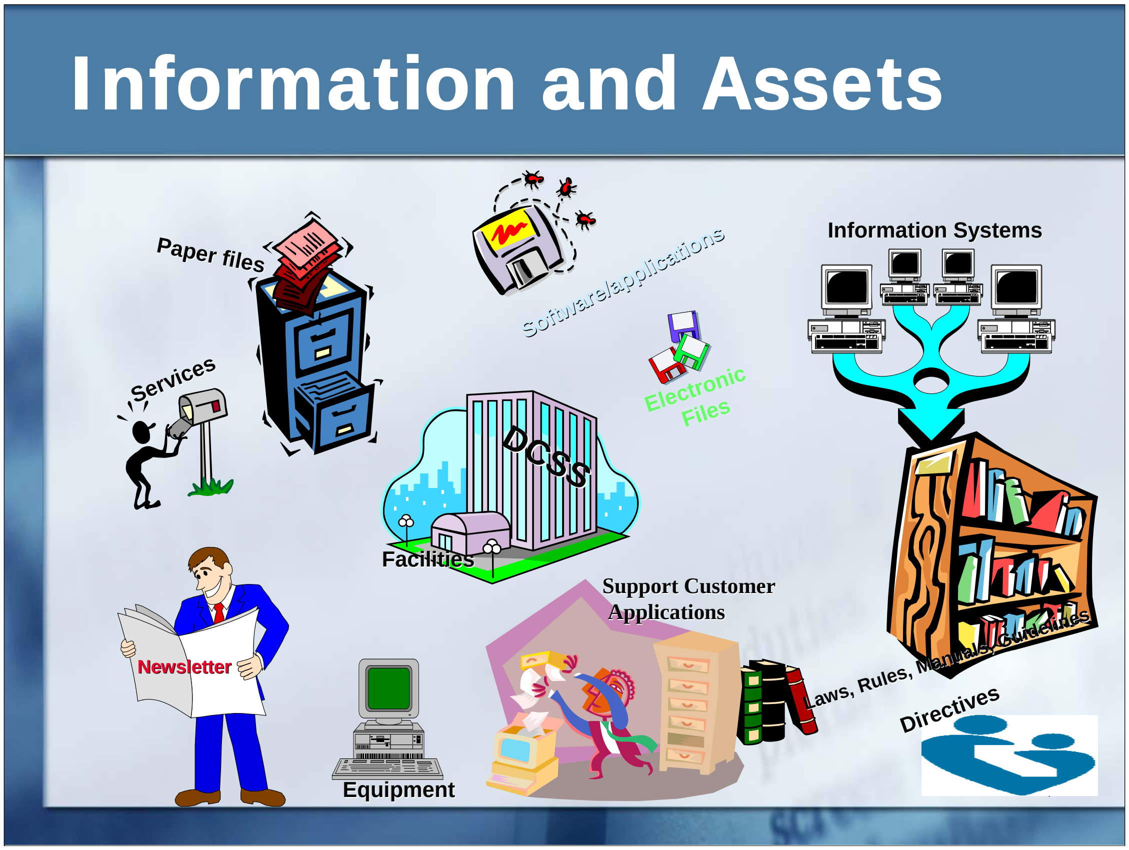


Why Information Security?

- Federal and State Requirements
- Protect Child Support Information and Services
- Preserve Public Trust
- Financial Losses
- Makes Business Sense

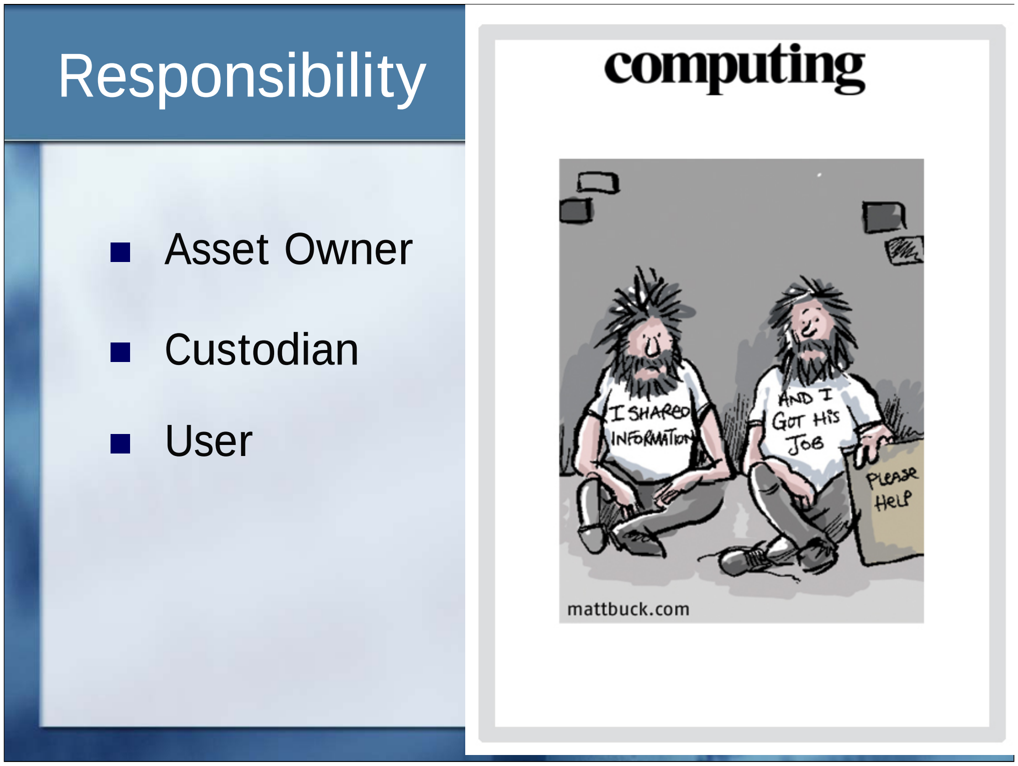
The need for Information Security:

1. DCSS's confidential information is protected by federal and state laws, regulations, and policies. Everyone (DCSS / LCSA, third party, contractors etc.) must comply with:
   - DCSS Information Security Manual
   - Federal Child Support Requirements- ACF guide to states; section H
   - IRS 1075 Safeguarding of Federal Tax Information
2. Information Security provides support in developing and implementing protective methods and processes to assure the confidentiality, integrity and availability of DCSS / LCSA information and resources.
3. DCSS gathers confidential information with the agreement it will be protected from inappropriate use. Protecting Child Support information, resources and services preserves public trust and the department's image.
4. Breach of information security requirements can include financial loss to the department, other private and government agencies. Breach may cause data loss, identify theft, the disruption of services, litigations and/or, civil liability or etc..
5. Protecting valued resources makes business sense.



Information and Assets

Information Assets include logical (soft copy, data, etc) and physical items. Information Assets include: customer data collected by DCSS to conduct business, the tools used to gather and process the data (computer systems, software, paper, etc.) the facilities that house the staff and data to support the Child Support program. These are information assets that are used to provide services to our customers and must be protected.



Responsibility

- Asset Owner
- Custodian
- User

Child Support Program managers authorized to develop and implement organizational (DCSS, LCSAs, business partners etc) data, systems, and processes are the asset owners. Sometimes the authority is delegated but overall responsibility to manage and protect the child support assets resides within the Child Support Program.

ULTIMATELY – IT IS EVERONE'S RESPONBILITY TO PROTECT DCSS INFORMATION

Asset / Data owners have responsibility to:

- Classify assets/data (Public, Confidential)
- Authorize assets/data access to user based on "need- to-know"
- Ensure confidentiality, integrity, availability.

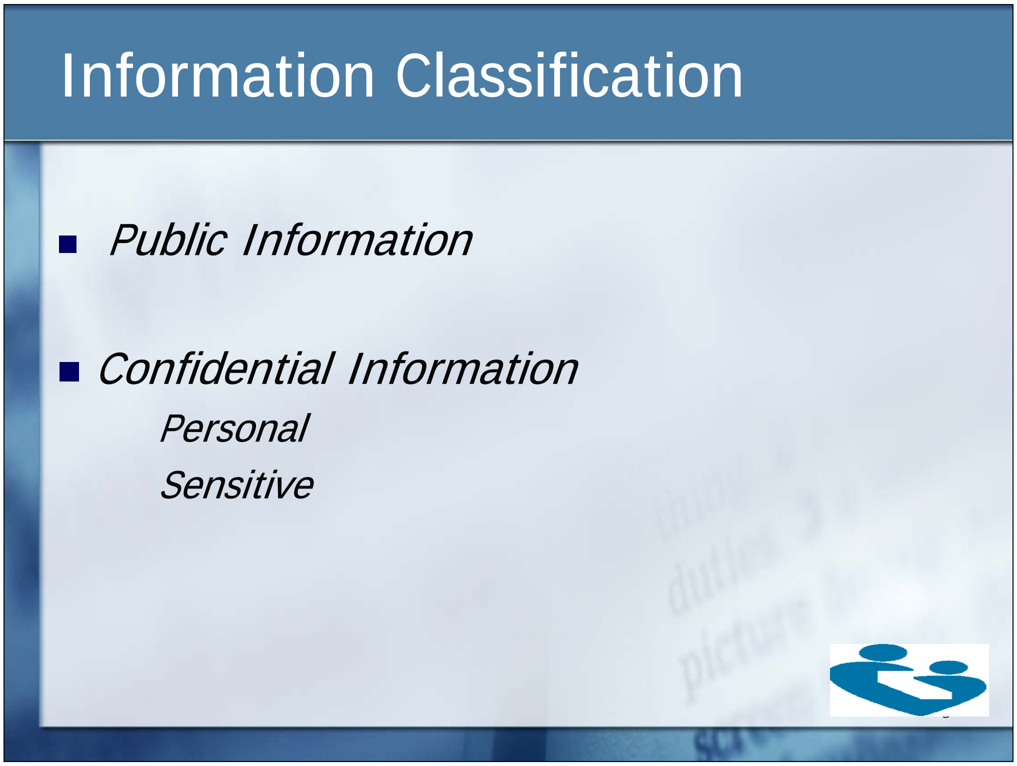
Asset Custodian (most commonly this responsibility resides with Information Technology area or the entity that provides IT services) have responsibility to:

- Protect the information and assets in their possession from unauthorized access, alteration, destruction or usage
- Establish and implement security counter measures agreed upon by the asset owner and consistent with policies and standards

User (s) have responsibility to:

- Access, process or handle ONLY authorized Child Support Information and Assets
- Apply good Information Security practices to their daily work and stay informed and knowledgeable on Information Security policy and procedures.
- Report possible Information Security issues.

Users may at times also have Custodian responsibility while traveling or transporting confidential information.



Information Classification

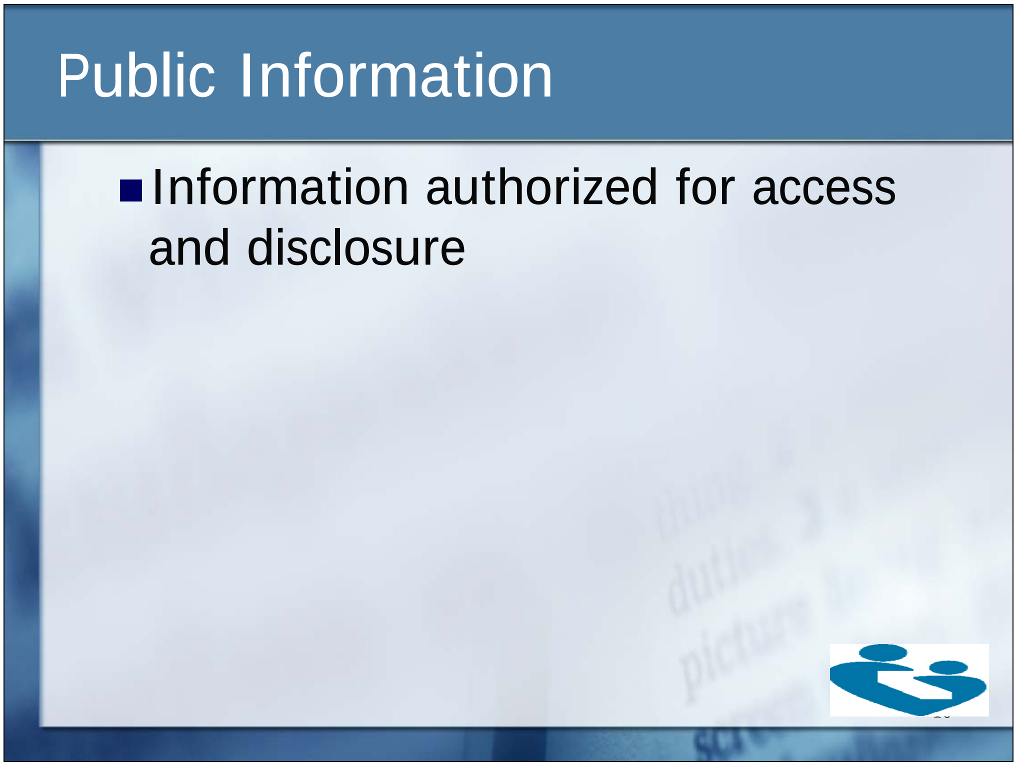
- *Public Information*
- *Confidential Information*
  - *Personal*
  - *Sensitive*

The CA State ISO has classified information and assets (files, data bases etc) into two categories: public and confidential.

