Welcome to the Initial Data Security Training

DeISA 1001 - Annual Security Re-briefing

Equal Opportunity Employer/Program Under Titles VI and VII of the Civil Rights Act of 1964 (Title VI & VII), and the Americans with Disabilities Act of 1990 (ADA), Section 504 of the Rehabilitation Act of 1973, the Age Discrimination Act of 1975, and Title II of the Generic Information Non-discrimination Act (GINA) of 2008, the Department prohibits discrimination in admissions, programs, services, activities, or employment based on race, color, religion, sex, national origin, age, disability, genetics, and retaliation. The department must make a reasonable accommodation to allow a person with a disability to take part in a program, service, or activity. For example, this means if necessary, the department must provide sign language interpreters for people who are deaf, a wheelchair accessible location, or enlarged print materials. It also means that the department will take any other reasonable action that allows you to take part in and understand a program or activity, including making reasonable changes to an activity. If you believe that you will not be able to understand or take part in a program or activity because of your disability, please let us know of your disability needs in advance if at all possible.

To request this document in alternative format or for further information about the policy, contact (602) 542-3782; TTY; TDD Services 7-1-1. Free language assistance for DES services is available upon request.
This course is required for ALL DES employees and ALL users of DES data. You have a mandated responsibility to know how to protect confidential data.

This course is intended to teach you important security principles as required by Federal and State statutes and DES policies.

The course should take less than 2 hours to complete.

Questions?

Contact the Training Support Center at 602-542-3782 or TDAGeneralMailbox@azdes.gov
Civil Damages for Unauthorized Disclosure of Federal Tax Information (FTI)

The Internal Revenue Code (IRC) Section 7213(a), states it is unlawful for any current or former state employee or other person to willfully disclose to any unauthorized person or entity any Federal Tax Information (FTI). Any violation is a felony punishable by a fine in any amount not exceeding $5,000, imprisonment of not more than 5 years or both together along with the cost of prosecution.

As provided by IRC Section 7213(a), it is unlawful for any current or former state employee or other person willfully to inspect, except as authorized, any FTI acquired by him or her or another person. Any violation is punishable by a fine in any amount not exceeding $1,000, or imprisonment of not more than 1 year, or both, together with the cost of prosecution.
Data security must be a major consideration in the day-to-day execution of your job whether you are a DES employee or a DES contractor.

Protection of confidential data is accomplished by people like you. Security programs, policies, procedures and training are in place to assist you.

You are required by Federal and State laws to adhere to the policies discussed in this course. These policies are designed to protect DES confidential data. A violation could result in employment discipline up to and including termination, as well as civil and/or criminal prosecution.
This course is mandated and participation is required by all DES employees that access any data, systems, facilities or clients.

Not everyone at DES handles or comes in contact with confidential information on a regular basis. However, nearly all DES employees will be exposed to some type of confidential data at some point.

Everyone, including you, has a mandated responsibility to know how to protect data.
Course Scope

This course covers the security principles and common sense security practices that are needed to protect confidential data.

This course may not cover all of the specific security requirements for the Divisions and programs operating inside or outside of DES.

The security specialists in your Division will train you on specific procedures that may be unique to your Division.
Lesson One: Roles, Responsibilities and Definitions

Objectives of this Course

After completion of this course participants will be able to:

1. Describe the primary purpose of DES Security Policies and the consequences of violating them;

2. Identify and distinguish between the roles of the Information Risk Management (IRM) group and the Division Security Specialists;

3. Identify the three relationships to data;

4. Define confidential data and identify the various types of confidential data that must be protected; and

5. Identify three results of violating security policies and the possible consequences for the unauthorized disclosure of Federal Tax Information (FTI).
The purpose of all DES security policies are to ensure the integrity, confidentiality and availability of State-controlled information by preventing unauthorized access modification or destruction.

Simply stated ...

The primary purpose of DES security policies is to protect DES confidential data.
The Information Risk Management (IRM) Group

All information security responsibilities are managed by the Information Risk Management (IRM) group within the Division of Technology Services (DTS) and it is led by the DES Information Security Administrator, also known as the Chief Information Security Officer (CISO).

