

information security is our shared responsibility



 information security office

<http://www.iso.dgs.ca.gov>

confidentiality - integrity - availability

Information Security and Privacy Awareness Annual Certification Training

Welcome to the Department of General Services Information Security and Privacy Awareness training. This training is required annually for all DGS employees, contractors and new employees upon hire.

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

The ISO provides DGS information security and privacy oversight for compliance with the State Administrative Manual and related Government, Civil and Penal Codes.

Through policy development, security awareness training, risk and incident management, the ISO is **your** resource to improving information security in your daily business.

The Information Security Office is located at the Ziggurat building in West Sacramento.

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

For more information about Information Security, please visit our website at www.iso.dgs.ca.gov

The ISO presents this Information Security and Privacy awareness training to inform you about DGS and State policy.

DGS recognizes...

- That information and department assets are essential public resources that must be protected.
- Access to the information or assets must be limited on a need-to-know basis only as required by law and to perform state business... and that
- Information Security and Privacy Programs are required to protect individuals' right to privacy, department assets, and to educate staff.

Strategic Design

The strategic design for implementing the DGS security and privacy programs requires a team effort.

The State Administrative Manual indicates that the Director is ultimately responsible for the protection of DGS assets.

The Information Security Officer has delegated oversight responsibility for information security and privacy risk management.

But in reality, securing DGS assets is a team effort which involves all DGS employees.

People are the key to making the DGS Information Security and Privacy programs a success.

All DGS employees, from our Director and Executive Management to office staff and maintenance personnel are responsible for good security and privacy practices. This includes our business partners such as contractors and other state and local agencies.

By understanding how information security and privacy affects the way we do business, we begin to create, use and apply good security practices.

Moving us forward to create a DGS Security Aware Culture.



Balancing Act

Information Security can be a balancing act between convenience and usability and good security practices.

Convenient usability is highest when security restrictions are relaxed. Heightened security while providing improved protection for assets also reduces ease of use and convenience for users.

If minimal security practices are in place, ease of use is extremely high and users can easily access information assets. However, in such an environment the probability of data loss or compromise is also extremely high.



On the other end of the spectrum, if extremely rigid security measures are put in place, business processes take a back seat to security and users end up spending more time dealing with security than getting work done. In this environment security becomes an obstacle to doing business.

Balancing Act

Striking a balance between good security practices and acceptable levels of usability are crucial to the success of an effective information security program.

Defining information assets and determining the best approach to protect them are the first steps programs must take toward this balanced goal.

The key function for Information Security and Privacy programs within DGS is to ensure that DGS's information assets are protected.

In order for DGS to successfully accomplish its mission and each division to do their job in support of that mission, we depend on our assets or resources to be reliable, accessible and available when we need them.

- **Confidentiality** addresses the collection, access, and disclosure of information
- **Integrity** addresses its accuracy and consistency
- **Availability** addresses the timely accessibility to information resources

Protection of department assets is accomplished through the development of risk management.

Starting by identifying assets through risk analysis, your office can begin to identify security threats and specific methods to protect your valuable assets.



Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems.

Breaches of confidentiality take many forms. Letting someone look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about DGS employees is stolen or lost, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Confidentiality is necessary for maintaining the privacy of the people whose personal information that DGS holds.



Information integrity means that data cannot be modified or changed without authorization.

Integrity is violated when an employee accidentally or maliciously deletes important data files, when a computer virus infects a computer, when an employee can change his own salary in ABMS, when a hacker vandalizes a web site and so on.

There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could simply mistype someone's address. On a larger scale, defective automated processes could change data incorrectly, leaving the integrity of the data compromised.

Information technology professionals are tasked with finding ways to create controls that prevent errors of integrity.



For any information system to serve its purpose, the information must be available when it is needed. This means that the systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must all be working correctly.

Availability is threatened by unauthorized access or intentional interruption to information or systems.

Examples of availability interruptions are lost or stolen documents, unsecured applications, websites or databases, and unstable or unreliable network connections to systems, email, or other services.

Now that we've explored some of the basic concepts of information security, let's look at how we go about bringing information security into how we do business every day.

We can basically look at it as

- What do we have?
- How do we classify and handle it?
- Who is responsible for all of this?

First, we'll look at our information assets. What we have to do to identify and inventory them. Then look at classifying these assets once identified.

Next, we'll look at the appropriate ways of handling and managing the information assets we are working with including proper methods for information disclosure.