Protection or handling of Information Assets is determined by each asset's classification

- Public: all information is available upon request unless it is exempt from disclosure per Federal and State Law. Such as Information Practices Act (IPA) and Public Records Act or other Program specific laws.
- Confidential - Protected by law for disclosure to only authorized entities or individuals.

Whenever you are unsure about the classification of information assets, check with Legal Counsel or the Information Security Office.



Public Information

- Information authorized for access and disclosure

As a public entity the DCSS must by law allow the public to inspect and or obtain copies of the work produced by the department unless it is exempted from disclosure by law.

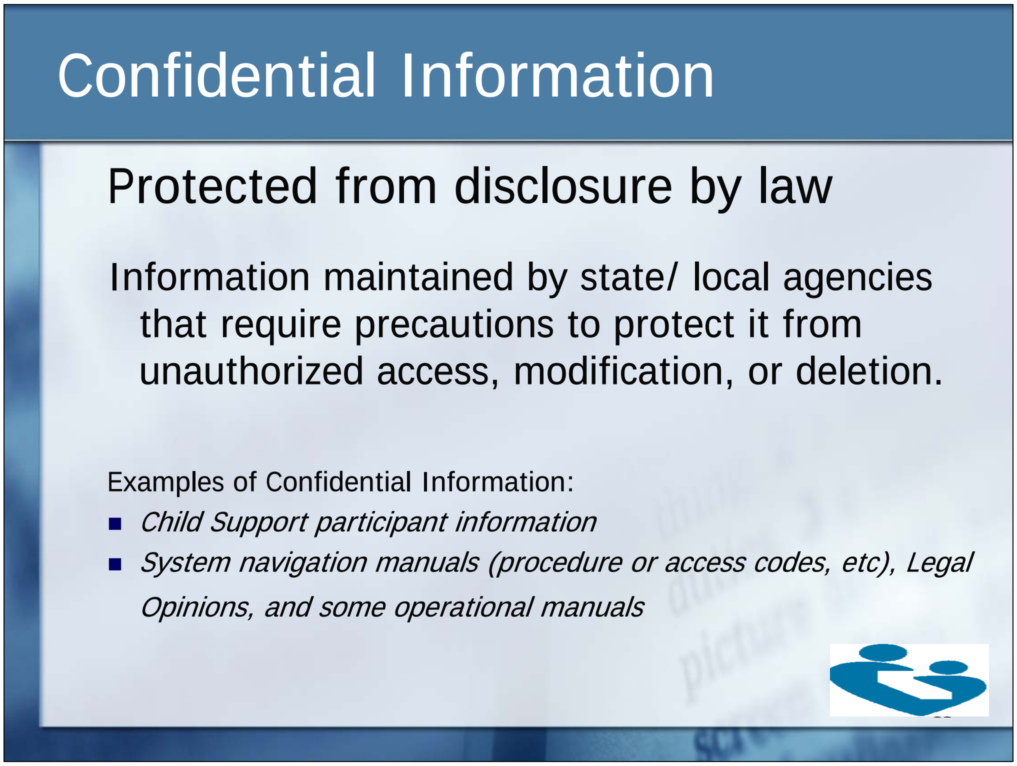
IT IS IMPORTANT TO PROPERLY CLASSIFY AND KNOW THE CLASSIFICATION OF INFORMATION FOR PROPER HANDLING AND DISCLOSURE

The Public Records Act makes most information collected and maintained by government agencies available to the public upon request

However, the law has important expectations to protect individual’s privacy and to ensure that government can conduct its business effectively and efficiently with public interest

Examples of Public information are: DCSS Information on the public internet, all communications and documents that are not classified as confidential or personal

It is the responsibility of the department to ensure that the information is accurate and made available when needed.



Confidential Information

Protected from disclosure by law

Information maintained by state/ local agencies that require precautions to protect it from unauthorized access, modification, or deletion.

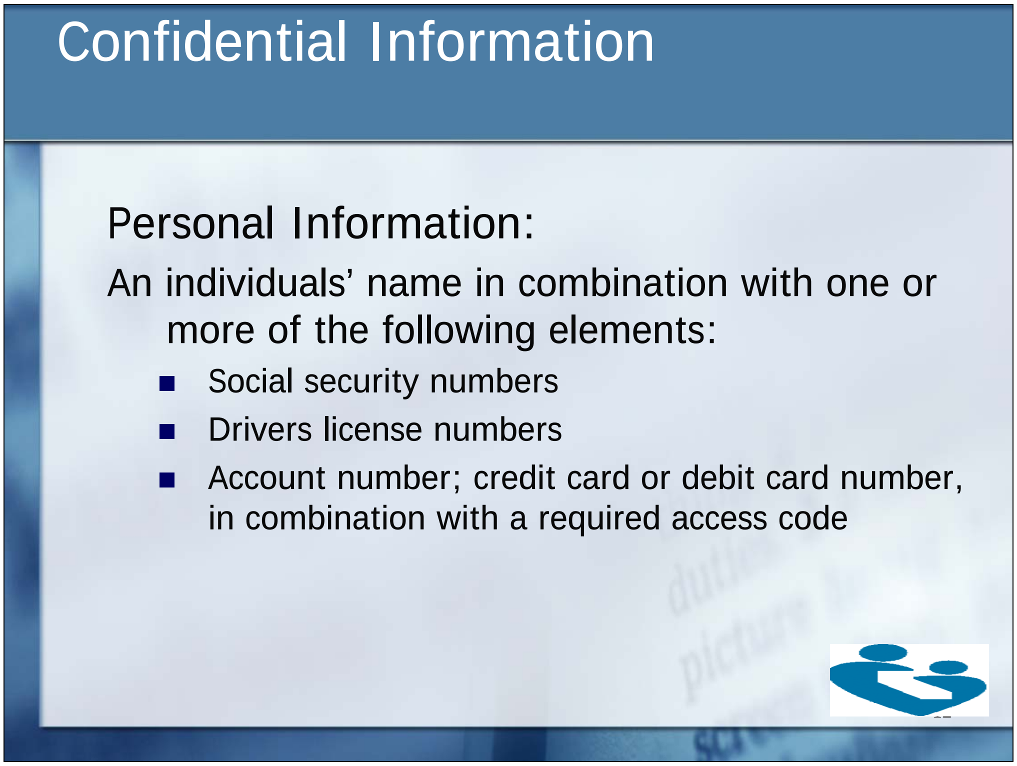
Examples of Confidential Information:

- *Child Support participant information*
- *System navigation manuals (procedure or access codes, etc), Legal Opinions, and some operational manuals*

The law has important expectations to protect individual privacy and to ensure that government can conduct its business effectively and efficiently with in the public interest

In general, any information that identifies an individual or provides personal information is confidential. In addition, information regarding the systems, networks or other assets that may be exploited to cause damage to the Child Support information is considered confidential and must be guarded from exposure to prevent any abuse or sabotage.   .

Information that is considered confidential in nature must only be accessed, used, copied, or disclosed by persons who have been authorized to access, use, copy, or disclose the information, and then only when there is an appropriate business need.



Confidential Information

Personal Information:

An individuals’ name in combination with one or more of the following elements:

- Social security numbers
- Drivers license numbers
- Account number; credit card or debit card number, in combination with a required access code

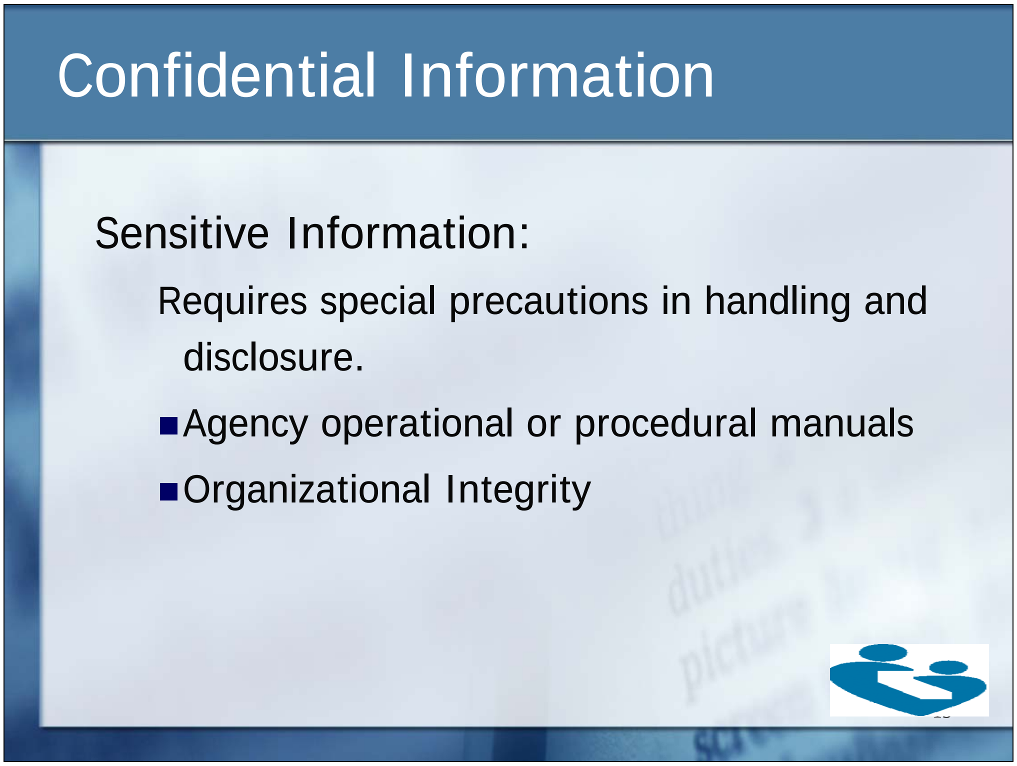
All personal information is confidential; however, not all Confidential information is Personal.

Personal information is a specific type of information about individuals which

if exposed or misused may cause significant damage to the individual whose information has been disclosed such as identity theft resulting in financial damages to the victim. Additionally, if Personal information is accessed by or disclosed to unauthorized person, the department is required by law to notify the affected persons of the disclosure and will result in additional cost to the department, affect department’s reputation, and loss of customer confidence.

Personal information as defined by statute includes an individual’s name in combination with any one of the following additional elements:

- Social Security Number
- Drivers license number
- Date of birth
- Bank accounts number with a password or access code



Confidential Information

Sensitive Information:

Requires special precautions in handling and disclosure.

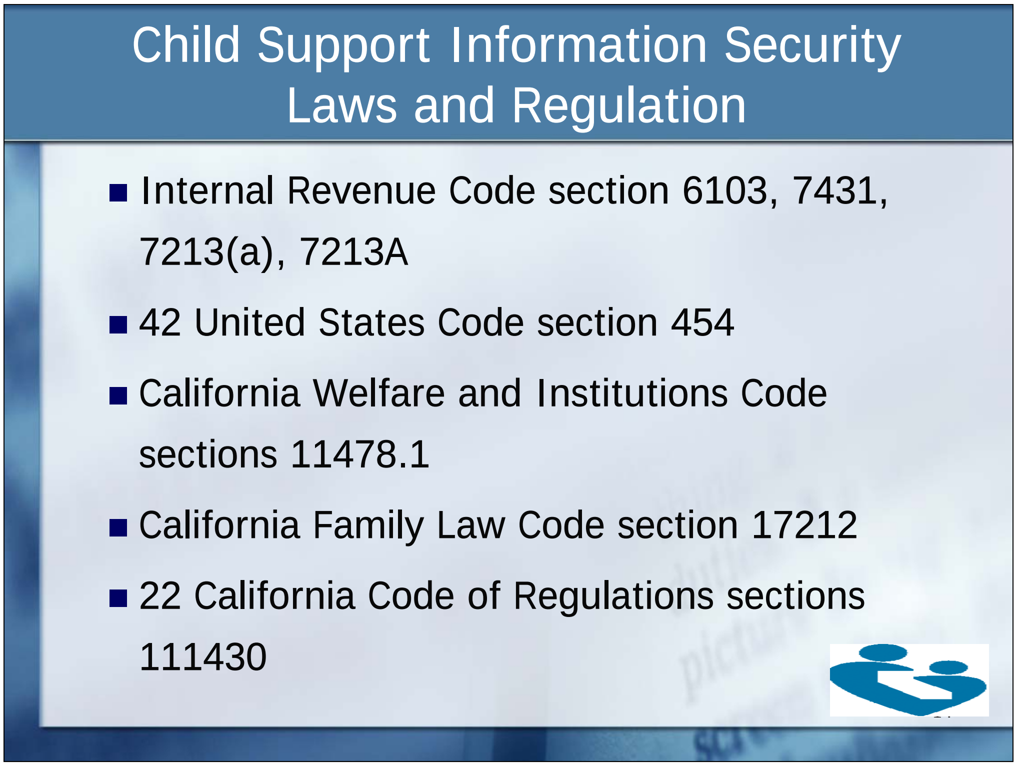
- Agency operational or procedural manuals
- Organizational Integrity

Confidential information **MAY** include data or documents that **IF** sanitized (confidential elements blocked, removed etc) MAY be released to the public.