The IRM group is responsible for controlling access by external system users, which includes federal, state, local and non-governmental users. They are also responsible for managing all DES employee access to non-DES computing environments. The IRM group also monitors all security training provided to DES users.

The responsibilities of the IRM Group are:

Security Reviews and Investigations
By federal mandate, the IRM group conducts regular security reviews of DES environments. (This is discussed later in this course.)

Investigates Security Incidents
When a security incident is reported, IRM follows the Department’s incident response plan, investigates the incident and reports findings as appropriate.
Security within DES is decentralized as this allows you to interact with local security specialists, who work with the IRM Team. The IRM group has delegated to the divisions/programs the authority to authorize access to their users and systems.

Divisional Security Specialists are assigned in each Division or program and are charged with maintaining the security within their organizations. Local security specialists within DES consult with the IRM for guidance on DES security policy.

Your Division Security Team is responsible for all items concerning security for your respective Division/Program, which includes:

- Monitor
- Audit/Review
- Grant Access
- Interpret and Enforce
- Document and Report
- Classify
Each Division Security section is independent and manages each Division specific secure environment according to the applicable Federal or State laws, DES policies and/or Division/Program specific requirements.

For any changes made to the secure environment, Division Security staff must follow the proper DES security guidelines as well as any Divisional/Program requirements.

Your local Division Security staff cannot be forced or influenced into relaxing or modifying any security requirements in violation of DES policies and procedures.
For Any Questions or Concerns About Security Contact Your Division Security Staff!

Division Security Staff are in place to help you maintain your security obligations as required by law. Division Security Staff will provide you with additional information concerning the specific security requirements for your Division/Program or any items that may deviate from the information presented in this course.

Division Security Staff may be viewed on the Information Risk Management SharePoint Site.

Note: If you do not have a SharePoint logon you are managed by IRM Security Staff.

You may contact the IRM group at any time and you do not have to provide your name and can do so anonymously.
All users of DES data have a distinctive relationship to the data they use. There are three (3) relationships personnel may have depending on their specific job duties and they are below:

1. **Data Owner and Managers**
   The DES Director is identified as the owner of all DES data. The Director designates the Assistant Directors and Administrators of Programs in which data originates as the managers of the data. Any conflicts that arise as a result of unclear origination of data will be referred to the Chief Information Security Officer (CISO) for resolution.

2. **Data Custodians**
   Information Technology personnel are the designated custodians of data. Data custodians assume responsibility for protecting and maintaining the data under their control. Any release of data maintained by the data custodian may occur only if authorization is received from the data manager.

3. **Data Users**
   All people and organizations that have approved access to DES data are designated as data users and can process DES data and/or disseminate DES data. Data users constitute the largest group. All approved non-DES employees are data users as well.
Confidential Data is defined under Arizona Revised Statutes, A.R.S. § 41-1959 as follows:

“Unless otherwise provided by law, all personally identifiable information concerning any applicant, claimant, recipient, employer or client is confidential and shall NOT be released unless ordered by a superior court judge or provided for by rule of court...”

What this means to you is that ALL personally identifiable information (PII) concerning any applicant, claimant, recipient, employee, employer or client is mandated as CONFIDENTIAL data.

Play it Safe!

When you are in doubt about the confidentiality of information, a document or database, consider it confidential data and protect it!
Federal Tax Information (FTI)

All information collected or used by the Federal Government must be treated as confidential data and that includes Federal Tax Information (FTI).

Federal law explains the regulations regarding maintaining confidentiality of FTI. (26 U.S.C. § 6103)

**Federal Tax Information (FTI) is defined by IRS Publication 1075 as:** Federal tax returns and return information received by specific state agencies from the Internal Revenue Service (IRS).

FTI shall only be viewed, distributed or used by individuals who are specifically authorized to do so and only for authorized administrative purposes. Any unauthorized individuals that view, distribute, or use FTI data can be subject to criminal and civil fines and/or imprisonment. DES employees are subject to employment discipline.

