



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 1

Intro

Welcome to the Department of General Services Information Security and Privacy Awareness training.

This training is provided to you by the DGS Information Security Office (ISO).

You can contact our office via email, phone or mail.

And for more information about Information Security, please visit our website at ISO.DGS.CA.GOV



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 2

Agenda

This presentation is part two of three presentations encompassing the entire information security and privacy training and lasts approximately 10 minutes.

In this presentation, we will introduce information asset identification and inventory, then look at classifying these assets once identified. We will then look at the appropriate ways of handling and managing the information assets we are working with, including proper methods for information disclosure.

Finally, we will look at the roles and responsibilities of the different parties involved with information security and how they work together to create a complete information security aware workforce.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 3

Information Assets

As mentioned in part one, the key element for risk management is knowing what you have, its value and how to protect it.

Identifying information assets is the critical first step. By determining what assets are owned by your office, you can move forward in classifying the type of information you have, and take steps to protect this information.

By Classifying information it helps to determine the value of your assets and the appropriate level of security that may or may not be required to protect our information.

Protective measures of an appropriate level ensure that all types of information are protected and programs can continue to work effectively.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 4

Defining Information Assets

Lets start by defining what DGS Information Assets are.

DGS has many assets which are valuable to the performance of its business function. Generally speaking these assets can fall into one of three main types. General information assets, information system assets, or information facilities.

All Information... paper or electronic stored, processed or accessible from any where. Items such as legal opinions, newsletters, email, personnel records

All Systems and Applications... technology, tools and applications that allow divisions access, storage and processing of data or information. They are things like your personal computing devices. PCs, servers, laptops, flash drives, the network and related hardware. Software or applications purchased or developed by DGS are also assets

All Facilities and Equipment... Buildings, work areas, special equipment or tools for doing your job are DGS assets. This includes the equipment necessary to do your job that go beyond automated tools.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 5

Asset - Information

Information and data are assets created or collected by anyone most anywhere.

DGS employees are able to create documents, spreadsheets, and many other types of information or data within the realm of normal work duties. This can be done with personal computers, mobile devices, copy and fax machines or even pen and paper.

Information can also be collected by way of forms filled out by public, contract bids, email or text messages. All of these varied and diverse documents are considered information assets.

In either hard copy, or electronic form these assets retain some sort of value and are subject to our protection.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 6

Asset – Systems & Applications

Systems and Applications assets are technology resources necessary to process, store or transmit data and provide key support to DGS infrastructure.

Examples of these systems include personal computers, servers, workstations, laptops, network devices and cabling as well as firewalls that connect DGS to the outside world.

Applications allow business to perform functions more efficiently and effectively through process automation. DGS manages applications developed in house as well as commercially purchased software. These applications and application suites are also considered DGS information assets.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 7

Asset – Facilities & Equipment

DGS Facilities house critical resources important to accomplish its mission.

It is important to classify the facility or work areas according to the information housed or processed within, to ensure its protection.

Controlled access to facilities provides a safe environment for its employees and protects the equipment necessary to perform business functions.

Examples include...

- Human Resources where confidential personnel records are stored and managed.

- Procurement because of contracts.

- Information Technology computer and network rooms because of critical equipment stored there

And critical information housed within RESD work areas



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 8

Classification of Assets

Classifying DGS information assets is critical

The classification process requires the identification of assets and their categorizing to determine the appropriate level of protection. It directs the way they are to be handled, processed, stored or transmitted. Classification also determines how or when they should or not be disclosed.

The State Administrative Manual has interpreted the Information Practices Act (IPA) and identified two main classifications for information assets (SAM 5320)

- 1) Confidential information which is broken into two subcategories. Personal / Private and Sensitive and
- 2) Public Information

Be aware that Personal and Sensitive information, may be *either* public or confidential, depending on the circumstances.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 9

Confidential Information

Confidential information is protected by law for disclosure to only authorized entities or individuals. According to the State Administrative Manual, confidential information is broken down into two categories, Personal/private Information and Sensitive information

Sensitive information may be confidential and should not be confused with personal information. It may pertain to non-personal information and tends to encompass departmental assets that need to be protected for their integrity and unauthorized access.