Finally, we'll look at the roles and responsibilities of the different people or roles involved with securing our assets and how they must work together to create a complete information security aware workforce.

Information Assets

As we already know, one of the most important elements in risk management is knowing what assets you have, their value and how to protect them.

Identifying the information assets you have 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, be it confidential or public information.

Classifying information helps to determine the value of your information assets and the proper level of security that may or may not be required to protect this information.

Proper classification can ensure security and control costs if done well.

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

Identifying Assets

Lets start by defining what DGS Information Assets are.

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

- General information assets,
- Information system assets, and
- Information facilities.



All information, whether it is paper or electronically stored, processed or accessible from any where are information assets.

Items such as legal opinions, newsletters, email and personnel records can be included under the term information asset.

All Systems and Applications... technology tools and applications that allow Divisions access, storage and processing of data or information are considered information assets. Things like your personal computing devices, PCs and laptops, servers, flash drives, the network and related hardware are all considered information assets. Also, software purchased or applications developed by DGS are considered information assets.

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

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 the public, contract bids, email or text messages. All of these varied and diverse documents are also considered information assets.

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

Asset – Systems and 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 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.

Asset – Facilities and Equipment

DGS Facilities house critical resources important to accomplish our mission.

It is important to classify the facility or work areas according to the information housed or processed 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

Classifying DGS information assets is critical to protecting them

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 and identified two main classifications for information assets

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

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

Public Information Defined

As a public entity the Department of General Services must by law allow the public to inspect 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.

Public Information Disclosure

Release of Public information has a process for proper disclosure.

Work with your manager 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 within a specific timeframe, it still needs to be protected to ensure its integrity

When DGS receives requests for information it must be done in a timely manner... normally within 10 calendar days.

Confidential Information Defined

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 as a name with Driver License number, Social Security Number, Health, 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.

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.

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:

- The data subject or person the information pertains to.
- 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
- 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.

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 programs.

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.

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 collects 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.
- Which program would be most affected, and to what degree, if the information were lost, compromised, delayed, or disclosed to unauthorized parties



Asset Custodians or Stewards have the 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.

Normally, information created or gathered is processed or stored in department networks and servers. As information technology divisions are typically the ones tasked with managing and maintaining these resources, they are typically considered asset custodians.



However, with technology advances and the portability of equipment and information, individual users have also taken the role and responsibility of asset custodians.

Employee – User

As employees and direct users of information assets, we come into direct contact with information and data every day. Employees are authorized to make changes, updates or even deletions of data. Because of this, employees have considerable impact to the confidentiality, integrity and availability of the assets we work with.

This makes each of us the first and last lines of defense in protecting our information assets.

Now that we know a little about the different roles and what role we might play in the department's security strategy, let's look at some security best practices that we can use in our workplaces every day.

For our discussion of "Security Best Practices" we will be covering four basic topics.

- **Facility Security** - general practices to ensure that our offices, buildings, shops and equipment are safe and secure
- **Electronic Security** - takes it one step further in ensuring that the electronic tools we use remain secure.
- **Social Engineering** - where we as individuals become the most essential link in the chain of information security
- And lastly, **Acceptable Use** where we explore some of the activities that are not appropriate in DGS computing environments

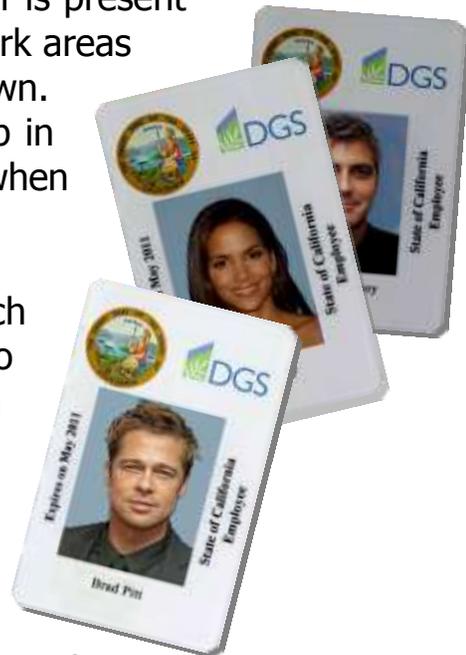
Keeping our facilities secure from outsiders produces a direct impact on helping ensure our people, systems and data are safe.

This begins with using the DGS ID badge. Being readily identified ensures that only authorized staff is present when working in sensitive areas or with sensitive information.