You may contact the DTS IRM group for any questions concerning FTI or you may refer also to IRS Publication 1075 for specific details.
Internal Revenue Code (IRC) Section 7213(a) mandates the following:

1. It is unlawful for any current or former state employee or other person to willfully disclose any FTI to any unauthorized person or entity.

   *Any violation is a felony punishable by a fine in any amount not to exceed $5,000 or imprisonment of not more than five (5) years, or both together with the cost of prosecution.*

2. It is unlawful for any current or former state employee or other person to willfully inspect any FTI acquired by him or her or another person except as authorized.

   *Any violation is punishable by a fine in any amount not to exceed $1,000, or imprisonment of not more than one (1) year, or both together with the cost of prosecution.*
IRC Section 7431 states the following in relation to the release of FTI:

If any current or former state employee or other person knowingly, or by reason of negligence, inspects or discloses any FTI with respect to a taxpayer in violation of confidentiality laws, the taxpayer may bring a civil action for damages against such person.

Penalties may be the greater of (A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or (B) the sum of the actual damages sustained by plaintiff as a result of such unauthorized inspection or disclosure, plus in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. Actions may be brought at any time within two (2) years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

What this means for DES employees and contractors is that you and the agency can both be held civilly and criminally responsible for any inappropriate inspection (disclosure) and/or use of FTI.
Some programs within DES receive Personally Identifiable Information (PII) from the Social Security Administration (SSA), like information received from the IRS, this data can only be viewed, distributed or used by individuals who have been specifically authorized to do so and only for authorized administrative purposes.

Any other individuals viewing, distributing or using data provided SSA can be subject to criminal and civil fines and imprisonment, as well as agency discipline.

You may contact the DTS IRM group for any questions or you may refer to the Privacy Act of 1974 for further details regarding the protection of PII.
Summary of the HIPAA Privacy Law

What is Protected Health Information?
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its regulations protect all individually identifiable health information created, received, held or transmitted by a covered entity or its business associates, in any form or media, whether electronic, paper or oral. The Privacy Law calls this information protected health information (PHI).

Individually identifiable health information is information, including demographic data, that relates to:

1. The individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual: and/or

2. Individually identifiable health information includes many common identifiers such as name, address, birth date (DOB) and Social Security Number (SSN).

This Privacy Law excludes protected health information employment records that a covered entity maintains in its capacity as an employer.
General Principle for Uses and Disclosures

The purpose of this Privacy Law is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities.

A covered entity may not use or disclose protected health information, except either:

1. As the privacy law permits or requires; or
2. As the individual who is the subject of the information or the individual's personal representative authorizes in writing.
1. A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Law.

2. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.

3. An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party.

4. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes.

5. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.
Consequences for Violating Security Policies

A violation of DES security policies may result in:

1. Disciplinary Action;
2. Termination of Employment; and/or
3. Civil and/or criminal prosecution.

But, it doesn't end there ...
DES Employees and Contractors

Both you and the agency can be held both civilly and criminally responsible for any inappropriate inspection and/or use of FTI.

Something to Remember

If you are charged with a violation of Federal or State laws or DES policies the Attorney General's Office is not obligated to defend you in any such actions.
Lesson Two: Keeping Data Secure

**Lesson Objectives**

At the end of Lesson Two participants will be able to:

1. Explain the "Need to Know" concept;
2. Describe how to protect confidential data;
3. State the purpose of the User Affirmation Statement;
4. Recall key prohibited actions listed on the User Affirmation Statement; AND
5. Describe the DES standards and limits for system passwords.
To legally access information you need both a right to know and a need to know the information.

- **Right to Know** means that the law allows DES to give you access to certain information and you are in a job that is authorized for that access.

- **Need to Know** means that your job duties require that you are able to access a certain confidential record to do your job.

For example, if you are assisting a client to receive DES services you have a need to access their confidential information. However, that does not mean that you can look up any information in the database just because you have access to do so.