Sensitive Information: Requires special precautions to protect from unauthorized use, access, disclosure or modification, loss or deletion.

For example organizational procedural manuals are sensitive and not for public release. But if organization specific data is blocked it could be shared as long as it didn't place the organization at risk or expose vulnerabilities.

Check with Legal Counsel or the Information Security Office to ensure appropriate disclosure.

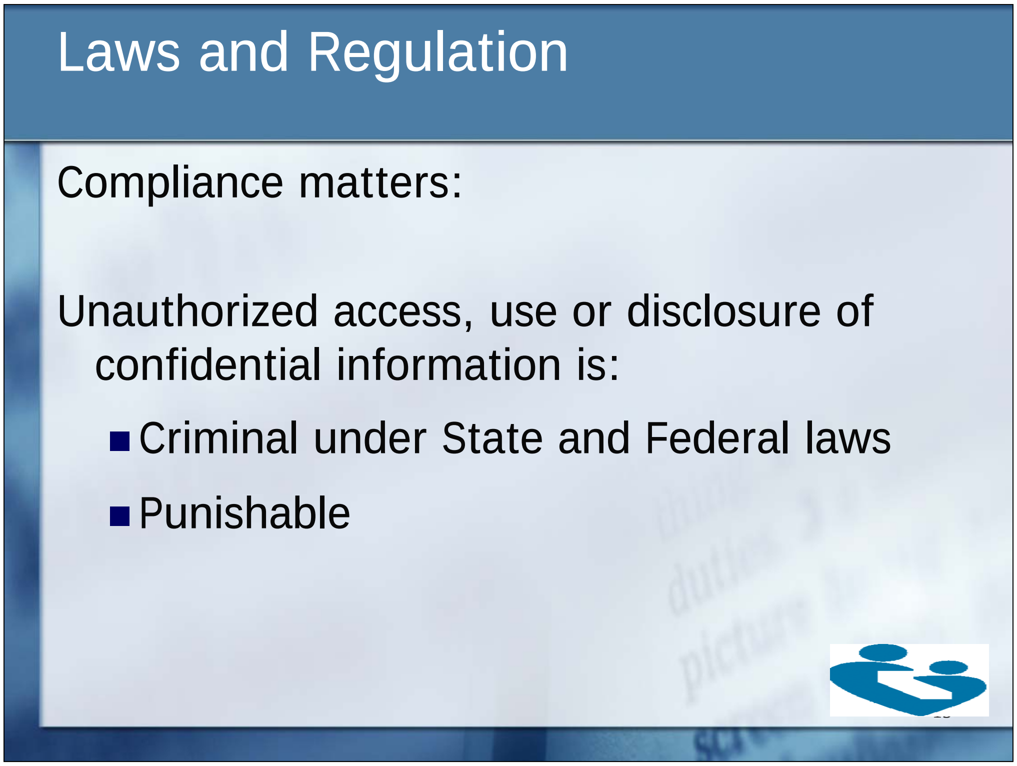


Child Support Information Security Laws and Regulation

- Internal Revenue Code section 6103, 7431, 7213(a), 7213A
- 42 United States Code section 454
- California Welfare and Institutions Code sections 11478.1
- California Family Law Code section 17212
- 22 California Code of Regulations sections 111430

These are laws specific to the Child Support Program restricting access and disclosure of Tax and Child Support information. Other State and Federal laws noted in the DCSS ISM or in other slides of the presentation, such as the California Privacy Law, work in conjunction to support the protection of DCSS and LCSA confidential information.

Since Child Support systems contain federal tax information all employees and contractors must follow procedures listed in the ‘IRS Publication 1075 - Tax Information Security Guidelines for Federal, State, and Local Agencies’



Laws and Regulation

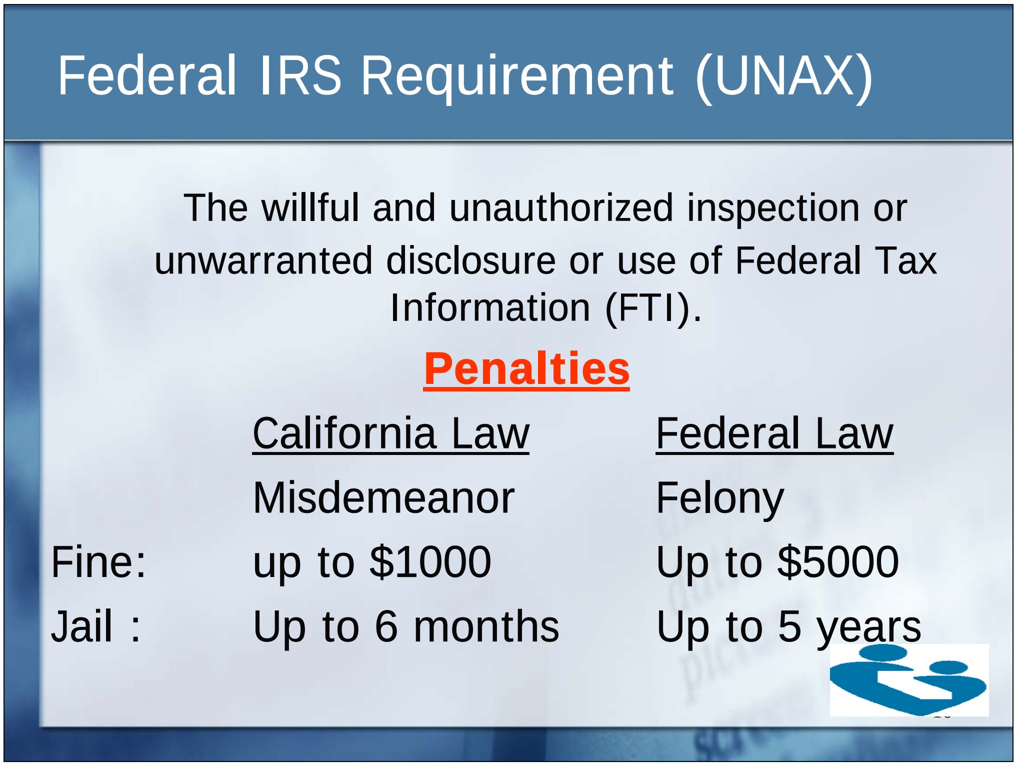
Compliance matters:

Unauthorized access, use or disclosure of confidential information is:

- Criminal under State and Federal laws
- Punishable

Compliance matters because Federal and State laws indicate potential liability and criminal prosecution as a result of violating information security.

Unauthorized access, use, or disclosure is a crime under state and federal law. Anyone, (employees, employers, third party, or contractors) violating confidentiality may be subject to administrative actions such as informal and formal for discipline, employment/contract termination etc, such violations are also punishable by law.



Federal IRS Requirement (UNAX)

The willful and unauthorized inspection or unwarranted disclosure or use of Federal Tax Information (FTI).

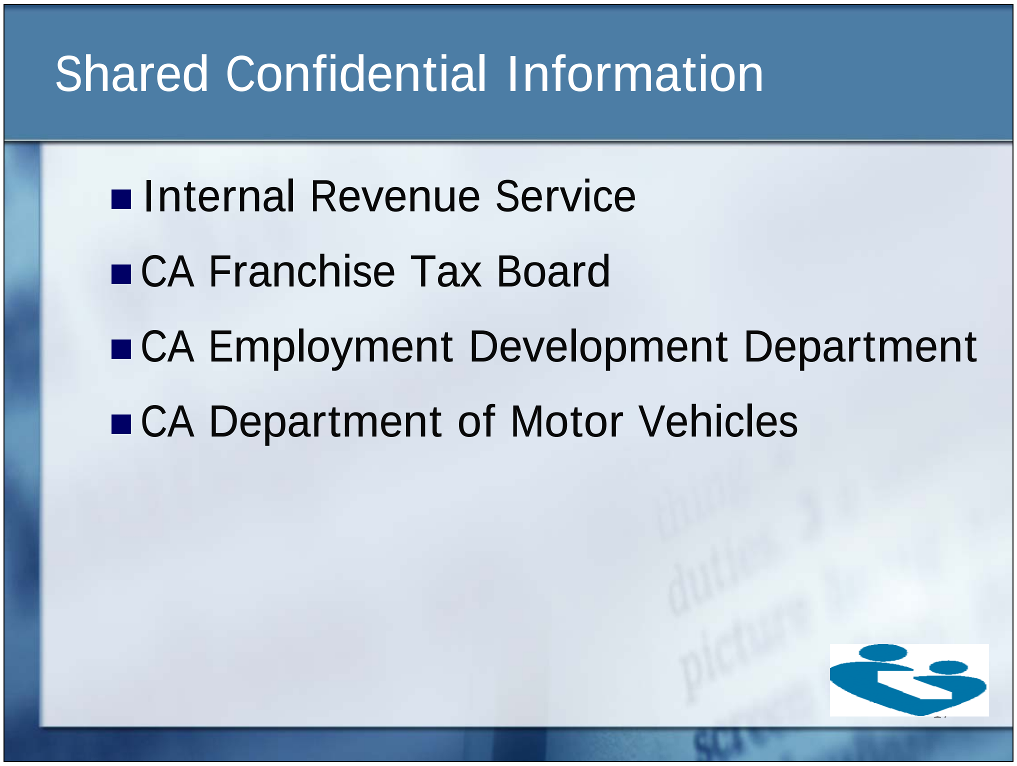
Penalties

	California Law	Federal Law
	Misdemeanor	Felony
Fine:	up to $1000	Up to $5000
Jail :	Up to 6 months	Up to 5 years

Internal Revenue Services violations can result in penalties for unauthorized access under the Federal and California jurisdiction. These penalties can compound if the violation involves California government computers or resources.

Under the California law, each unauthorized disclosure is a misdemeanor, punishable by a fine of up to $1000, and incarceration of up to 6 months for each record being disclosed.

Under Federal law, each unauthorized disclosure is a felony, punishable by a fine of up to $5000, and incarceration of up to 5 years in prison for each record being disclosed.



Shared Confidential Information

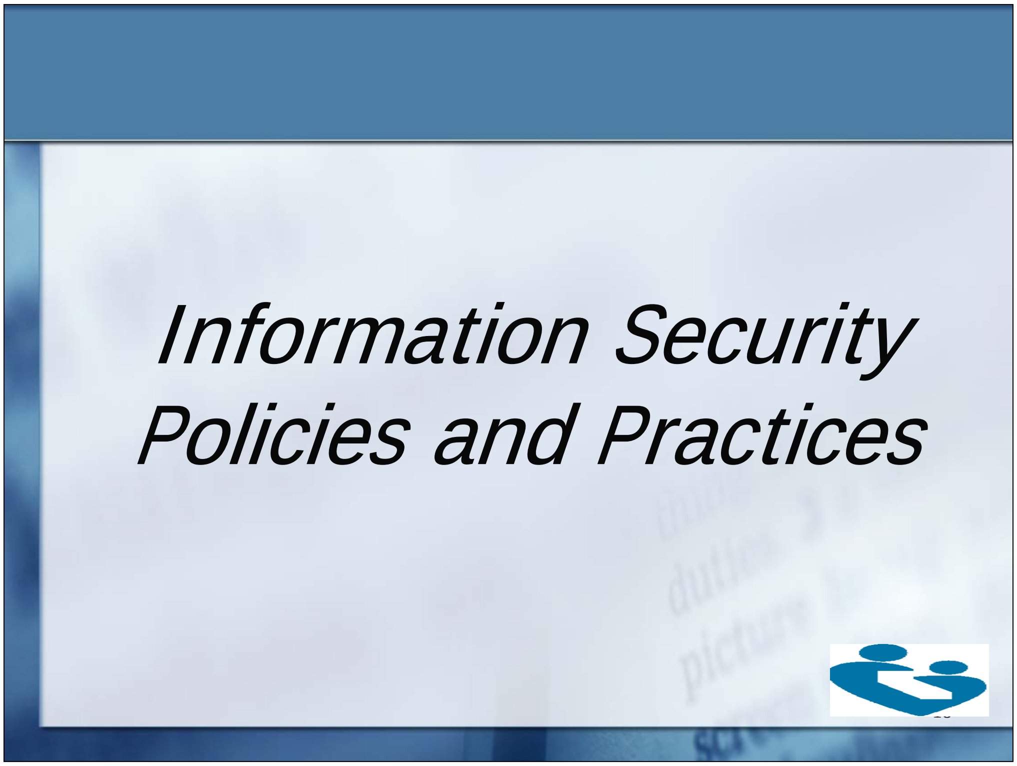
- Internal Revenue Service
- CA Franchise Tax Board
- CA Employment Development Department
- CA Department of Motor Vehicles

As part of doing child support business, information is sometimes shared with authorized state and federal entities.