Sensitive assets may be available for public disclosure but only under certain conditions.

Personal / Private includes personally identifiable information such a name with Driver License, SSN, Health or Medical or Financial records or accounts. When this is inappropriately disclosed or compromised the department is required by law to notify the individuals that the information is linked to.

Again, Personal and Sensitive information, may be either public or confidential, depending on the circumstances.

If your office collects personal confidential information you must provide a privacy notice indicating what law authorizes the collection of the information, for what purpose and potential risk of unauthorized disclosure.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 10

Confidential Information Handling

DGS like all state agencies is directed by law and the specific program requirements on how and who can collect, use, and maintain information necessary to conduct state business.

Information is collected in the administration of programs.

When confidential information is collected, we are required to provide a privacy notice

When confidential information is accessed, it is to be done on a need to know basis and only as needed to perform official business of the department function.

Regardless of format, be it paper or electronic; confidential information must be stored in a secure fashion.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 11

Confidential Information Disclosure

The proper disclosure of confidential information is critical in retaining the information's security.

Information may be requested in person, by phone, mail or by fax.

Regardless of the method, the requestor must be identified and authenticated to ensure they are authorized to receive the information.

The law permits disclosure to:

- 1) The data subject or person the information pertains to.
- 2) Third Parties – A representative authorized by the data subject such as a legal representative, friend or relative. This authorization must be proven by the data subject
- 3) Federal or State public agencies if mandated by law are also authorized to receive confidential information. There must still be an agreement or contract to ensure terms and conditions are clear and that it is a legal disclosure.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 12

Public Information - Defined

As a public entity the Department of General Services must by law allow the public to inspect and / or obtain copies of the work produced by the department unless it is exempt from disclosure by law.

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

It is the responsibility of the department to ensure that this information is correct and is available when needed. Thus we must preserve integrity and availability of the information and the information systems that house or support its processing.

The systems on which public information is processed or made available remains classified confidential and must be protected from inappropriate access or manipulation.

Examples of Public information are: DGS Information on the internet, all communications and documents that are not classified as confidential/personal or confidential/sensitive).



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 13

Public Information Disclosure

Release of Public information also has a process for disclosure.

Work with your manager and or your Division's designated Public Records Request office. The Legal and Public Information Office are available to assist you with Public Release Act requests.

Though public information is available for disclosure upon request with a specific timeframe, it still needs to be protected to ensure its integrity

When DGS receive request for information it must be done in a timely manner, within 10 calendar days.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 14

Roles and Responsibilities

Now that we have explored assets and their classifications we can detail the most important element of the information security program.

You.

People are the key to the success of Information Security and privacy program.

You as an employee, contractor, supervisor, manager, or Executive play the key role in protecting department information.

Understanding your role in the development, use, and processing of information guides you in determining your responsibility and how to protect DGS assets.

Asset Owner

An asset or data owner is normally an organization.

It's who owns the information, the technology, facility or equipment.

The asset owner has the responsibility to classify the information and determine authorized access to owned assets based on the need to know.

They also ensure the confidentiality, integrity and availability of the resource

Normally, responsibility resides with the manager of the program that creates or employs the asset.

For example... when the information is used by more than one program, ownership responsibilities include the following considerations:

- Which program collected the information
- Which program is responsible for the accuracy and integrity of the information.
- Which program budgets the costs incurred in gathering, processing, storing, and distributing the information.
- Which program has the most knowledge of the useful value of the information.
and
- Which program would be most affected, and to what degree, if the information were lost, compromised, delayed, or disclosed to unauthorized parties



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 16

Custodian / Steward

Asset Custodian or Stewards have responsibility to:

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

Normally, information created or gathered is processed or stored in department networks and servers which are managed by Information Technology departments. This makes them the typical asset custodian.

With technology advances and the portability of equipment and information, users also have taken the role and responsibility of custodians / stewards.



Information Security & Privacy Awareness Annual Certification Training

Narration Transcript Part 2

Slide 17

User / Employee