Your Division Security staff grants you access to certain information systems based on your **Right to Know**. You are responsible for monitoring your **Need to Know**.

Every DES information system that processes confidential information is required to capture transaction logs. Transaction logs are created for audits, investigations or supervisors, so they can determine who has accessed information in the system.

If you have questions about Right and Need to Know, your Divisional Security staff or your supervisor will guide you through the areas of confidential information that you need to do your job.
Preventing Security Violations

To help prevent security violations, you must log off your computer (PC)/workstation before going home, to meetings, lunch or if you will be away from your desk for any period of time.

If you have a PC with a password protected screensaver, you can use the screensaver to lock your PC when the situation warrants it.

You must secure any confidential documents that you have in or on your desk when you leave your workstation.
The requirement to protect confidential data is not confined to the data within a computer. Data security applies to all confidential data regardless of its location or media.

Confidential data may be found on desks, printers, in-baskets, day planners, and in the trash. Unprotected data can be picked up or read by anyone.

Every effort MUST be made to ensure that confidential information is:

- Secured in desks or file cabinets which are then locked;
- Disposed of in confidential shred containers;
- Secured in offices that are locked at the end of the day; and
- Immediately retrieved from printers after printing.
Access to DES Information Systems will be granted as stated below:

If you are a new or transferring employee, your supervisor will complete an online request to give you basic computer access and email. You will be provided with a logonID and a password by your Division Security staff. Once you receive your logonID and password you must complete all of the required training and sign a User Affirmation Statement. After you have completed the required training and signed the User Affirmation statement, you will then get any additional access that you need to do your job.

You must use your new account regularly. If an account is not used for 90 days it is deleted.

If your job requires it, you may also be issued a token, which is a small device or smartphone application, that allows you to access DES information systems remotely.
User Affirmation Statement

The User Affirmation Statement (UAS) was formerly as a hardcopy form known as the J-129.

Today the UAS is an online electronic form and must be completed before any access to a DES Information System will be granted.

The UAS outlines your responsibilities as a user of DES data and lists some of the basic security requirements instituted by DES.
The following is a list of actions that are expressly prohibited. By signing the User Affirmation you agree to not engage in any of these following activities:

1. Revealing **DES** data to any person or persons outside or within the **DES** who have not been specifically authorized to receive such data;
2. Attempting or achieving access to **DES** data not related to your mandated job duties (violating "Need to Know");
3. Entering, altering and/or erasing any **DES** data for direct or indirect personal gain or advantage;
4. Entering, altering and/or erasing any **DES** data maliciously or in retribution for real or imagined abuse, or for personal gain or for personal amusement;
5. Using another person's **DES** password and/or LogonID;
6. Revealing your personal **DES** password to another person; AND
7. Asking another user to reveal his/her password.
Your password must be changed every 90 days and must be:

1. At least 8 characters long;
2. Must contain UPPER and lower case letters;
3. Must contain at least 1 number;
4. May not be the same as you logon ID;
5. Must not be a common phase;
6. May not be reused within a 24 month period; AND
7. May not have repeating characters (XX or XYXY).
Password facts

• Passwords expire after 90 days.

• If you enter your password incorrectly 3 times, your account will lock and you will be required to reset your password.

• You are notified at least 7 days before your password expires.

• You have 20 seconds from the start of the mainframe login process to enter a correct password before your session will expire.
DES prohibits the divulging of your password **TO ANYONE**.

This means if your mother, coworker, supervisor, manager, staff, administrator, assistant director, or director asks for your password, JUST SAY NO!

**NO LEGITIMATE PERSON WILL EVER ASK FOR YOUR PASSWORD OVER THE PHONE!!**

Inform the requester that it is a violation of DES policy to divulge your password to anyone. Any requests for your password should be reported on a J-126 Security Incident Report Form.

"Be Wary of Phishing. Verify credential before giving information."
“Phishing” is a hacker activity designed to get you to click on a harmful link or to give up confidential information to a caller over the phone.

Some things to remember:

• NO legitimate person will ever ask you for passwords or other confidential information over the phone.