As such, access to Department of Child Support Services by partner entities falls under Federal and State laws and is required by law to be protected.

Child Support systems process and store information obtained from the IRS, Social Security Administration, Office Child Support Enforecement, OCSE , CA Franchise Tax Board, CA Employment Development Department, and CA Department of Motor Vehicles.

A violation involving Child Support information and resources may be subject to laws and regulation of these partner agencies. It is our responsibility to protect this information.



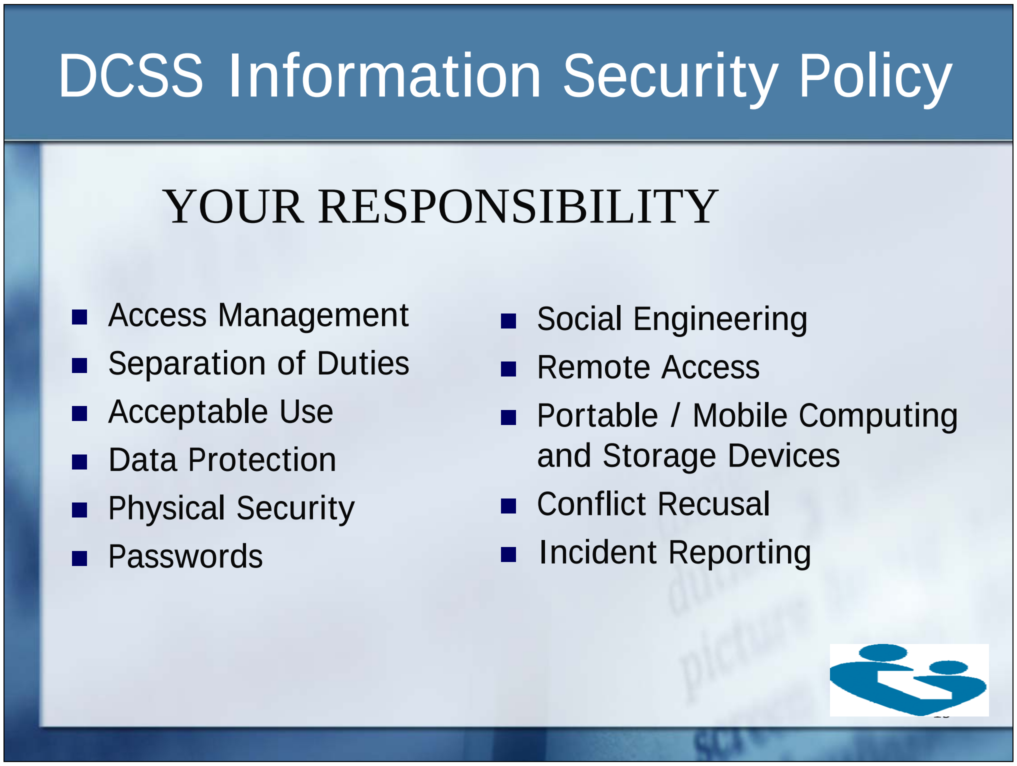
Information Security Policies and Practices

The DCSS ISM applies to everybody with access to Child Support information and assets (all DCSS staff, LCSA, 3rd Parties, Service Providers, etc…).

The following information security policies and practices are a sample and provide guidance on how to protect information assets.

Other tools and examples are expected to be provided via the DCSS Information Security web site to assist in the implementation of the Information Security Program.

The complete DCSS ISM is available on the LCSA secure web site for review and understanding of all DCSS policy, standards, and guidelines. If you do not have access, ask your manager to get you a copy of the DCSS ISM.



DCSS Information Security Policy

YOUR RESPONSIBILITY

- Access Management
- Separation of Duties
- Acceptable Use
- Data Protection
- Physical Security
- Passwords
- Social Engineering
- Remote Access
- Portable / Mobile Computing and Storage Devices
- Conflict Recusal
- Incident Reporting

You are responsible for protecting Child Support information and assets. Your role in securing the department's resources may vary depending on your job functions and the level of access given to you.

However, we all have a responsibility to protect the Child Support information and resources. DCSS ISM contains security policies, standards and other security documents that all Child Support staff must abide.

Access Management

Golden Rule

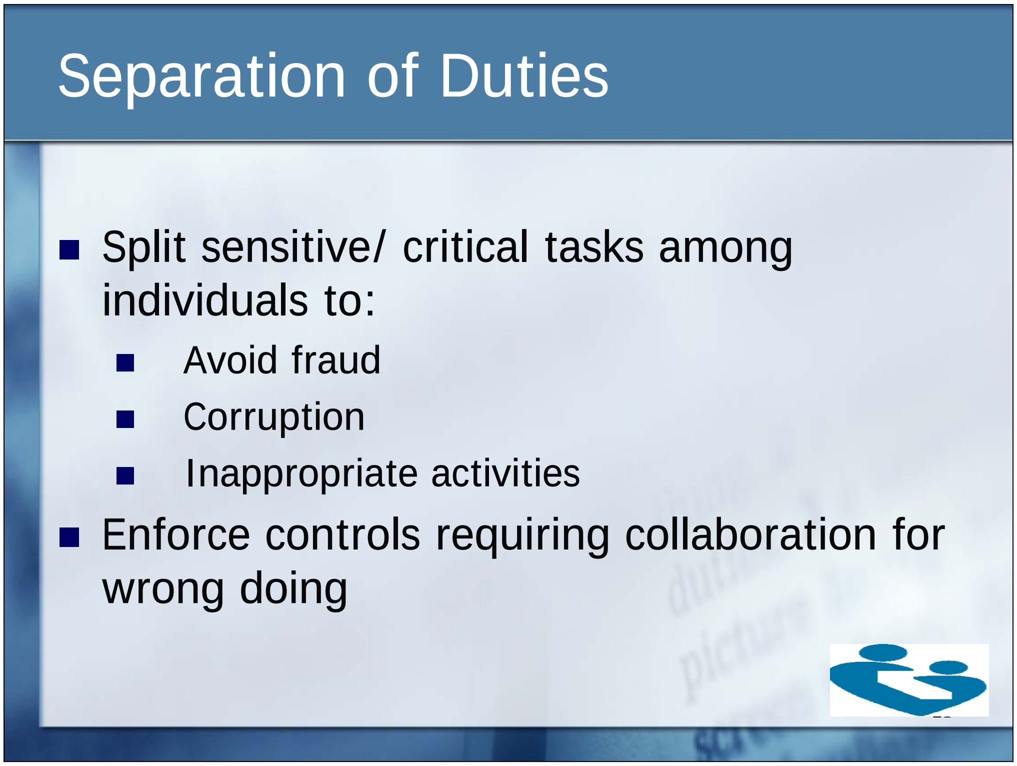
Acceptable Use

- Need to Know
- Authorized

Managing the access to confidential information is an important step to its protection. Reviewing and authorizing employee need-to-know based on work function and updating their access is a key element in ensuring acceptable use. Prior to accessing the Child Support Information and Assets, the individual must:

1. Have received security awareness training and
2. Signed a DCSS Confidentiality statement and UNAX forms.
   Authorized users may access the specific information and assets that are needed to perform their assigned job.

Example: if your job is to locate individuals, you may look at the screens that describes child support participants, their addresses and employers, etc. However, you may not look at screens that describe participants financial information.



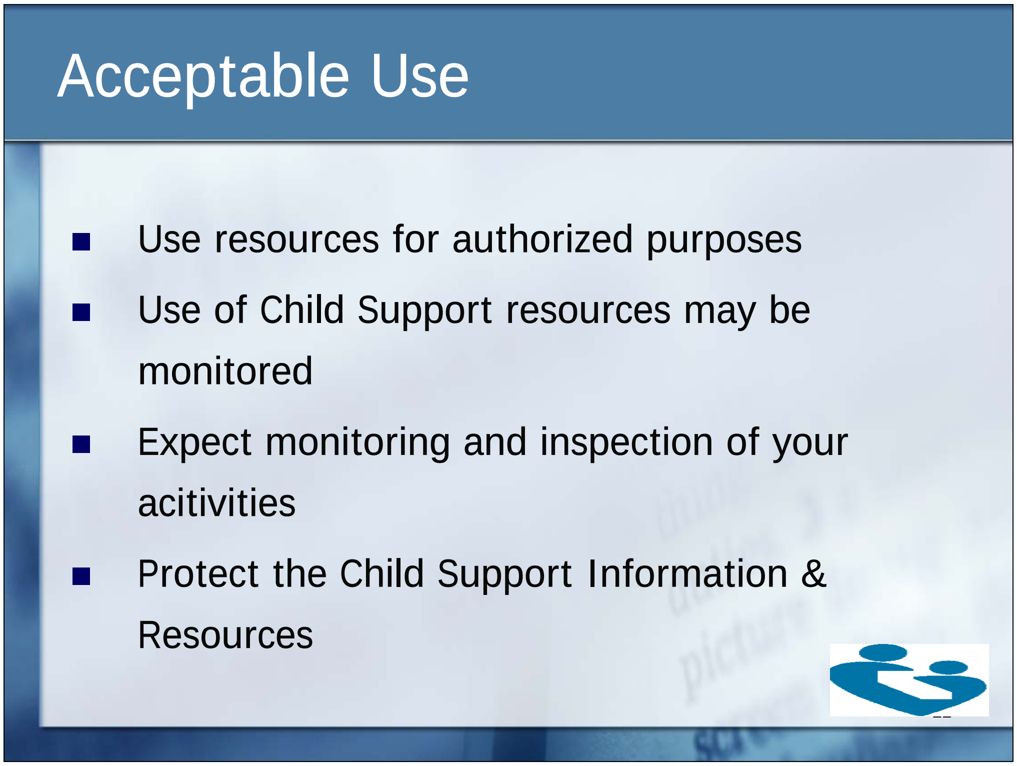
Separation of Duties

- Split sensitive/ critical tasks among individuals to:
  - Avoid fraud
  - Corruption
  - Inappropriate activities
- Enforce controls requiring collaboration for wrong doing

Separation of duties segregates responsibilities and tasks of work functions among different individuals.

The intent is to ensure data, system and process integrity via process and administrative controls. This protects the organization and employee from unauthorized or accidental activities such as data loss, system compromise, fraud, corruption and/or other inappropriate activities.

This approach provides additional mechanisms through processes and procedures, as opposed to reliance on system enforced controls.