• Links on emails can be dangerous. So, be sure you know the sender as the email can appear to come from someone you know.

• Emails can be spammed.
Lesson Three: System and Email Usage

Lesson Three Objectives

By the end of this lesson, participants will be able to:

1. Identify appropriate and inappropriate actions regarding copying or transferring user-owned and/or downloaded (freeware) PC software;
2. Identify examples of unacceptable use of DES computer resources, DES email and the internet;
3. Recognize that DES email is public record and identify when email must be sent encrypted; and
4. Define spyware, malware, adware and similar malicious software and recall the policy concerning it.
All DES users of DES data are responsible for the protection of DES data to insure against the loss of, unauthorized modification to, improper destruction of, misuse or unauthorized disclosure of data.
As a DES user you are required to protect the computer equipment under your control as per all Federal and State laws or DES policies, including software license agreements.

All software shall be used in accordance with the terms of the Manufacturer's Software License Agreement.

Absolutely no duplication of licensed software is allowed unless approved to do so in writing from the manufacturer and your management.

The User Affirmation Statement states:

"As a computer system user you are responsible for the proper use of DES owned software products and associated literature, such as user manuals, user guides, etc."

PC Software License Agreements

Purchased products are protected by the U.S. Federal copyright act, which makes a willful act of infringement a crime, subject to criminal prosecution, liability for civil damages or both. Violators may be subject to a $250,000 fine or one year in prison or both.

Transferring software between Divisions is prohibited. Any exception requires the approval of each Division LAN Managers.
Individually purchased and/or owned software shall not be installed on any DES computer system.

This includes software from the internet, including software described at “Freeware".

All exceptions must be approved in writing by local Information Technology management.
State computer resources are purchased and operated for State Agency use.

Anyone who is authorized to utilize State equipment may not use State resources in any project designed for **personal financial gain**.

Software developed in the course of employment by Employees, Consultants, Contractors or using any State computer resources, remains the property of the State of Arizona.
DES computer and office equipment resource use policy for all DES users is contained in the DES Information Technology Acceptable Use Policy 1-38-8280.

Acceptable use of IT, office equipment and other resources is limited to:

1. Work related activities as defined by DES management;
2. Department training activities that are considered career enhancing or are directly work related; and
3. Personal use of DES computing and office equipment is allowed only if guidelines are followed.
Unacceptable Use of IT and Office Equipment and Resources are as follows:

- Private business activities;
- Solicitation for personal profit or gain;
- Viewing or downloading of obscene (explicit sexual) materials, per A.R.S. § 38-448;
- Copyright infringement;
- Sexual harassment;
- Discriminatory and defamatory activities;
- Any deceptive, fraudulent, malicious or illegal activity;
- Perpetuate chain email letters or their equivalents. This includes letters that ask the recipient to forward an email to a specified number of addresses in order to achieve some monetary, philosophical, political, superstitious, or other goal;
- Downloading, installing, and/or using any image or other file not specifically related to your job duties or and authorized by your management;
- Bringing discredit on the State in your operation and use of information technology and office equipment and resources;
- Creating or distributing messages that promote or support political parties, positions, or activities;
- Use or visiting of gambling websites;
- Any other inappropriate activity as deemed by DES management;
- Use of DES computing facilities for tax preparation; OR
- Using any streaming audio or video for non-work related purposes.
Any deviation from this policy without express written approval from your local IT management constitutes a violation of DES policies and may subject the offender to disciplinary actions up to and including termination.

All users of DES IT equipment must become familiar with the Acceptable Use Policy.

Internet use on the DES network passes through a web filter and each internet visit is logged.
All DES Email is Public Record

- Public records are broadly defined and may include any information in an email produced or received on State-provided systems.
- Public records, including email, may be subject to disclosure under state public records law or other applicable law, including by subpoena.

Note: If information is considered to be a public record, this does not mean you are authorized to disclose it at any time to anyone. All disclosure of information must be authorized and approved prior to the disclosure.