Acceptable Use

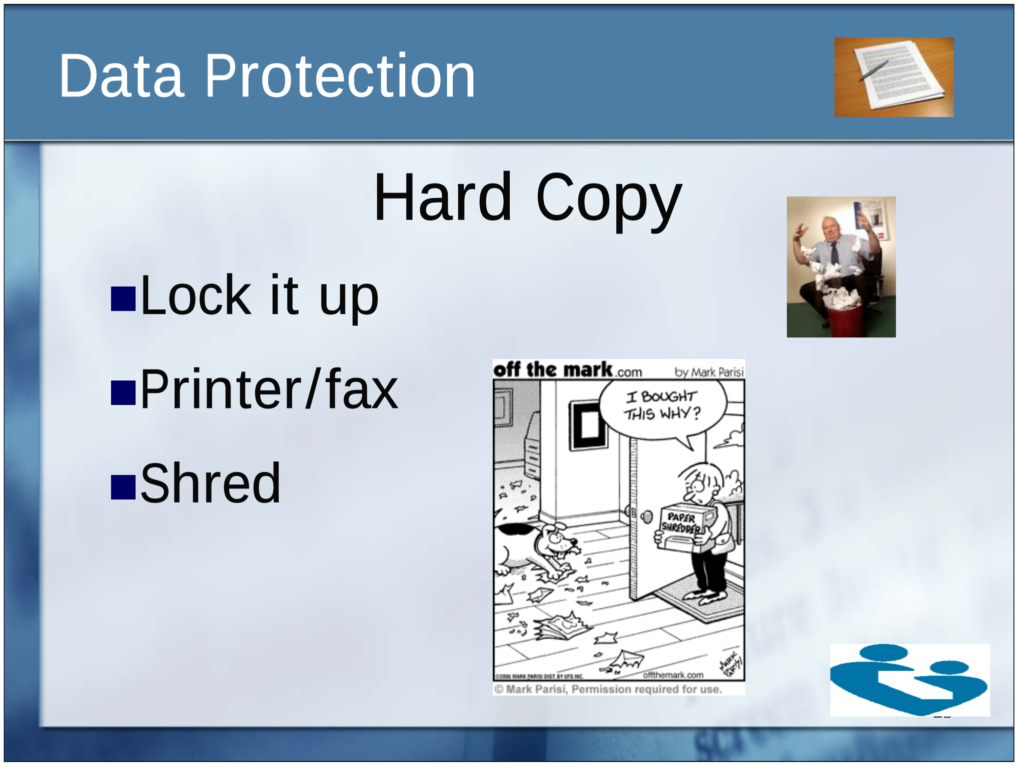
- Use resources for authorized purposes
- Use of Child Support resources may be monitored
- Expect monitoring and inspection of your acitivities
- Protect the Child Support Information & Resources

DO NOT Expect Privacy when accessing Child Support systems.

Your activities on department systems are monitored, logged and can be recovered without notifying you.

Your organization is required to cooperate with any investigation of security breaches involving your organization.

The content of your email messages or activities are open for review, monitoring, investigation and may be given to law enforcement or other officials in the event of a legal investigation.



Data Protection

Hard Copy

- Lock it up
- Printer/fax
- Shred

off the mark.com by Mark Parisi
I BOUGHT THIS WHY?
PAPER SHREDDER
offthemark.com
© Mark Parisi, Permission required for use.

All data , both. electronic and hard copy, must be protected:

•Hard copy must be protected while in use – lock up confidential, personal and Federal Tax information when leaving your work area

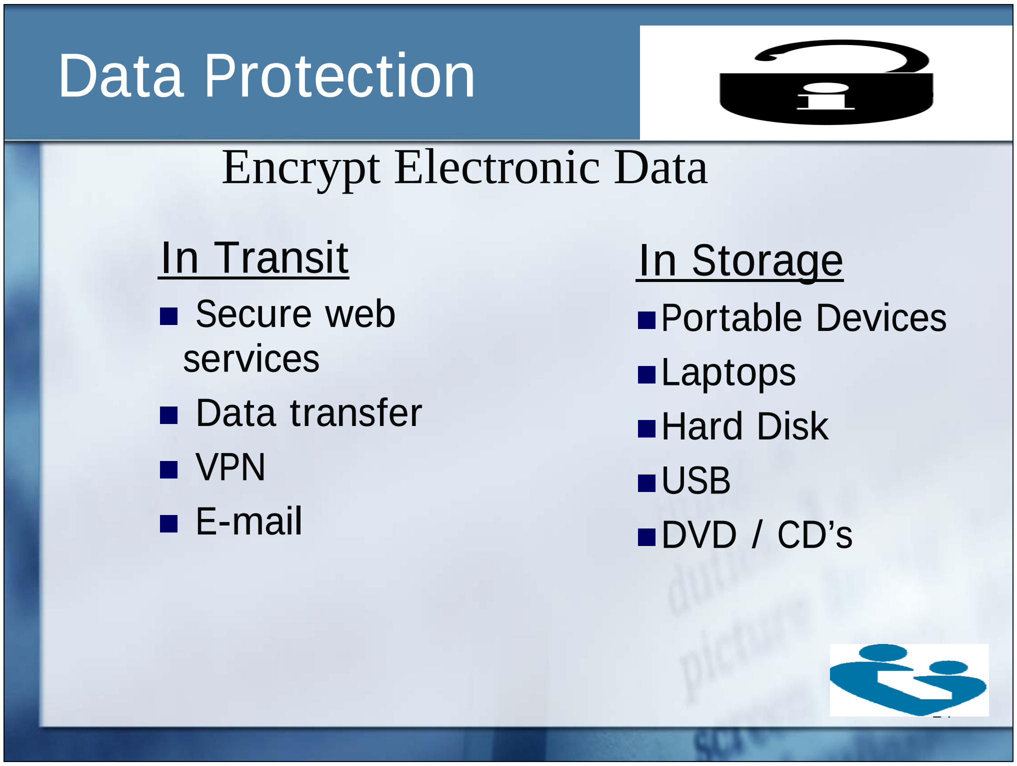
•Don’t leave documents on the printer or fax

•Place fax and printers in secure area – don’t place them in the busy walkways

•Shred hardcopies when not needed – don’t throw them in trash or recycle bin.

•Do not keep confidential and sensitive information longer than needed – shred unneeded media to avoid exposure.

Remember to keep material according to their retention schedule and ensure appropriate protection and disposal.



Data Protection

Encrypt Electronic Data

In Transit

- Secure web services
- Data transfer
- VPN
- E-mail

In Storage

- Portable Devices
- Laptops
- Hard Disk
- USB
- DVD / CD's

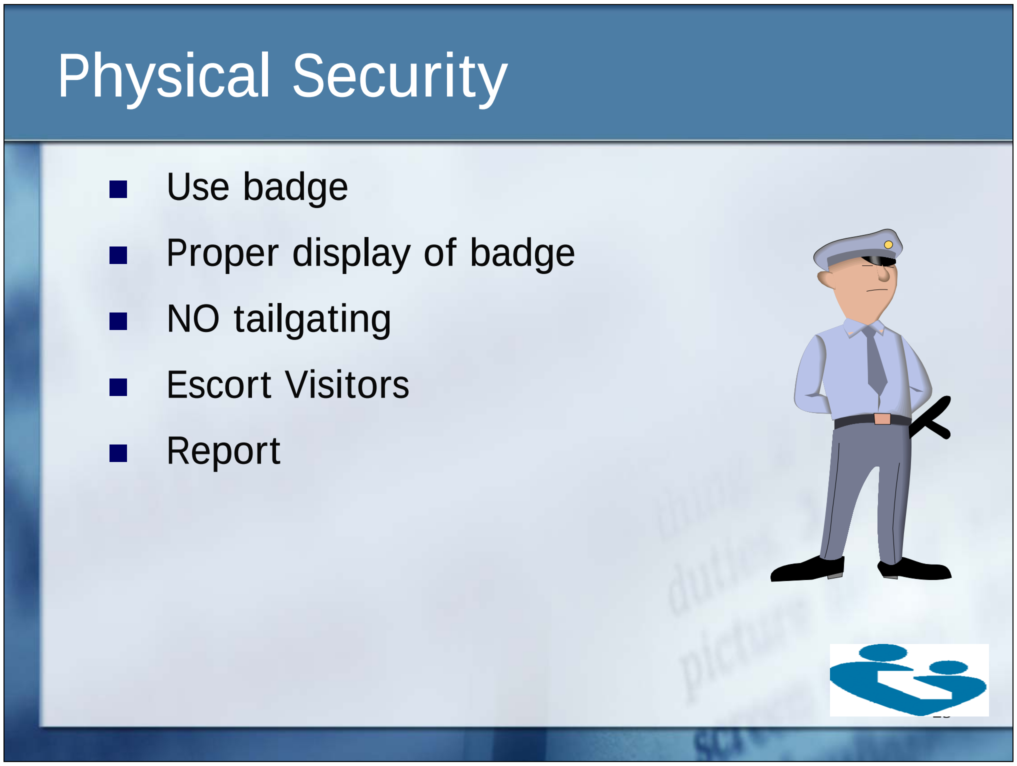
Protect confidential and personal information in all phases and forms i.e. in transit, in storage and in use and in electronic.

Review the business need for transmitting or storing confidential information in other than established secure organizational methods to determine if the risk of loss, theft or disclosure is acceptable.

Confidential information must be encrypted in transit.

All laptops, DVDs, CD and flash drives should be encrypted must if personal information.

Develop a habit of regularly purging documents and removing information that is no longer needed. This also helps maintain storage capabilities on laptops, USB flash drives or other portable devices.



Physical Security

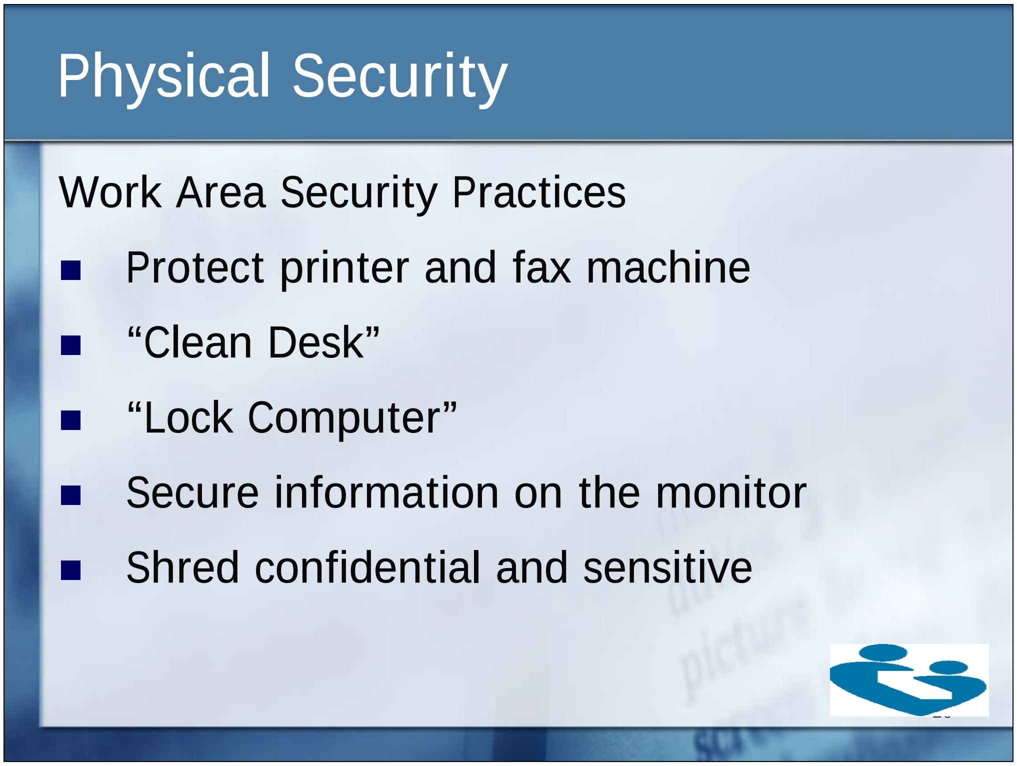
- Use badge
- Proper display of badge
- NO tailgating
- Escort Visitors
- Report

Physical Security is one of the first layer of protection from unauthorized access.

Organizations that have access to Child Support Information must incorporate physical security practices.

For example, the organization must identify areas of the facilities where confidential information is accessed and processed. The organization must construct physical barriers to restrict unauthorized persons from those areas. Such areas can be protected at the minimum by limiting access only to the authorized individuals by employing badge access controls and escorting visitors.

It is your responsibility to challenge un-badged / unauthorized individuals in restricted areas. As a way to validate their authority to be in the restricted area ask to see their badge. If a person is lost, escort them to the person identified as their contact. Or if an individual cannot produce a badge, report the incident to your supervisor or organization’s ISO or contact security guard.



Physical Security

Work Area Security Practices

- Protect printer and fax machine
- “Clean Desk”
- “Lock Computer”
- Secure information on the monitor
- Shred confidential and sensitive

Secure confidential information in your work area:

DO NOT leave confidential or personal information unattended – in the work area, on the printer, or on the fax machine.

•Practice a clean desk strategy. When you leave your desk, make sure your desk is clear of all confidential and personal information.

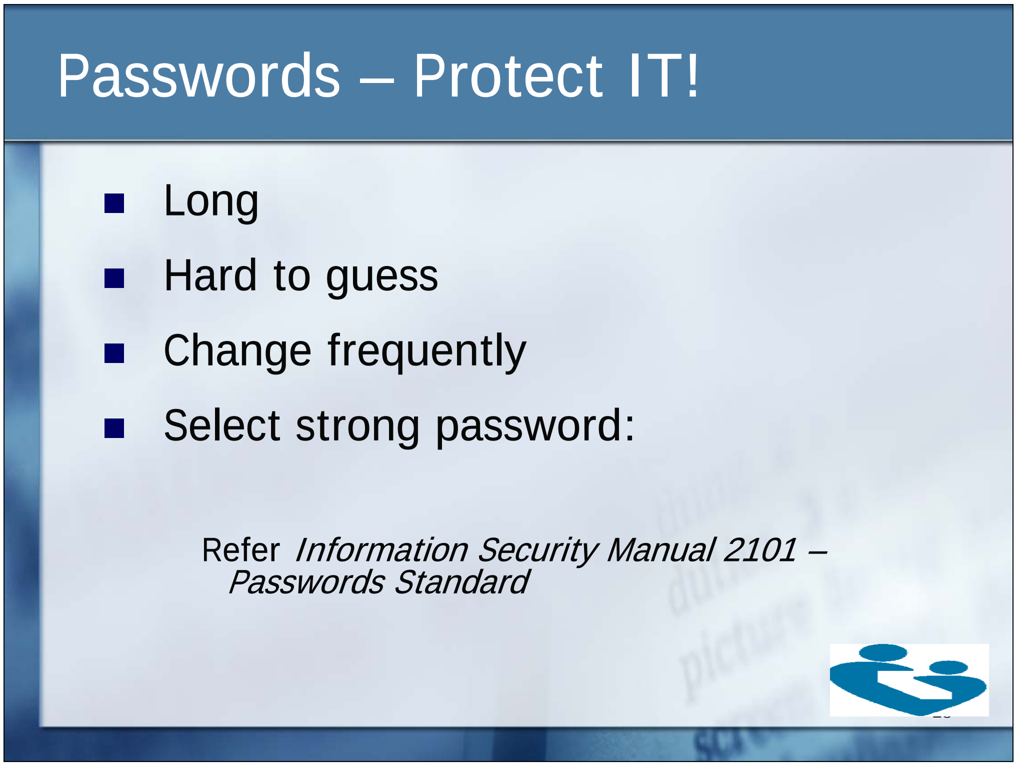
•Lock your computer when you leave it. If you do not do this, others may access unauthorized information. To lock your computer, press Control, Alt Delete simultaneously and then click on “Lock Computer.”

•If you receive confidential information by fax frequently, and you share your fax machine with others, make sure the machine is located in a low traffic area.

•If you send faxes containing confidential information, verify the number and arrange fax delivery with the sender to ensure that it is immediately removed from the fax.

Keep personal/confidential information only as long as needed. Arrange your work space so that your monitor cannot be viewed easily by unauthorized persons.

BAD NEWS! OUR ID's BEEN STOLEN!
THE GOOD NEWS IS THAT IT TOOK THEM TWICE AS LONG, THOUGH.
MICROSOFT VISTA
STAHLER. 2007.



Passwords – Protect IT!

- Long
- Hard to guess
- Change frequently
- Select strong password:

Refer *Information Security Manual 2101 – Passwords Standard*

Access to child support systems requires an individually assigned identifier (user id) and password. Protect your access and password.

Use strong passwords such as pass phrases, Ex: Mary have a little lamb, and passwords with upper and lower case letters, numbers and special characters.

Change your password frequently. If you believe your password has been compromised, change your current password immediately.

DO NOT:

- use User ID as password or write down your password
- share your password with anyone
- use your e-mail name as password
- use dictionary words, kids or pets names
- store passwords in unprotected files

Check the strength of your password at:
http://www.microsoft.com/athome/security/privacy/password_checker.mspx

Passwords

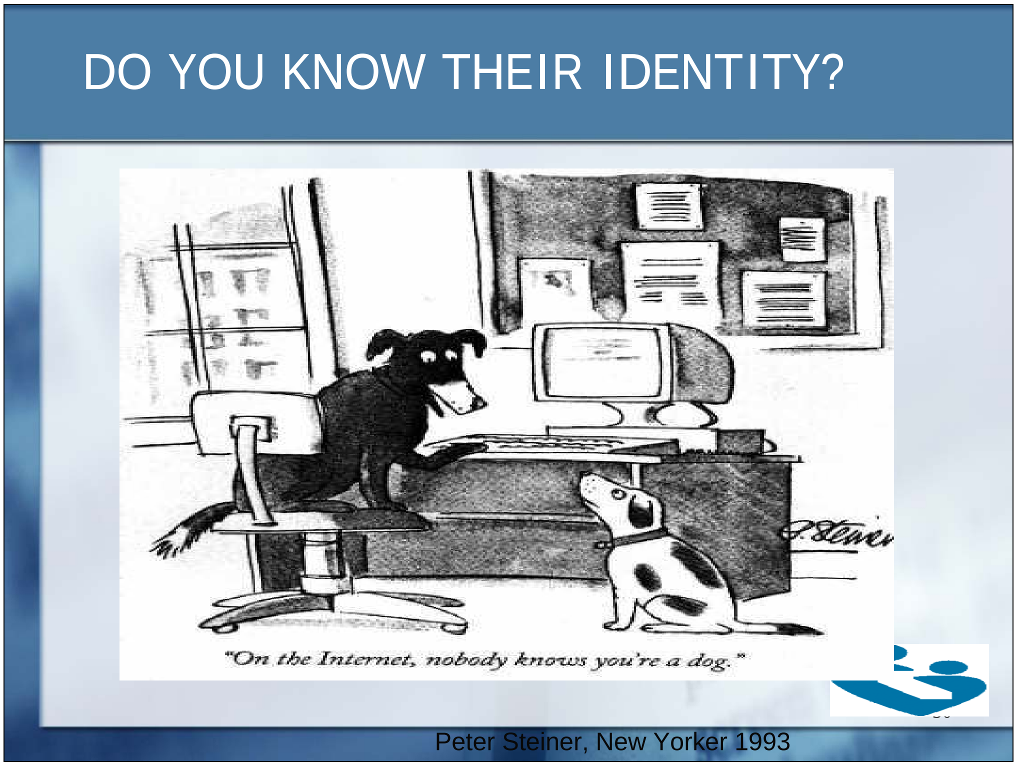
You are personally responsible and accountable for all activity occurring under your User ID and password.

Protect Your Password

You are personally responsible for any activity on the child support systems under your user ID and password. So---

Protect your PASSWORD!!

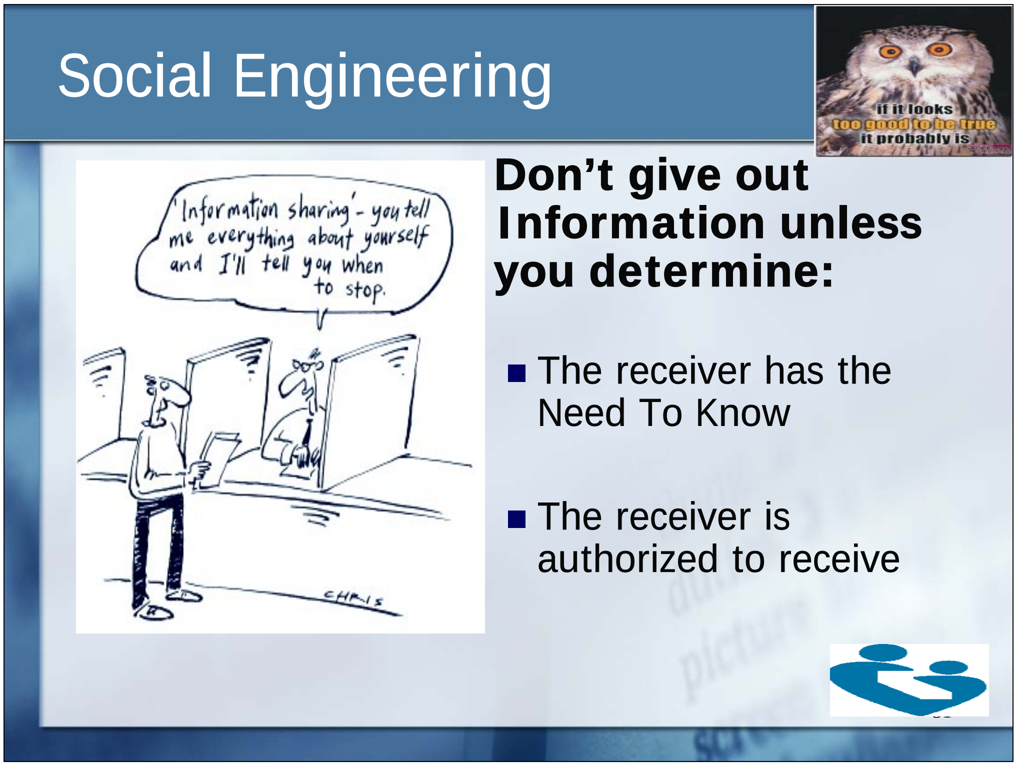
Any users account User ID(s) and Password(s) that is/are assigned to you to perform your work, you must ensure their protection by adhering to DCSS's security policies.



DO YOU KNOW THEIR IDENTITY?

Peter Steiner, New Yorker 1993

No body knows on the internet who they are dealing with – ….



if it looks
too good to be true
it probably is
'Information sharing' - you tell me everything about yourself and I'll tell you when to stop.
CHRIS

Social Engineering

Don't give out Information unless you determine:

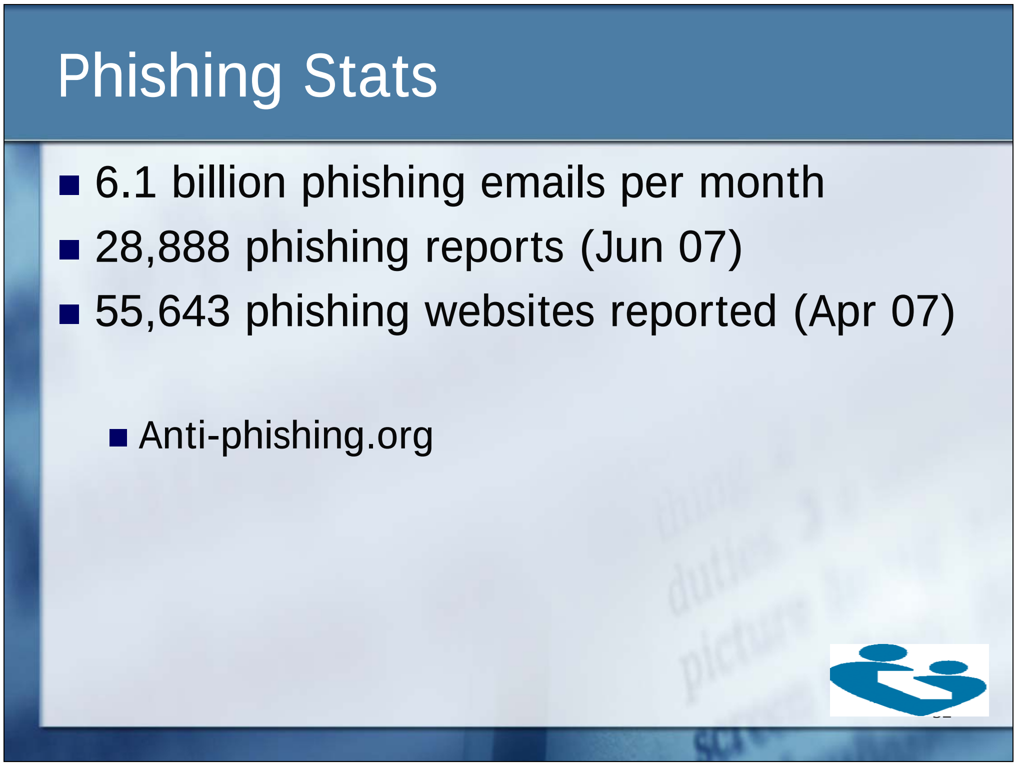
- The receiver has the Need To Know
- The receiver is authorized to receive

Social engineering involves obtaining information by manipulating legitimate information and deceiving an authorized user to release confidential information or allow unauthorized access. Be cautious and alert about giving out information.

Don't give out confidential information or personal information over the phone without verifying identity of the user.

Ensure the user has the authority and the need to receive information.

If you have any doubts about the caller talk to your supervisor.