Email Encryption

- Email sent internally to DES is protected by our network structure, sending any confidential data outside of our network requires the use of an approved email encryption application, please see your Division Security Staff for instructions on this process.
- Generally speaking, Federal Tax Information may not be sent in an email.
Confidential information should normally NOT be sent electronically for several reasons, two of these reasons are below:

- Messages can inadvertently be sent to the wrong addressee.
- You have no control over the message once it is sent.

Email should always be used with the assumption that messages will be read by someone other than the intended recipient.

*Examples of Unacceptable Email is email used for:*

- Personal gain;
- Soliciting;
- Political campaigning;
- Unethical, illegal, unprofessional, or disruptive activities;
- Any activity that would jeopardize the legitimate interests of the citizens of the State of Arizona
- Participation in Chat Rooms; AND
- The creation, distribution or forwarding of Chain Letters.
Unacceptable Email Use

Example:
Rose received an email that supports a very worthwhile cause. The email asks the receiver to send it to 10 other people that might be interested in this worthwhile program. Is it OK for Rose to send the email during her break?

Answer: No, this is a chain email and a violation of policy.
DES monitors and logs internet usage by any user without notice. The abuse of Internet resources may be cause for discipline or dismissal (A.R.S. § 41-773).

The willful introduction of viruses to State information technology systems may be cause for discipline or dismissal (A.R.S. § 41-770). If you become aware of an internet usage violation, it must be reported to your immediate supervisor, Security Specialist and IRM.

You should not knowingly use, view, submit, publish, display, or transmit any information on any computer system that:

- Utilizes the internet for an illegal purpose;
- Conducts any gambling, betting or gaming activity;
- Violates or infringes on the rights of any other person; OR
- Contains defamatory, false, abusive, obscene, pornographic (A.R.S. § 38-448), profane, sexually oriented, threatening, racially offensive, otherwise biased, discriminatory, illegal material, violates any applicable Federal, State, or DES policies, laws, and regulations prohibiting sexual harassment, or distributes chain letters.
Spyware programs collect data on users and their computing behaviors and then transmit that information back to a spyware host server.

These programs can also monitor keystrokes, scan files on PCs and servers, secretly install other programs and make changes to default computer settings. Spyware is often acquired secretly when users download a real application or file, visit websites or click on a deceptive pop-up window. Knowingly downloading any of these types of programs is strictly forbidden.

On many occasions a user may not be aware of downloading these programs. Great care should be taken when browsing unknown internet sites.

It is forbidden to download any program from the internet without local IT management approval.
Unauthorized Devices

The following is a list of unauthorized activities with respect the DES network:

1. Connecting a non-DES owned device to the network without authorization from DTS Network Operations;
2. Connecting any wireless access point, switch, hub or router not managed by DES/DTS Network Operations; OR
3. Establishing a virtual private network or secure tunnel to any location outside of the DES Network unless it is sanctioned by DES/DTS Network Operations or Information Risk Management.

Note: The State of Arizona maintains a wireless network in many DES facilities, sometimes known as Copper. DES does not regulate that network and has its own acceptable use rules, which you may read if you access the network.
Unauthorized Connections

DES takes extensive and expensive measures to protect confidential client information and other sensitive data by encrypting hard drives, installing data loss prevention devices and implementing additional security controls to ensure that confidential information is not lost or transferred to unauthorized individuals.

The following connections are not permitted on a DES owned computing device unless expressly authorized by a Division Security staff or Information Risk Management.

• Connection of any mass storage device to a DES owned computer, such as a USB (thumb) drive, CD-ROM, writeable DVD or external hard drive. Note: File transfers should be accomplished by using DES owned shared drives or authorized file transfer software.

• The connection of personally owned devices to any DES owned computing devices, such as, iPods/iPads, tablets, smartphones, for the purpose of charging or transferring files, pictures or music.