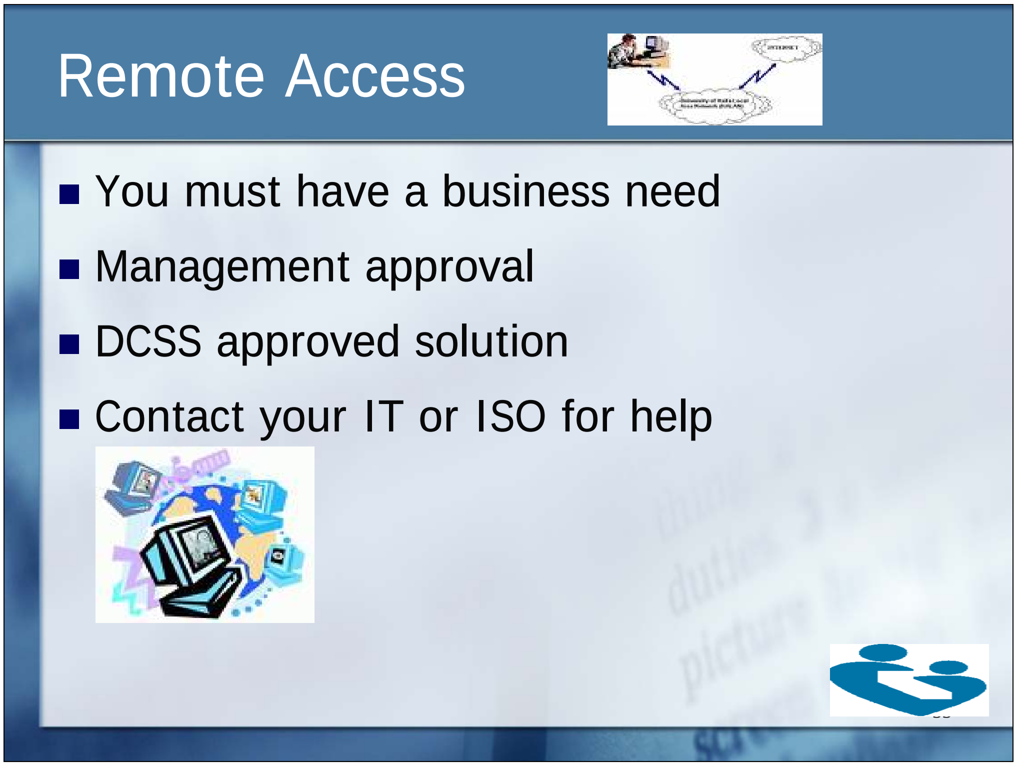


Phishing Stats

- 6.1 billion phishing emails per month
- 28,888 phishing reports (Jun 07)
- 55,643 phishing websites reported (Apr 07)
  - Anti-phishing.org

(fish´ing) **(n.)** The act of sending an e-mail to a user falsely claiming to be an established legitimate entity in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security and bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the user’s information.

Phishing, also referred to as *brand spoofing* or *carding*, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.



Remote Access

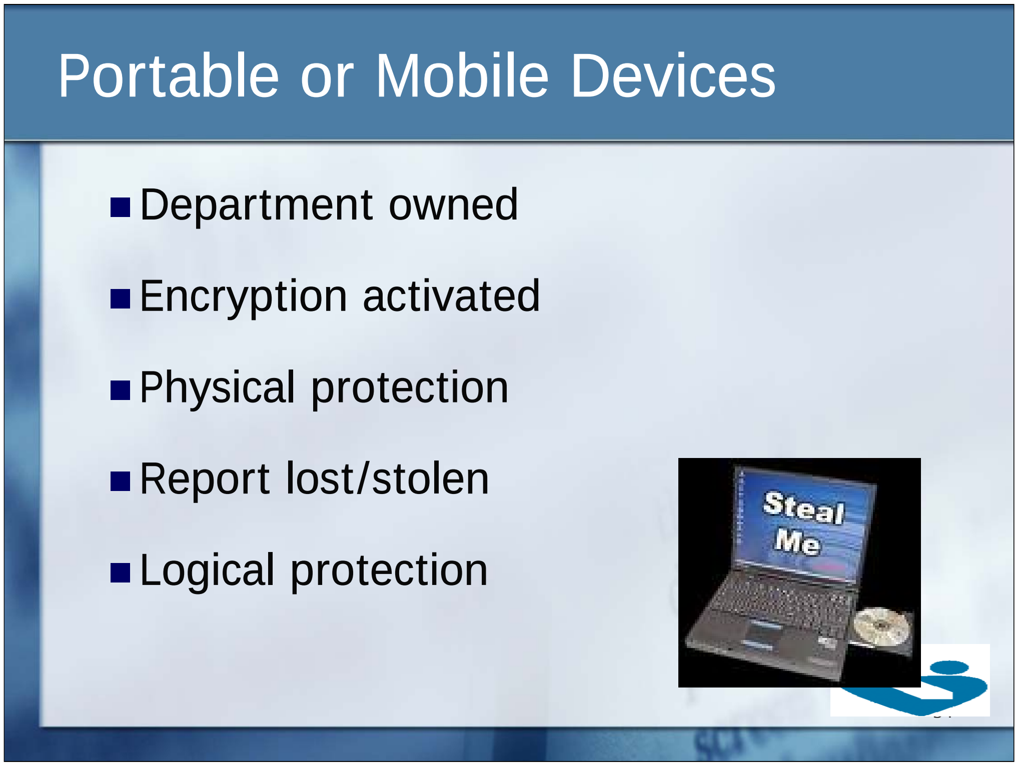
- You must have a business need
- Management approval
- DCSS approved solution
- Contact your IT or ISO for help

Remote access has the potential to introduce additional vulnerabilities to the network or systems environment. The following requirements are established to mitigate potential risks introduced by remote access:

•Remote access to the network supporting Child Support services must be restricted and managed as directed in the DCSS ISM.

•Remote access must be limited only to laptops or computers owned and managed by the organization (DCSS or LCSA).

•These laptops computers must be configured securely in accordance with the DCSS ISM requirements -



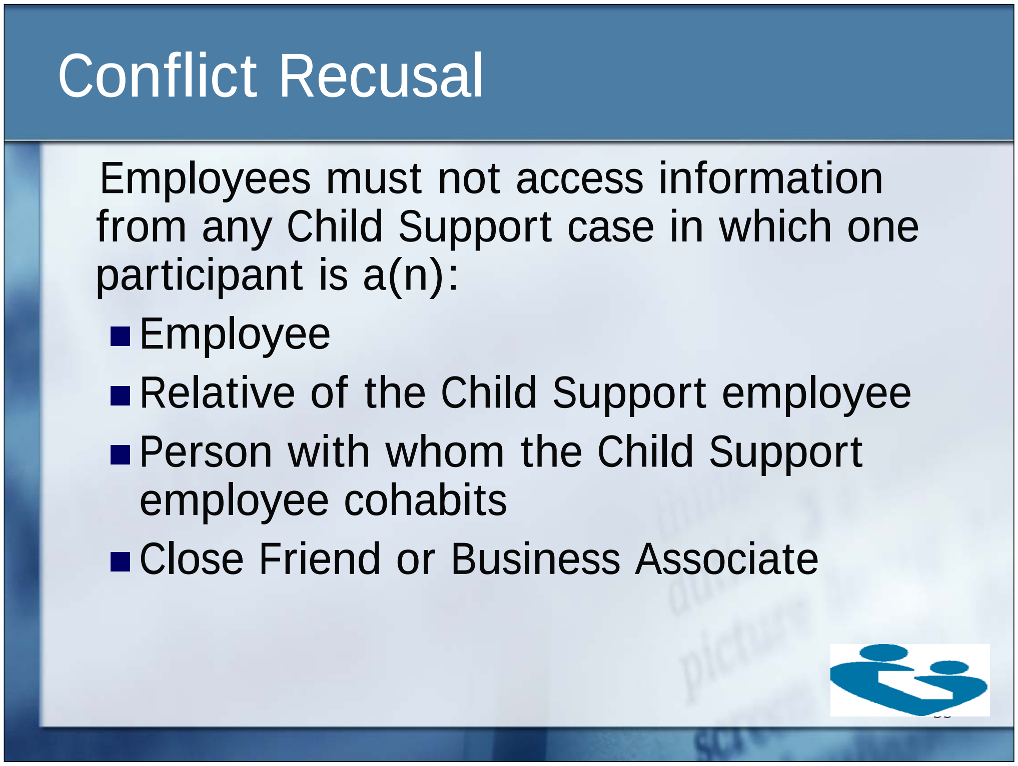
Portable or Mobile Devices

- Department owned
- Encryption activated
- Physical protection
- Report lost/stolen
- Logical protection

Personally owned mobile computing and storage devices such as laptops, Blackberries, PDAs, CDs and Flash Drives should not be used for Child Support Services business.

Here are some of the rules that should be applied when using Mobile Computing or Storage Devices:

- It must be owned by your department
- The device must be encrypted (refer to DCSS ISM)
- You must not leave the device unattended in public. In traveling ensure protection while at the hotel, in your car (put in trunk) or at home.
- You must report the incident if a computer and/or storage device(s) is lost or stolen.
- Must not connect to personal equipment



Conflict Recusal

Employees must not access information from any Child Support case in which one participant is a(n):

- Employee
- Relative of the Child Support employee
- Person with whom the Child Support employee cohabits
- Close Friend or Business Associate

Recusal refers to the request to excuse ones self from participation in a decision on grounds of prejudice or personal involvement in the decision making because of the potential for unbiased impact. DCSS or LCSA employees with access to confidential information pertaining someone they know or are related while performing their work function must comply with this standard.

This standard requires employees to avoid conflict of interest in such situations. Employees should not access information on their own case, their family, relatives, friends, or anyone else that may result in an unbiased impact to the subject or person in question.

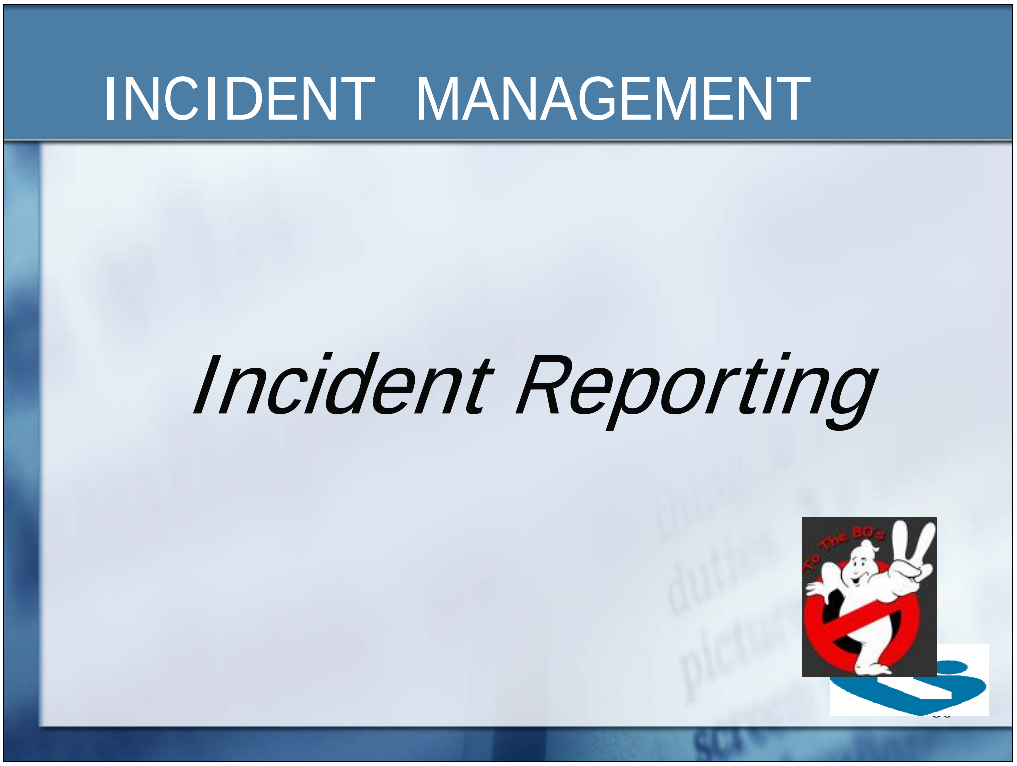
If you are assigned a case that may cause a conflict according this standard, you must inform your supervisor and recuse (excuse) yourself from the case.

Definition:

Relative – any individual that is related by blood, marriage or adoption.

Cohabit – sharing a residence with another individual regardless of whether or not there is a romantic relationship.

Close Friend or Business Associate – An individual with whom the Child Support Employee’s personal or business relationship has resulted in in-depth discussions about the Child Support Participant’s case within the last three years.