• This guidance does not restrict the connection of devices that cannot hold or transfer data, such as external speakers, headsets, monitors, etc.
Lesson Four Objectives

By the end of this lesson, participants will be able to:

1. Recall the definition of a security incident;
2. Identify the proper procedure and form for reporting a security incident;
3. Define a Data Sharing Agreement (DSA) and how it is initiated;
4. Define a security audit and identify what is covered; AND
5. Identify acts prohibited when telecommuting.
A security incident includes:

• Violating the confidentiality of any person, place or thing involved with DES;

• Intentional or unintentional destruction, loss, alteration, unauthorized access to or damage to DES data;

• Revealing confidential DES data to unauthorized persons;

• Intentional disclosure of a password; AND/OR

• Attempts or successful phishing attempts either by phone or by email link.
How Do I Report A Security Incident?

A Notice of Security Incident (J-126) form should be completed for each security incident and sent to the IRM group. In addition to filling out the form, you should also immediately notify your supervisor and your Division Security Staff.

**Note:** You do not need any permissions to file a security incident report. No person, including your management, should prevent you from filing a security incident report form. You cannot be punished for filing a legitimate security incident report, even if the subsequent investigation does not reveal a breach of security.

Forms can be furnished upon request. The forms used by the IRM are available in electronic form in the DES Digital Library.

If you have any questions concerning the Notice of Security Incident (J-126) form or other security matters, please phone (602) 771-2670. For all other security issues, contact your Division Security Staff who will either address the problem or refer you to IRM.
Additional Security Incident Reporting Information

Any time you observe or are made aware of a breach of security **you must report the incident to IRM and your supervisor within eight (8) business hours.** Time is very important in investigating security incidents. The sooner an incident is reported, the sooner an investigation can begin and the easier it is to get the necessary information for the investigation.

Report the incident on a Notice of Security Incident (J-126) form. Electronic submission of the form is preferred, however, phone and fax requests will also be honored.

Send the completed J-126 form to:

**Interoffice:**
Information Risk Management
Mail Drop 1426

**US Mail:**
Information Risk Management
3443 North Central, suite 1105
Phoenix AZ, 85012

**Email:**
irmadmin@azdes.gov

**Telephone:** (602) 771-2670
Security Incidents involving Federal Tax Information and Social Security Administration data have special reporting requirements. Some are very time sensitive. Report these immediately by telephone or email to IRM or your Division Security Staff.

Federal Tax Information

1. Notify IRM;
2. Internal Revenue Service (IRS); AND

Social Security Administration Information

1. Notify IRM;
2. United States Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident;
3. SSA Systems Security contact named in the SSA agreement.
Upon notification of a security incident, IRM will implement the Incident Response Plan by:

- Blocking a web site at the firewall; AND/OR

- Completing a more detailed investigation into the incident.

Note: Your assistance in any investigation is essential and mandatory.
Correcting the Problem that Led to the Incident

IRM personnel will conduct a thorough investigation and some of the items that may be investigated are:

- Who was involved;
- How many people reported the incident;
- Who was in a position to know about the incident;
- Was this an intentional or unintentional breach of security;
- When did the incident occur;
- How long was the data exposed;
- Is the exposure closed at this time;
- Where did the incident occur;
- Is the area under DES control;
- Does DES have access to the area;
- Determine the extent of loss of data;
- What type of data was compromised;
- Estimate the damage done by the loss of data;
- Who is affected by the compromise;
- Evaluate what policies or procedures were violated that caused the loss;
- Do policies need to be clarified or revised;
- Recommendations to help prevent future losses; AND
- Are training revisions needed.
Data-Sharing Agreements (DSA) allow individuals or entities outside of DES to access confidential data under DES control.

To gain access to another Division’s data or allow another group to access data under your control, a DATA SHARING REQUEST/AGREEMENT (Form J-119) must be completed and filed with the IRM prior to any data being shared or transferred.

Electronic submission of a DSA is required. The e-form is available on the DES intranet web server, if you do not have access to this server, please contact the IRM.

Send the completed FORM J-119 to: +IRMadmin@azdes.gov

Questions? Call the IRM at (602) 771-2670.
Security Audits

A security audit determines how well an organization is meeting its security obligations. It incorporates all personnel in the organization and may be mandated by Federal or State laws, or DES policies.