INCIDENT MANAGEMENT

Incident Reporting

Information Security Incident Management is the handling of suspected or known activity that may affect Child Support Program negatively.

Incident Reporting is a critical element of the incident management process – All employees are responsible for reporting incidents

Information gathered from the Incident Report helps to:

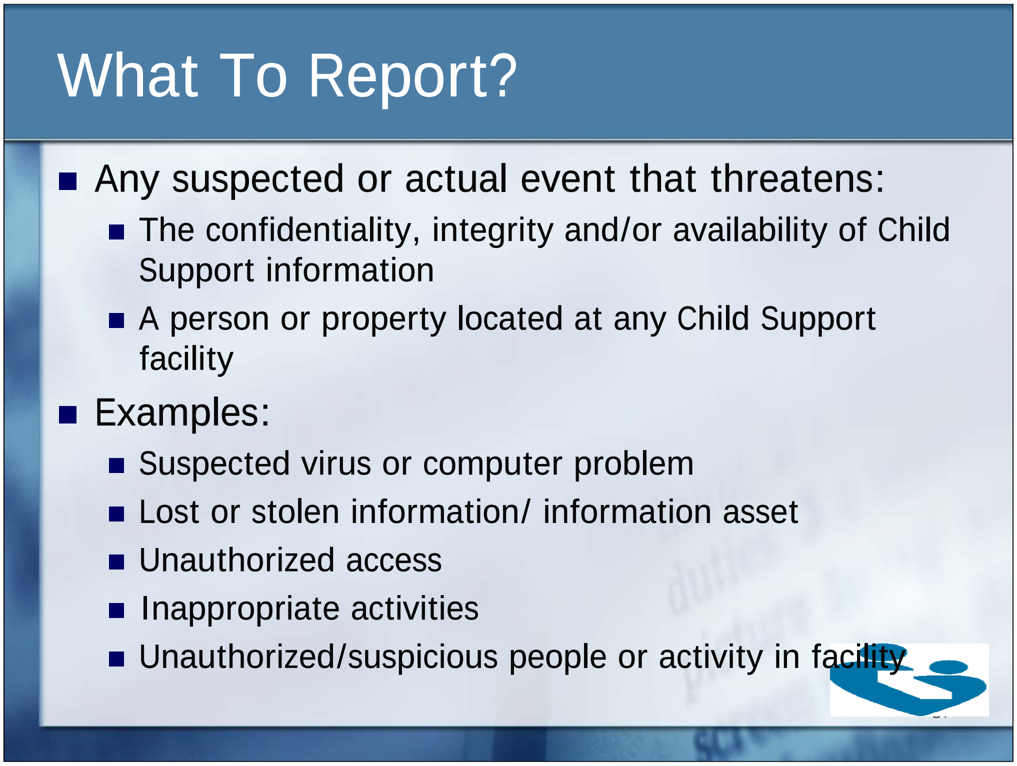
1) Mitigate the negative impact of the threat by preventing further damage or harm to an individual or the organization.

2) Meet the State and DCSS information security reporting requirements .

3) Identify areas of focus for future information security training or resource allocation.

Note: If you feel there is an imminent threat to individual or property call 911.

If you observe a activity in progress that may cause further damage to DCSS services or personal notify your supervisor or manager immediately.



What To Report?

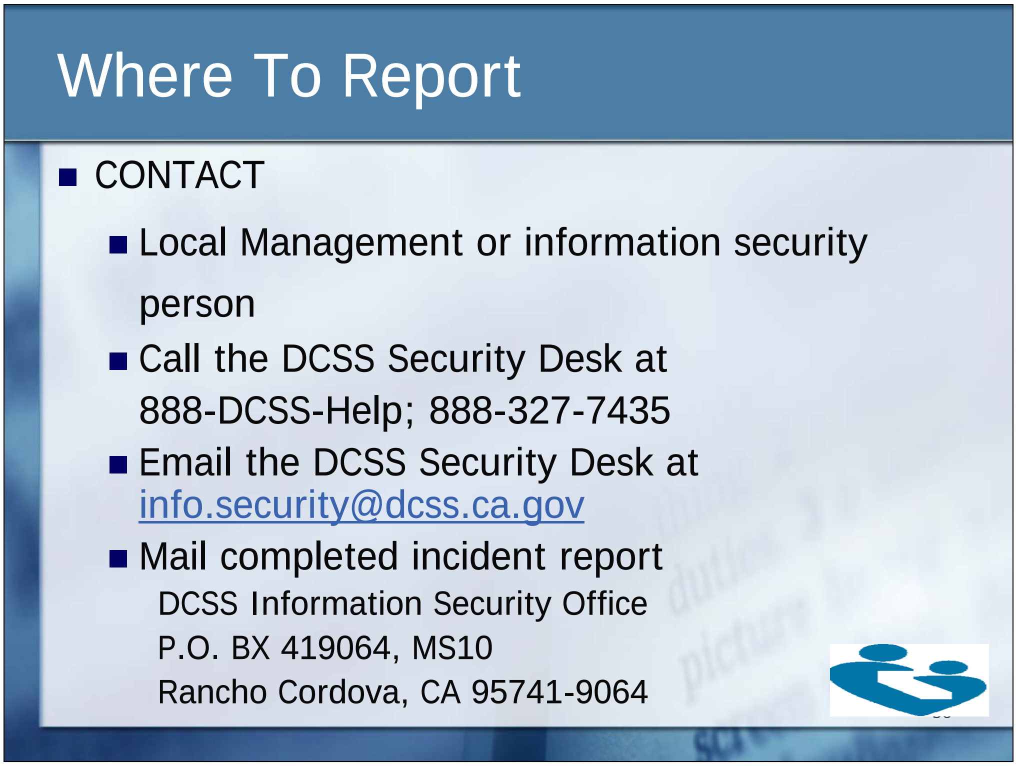
- Any suspected or actual event that threatens:
  - The confidentiality, integrity and/or availability of Child Support information
  - A person or property located at any Child Support facility
- Examples:
  - Suspected virus or computer problem
  - Lost or stolen information/ information asset
  - Unauthorized access
  - Inappropriate activities
  - Unauthorized/suspicious people or activity in facility

Report information security incidents that may potentially impact the confidentiality, integrity or availability of the information resources. This may involve Information, Information Systems Security, Facilities or other resources supporting child support services.

It is better to over report than under report being on the side of caution versus ignoring. If you think there is an opportunity or vulnerability where information can be exposed, you must report it.

Here are some examples:

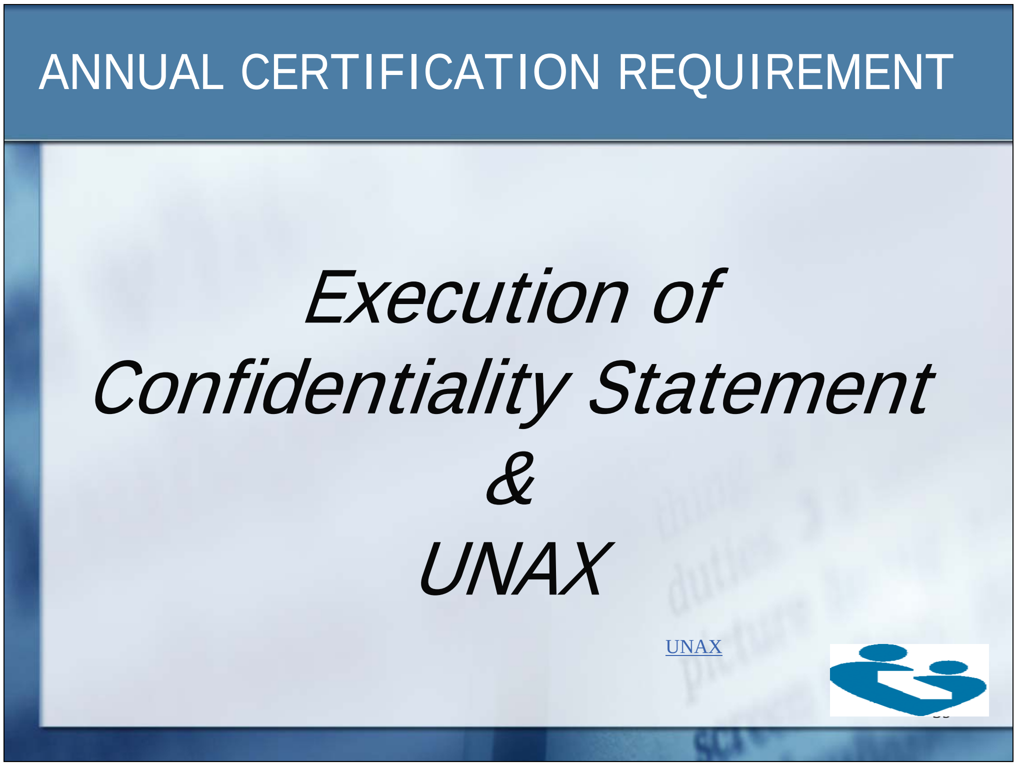
- An email with a virus triggering event was opened resulting in infecting computers and/or spreading viruses on the network supporting child support services
- Confidential information was found unattended in an area that may offer opportunity for exposure
- Loss of a laptop, mobile computing device
- You become aware that information has been disclosed to an unauthorized person
- Received an email threatening activity against child support employees.



Where To Report

- CONTACT
  - Local Management or information security person
  - Call the DCSS Security Desk at 888-DCSS-Help; 888-327-7435
  - Email the DCSS Security Desk at info.security@dcss.ca.gov
  - Mail completed incident report

    DCSS Information Security Office
    P.O. BX 419064, MS10
    Rancho Cordova, CA 95741-9064

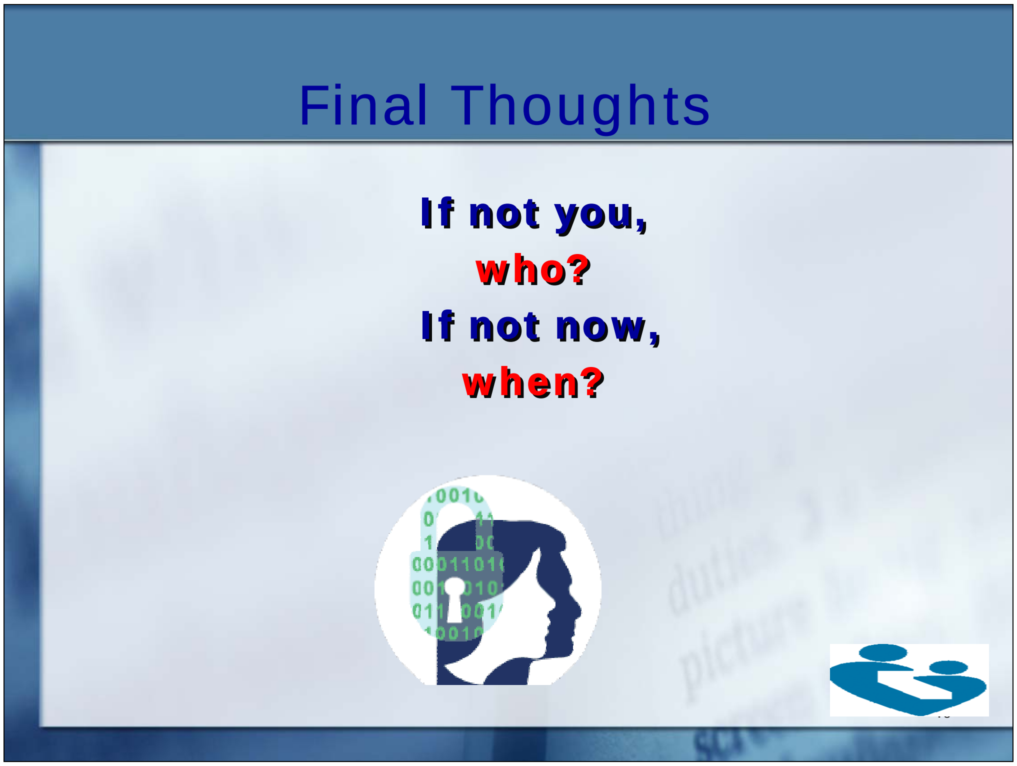


ANNUAL CERTIFICATION REQUIREMENT

Execution of Confidentiality Statement & UNAX

UNAX

Read and complete the Confidentiality Statement & UNAX forms. Make sure your supervisor (contracting entity) signs acknowledging your completion. You may make a copy of the form for your records. Your organization must retain the original, or send to the Human Resources Section.



Final Thoughts

If not you,
who?
If not now,
when?

- Remember!

Security is Everyone’s Business!!

Department of Child Support Services