A security audit examines:
• The state of physical security in facilities; and
• The security measures used by technology applications.
What is Covered in a Security Audit

- All policies, Procedures, Practices, Documentation;
- Systems: Hardware, Software;
- Operating Systems;
- Applications;
- Networks;
- Security tools;
- Reported security incidents;
- User access methods;
- Account maintenance;
- Password protocols;
- Encryption;
- Remote access procedures; AND
- Many other security controls.
Security Audits, Reviews, and Evaluations

Security Audits

1. **Self Audit**
   A unit examines its policies, systems and work processes against the standards it is required to adhere to.

2. **IRM Audit**
   IRM has a responsibility to maintain a continuous audit program. IRM may also use outside security firms to conduct audits of DES systems.

3. **OIG Audits**
   The DES Office of the Inspector General conducts many types of internal audits, and one of these is information security.

4. **External Audits**
   Regulatory bodies such as the IRS, Social Security Administration, Auditor General’s Office, etc., regularly audit DES programs.
Even with all of those people conducting audits and inspections. The most effective security control is **YOU**. **YOU** are there everyday and **YOU** determine the degree that security policies and procedures are followed. **YOU** have a responsibility to maintain a high degree of security compliance and to help others in your group to do the same. Education and training along with constant monitoring of your compliance and the compliance of others is vital in maintaining a secure environment.
Required security training can be accomplished through several different methods including:

1. The IRM-provided Security training;
2. This Security Awareness Training CBT;
3. Training classes from your Security Specialists;
4. Periodicals referencing security issues; AND
5. Alerts from governmental agencies.

Continuing training is a vital and an important part of a total security program for your area.
DES Telecommuting Policy prohibits restricted-access materials from being taken out of the office or accessed through the computer unless approved in advance in writing by the supervisor.

Unauthorized Disclosure of Data, Unauthorized Access

If you work at a state office, work at home as a telecommuter or are on assignment in the field security is your responsibility. The computer equipment you use and all State confidential material must be protected at all times.
This concludes your Basic Security Training. You have been provided with the knowledge of many basic data security principles. You can now take this knowledge and apply them to your everyday practices on the job.

**Security is your responsibility!** If you work at a state office, work at home as a telecommuter or are on assignment in the field, all State confidential material and the computer equipment you use **must be protected at all times.**
There are a few additional steps before closing out of this web site.

- Click in the box “I have read the material…” box

**Certification**

You will be asked for certain information so that we can give you credit for completing this training.

- Your first, middle, and last name. People have lots of names. Maybe you used your legal name when you filled out your employment paperwork but use a different name for getting email. Please use the name as it appears in the Department of Administration, Human Resources Information System – This will be the name you used on your employment application.
- Your DES EIN – This is your state issued Employee Identification number that identifies you in the HR and Payroll systems. If you are a contractor use the EIN provided by the ERMA training system. If you are a new employee, you may not have had it issued yet. If you have an EIN, it is important that you provide it.
- DES Logon ID. This is important. Please use your DES LogonID It is one way we track your training. Make sure it is correct.
- Division & employee type. If you have a question about these please ask. They have to be correct.
- Email address: If you are a DES employee or contractor, this will be your work email address ending in @azdes.gov. If you work for another agency or partner you may not have a DES email address. If this is the case use your work email from the other agency or partner. If you have a DES email address, please use it on this form.
- Click on “I ACCEPT”, then click on “Submit”

**User Affirmation Statement**

*If you have completed the User Affirmation Statement within the last year, you are now compliant*
*If you have not previously completed the User Affirmation Statement form*, navigate back to the User Affirmation Process page (https://uas.azdes.gov/) and:

- Read the User Affirmation Statement and check the box;
- Read the Access Agreement and check the box; AND
- Complete the form at the bottom. – Yes it is all the same questions but we track your user affirmation statement and your training separately. I know you want credit for both.

Congratulations! You are now finished with your training and user acceptance procedures and may now use the DES computer network. You will be prompted to complete a different training module and execute another User Affirmation in one year.