Once we ensure that only authorized staff is present in our work areas, we can ensure that work areas are properly secured or locked down. Sensitive information should be locked up in secure offices or locked file cabinets when not in use.

Access cards should be issued to each individual employee to allow access to work areas. Keep your access card with you at all times to avoid theft and potential unauthorized access.

Care should be taken when using access cards to enter work areas. Tailgating is the process of allowing another person to follow behind you when accessing a secure area using an access card. Disallowing tailgating ensures that personnel are authorized entry and that work areas remain secure.



Securing Computer Devices

Because so much of the data we manage has become so portable, individual users have become data custodians and are responsible for safeguarding data from loss or theft.

Just as we must secure our facilities and offices, it is important to properly secure our laptops and personal computers, flash drives and smartphones as well as traditional paper files. These types of portable media should be properly stored in locked cabinets or offices. Devices should be encrypted with password protection to ensure that if the device is lost or stolen, the data contained remains secure.

When leaving your computer unattended, be sure to “lock” your computer. On windows PCs this is done quickly and easily by pressing and holding the “windows key” and “L” together. This immediately locks your computer. Locking your computer ensures that other users cannot use your computer while you are away.



Proper handling of the physical devices goes hand in hand with the proper management of sensitive data. Retired PCs, laptops, and servers headed for surplus property should be inspected for sensitive data and the data removed and the disc drives properly sanitized prior to disposal. This along with proper shredding and disposal of sensitive paper documents prevents data “leakage” through unexpected channels.

Your account on DGS networks is special. It has been set up for you, for your exclusive use. It has features that help you to get your work done and establish your online identity in regards to email and access to files and information assets throughout DGS. The primary method that your account or identity is protected is by the password you create on your account. Using a strong, secure password not only helps to protect DGS assets, but ensures that your account and files are kept safe.

The best defense against password cracking is to create a password that is hard to guess. Passwords should also be at least eight characters long and include a few symbols—such as the dollar sign, “star”, or exclamation point—as well as letters and numbers. Long, complex passwords are much harder to break than short simple ones. Avoid using personal information such as names of family members, friends or pets. Also, avoid using birthdays or the names of your favorite sports teams or bands.



Whatever passwords you create, it is best to never share your passwords with anyone or allow yourself to be tricked into giving them away. Don't write down your password. Commit it to memory. Change your password according to DGS policy and remember that creating a strong password and protecting its secrecy is critical to protecting DGS information and systems as well as for protecting your own personal information.

Telework Mobile Security

With Telework on the rise many DGS employees are finding themselves working either while mobile or outside the confines of DGS facilities.

Special care should be taken to ensure that you are working securely while teleworking from home, in a remote location, or using mobile devices such as smart phones.



If possible, avoid using public “hotspots” for Internet connections and avoid working with sensitive material in public places to avoid the possibility of “eavesdropping” by passers-by.

If you must access DGS resources via a wireless network, ensure that connections are secure using wireless encryption and try to keep sensitive material access to a minimum.

The basic rule of thumb with mobile security is to let the work you are doing determine the level of protection or security. If you find that you can not properly ensure the security of your work at the mobile or remote location, then it is probably best to conduct your work when you can get to a more secure location.

Avoiding Security Pitfalls

The result of almost all security violations, incidents or pitfalls is the loss or unwanted release of data. Whether its private information, personal pictures, banking information, or any other data that was not intended to be shared.

Most of the security pitfalls today are centered on a type of attack referred to as "Social Engineering." Social engineering is the art of tricking or fooling a person in to giving out information that they shouldn't. It is used to gain information such as passwords, schedules, locations of people or important assets, or even something as simple as a private phone number. The smallest, mundane piece of information can be used by this type of attacker as they can combine many small pieces of information together to create a detailed plan of attack against our department.

This type of attack centers around contacting you personally... via

- Phone Calls
- Emails
- Personal Contact

Through a technique called "phishing" an attacker tries to prod his victim for information. This can be done by a phone call asking for sensitive information, or asking questions that may seem "out of the ordinary." Spam emails often do the same thing by asking for sensitive information or asking you to click a link that leads to a suspicious website.

Attackers are always looking for the easiest way to attack our department. And because its human nature to be helpful and give people as much information as we can give that is asked from us, we can find ourselves becoming the easiest point of attack.

Avoiding Security Pitfalls

It is possible to avoid security pitfalls while remaining helpful in providing information to our customers.

The best way to avoid these security pitfalls is to remain vigilant.

Take a moment to ask yourself,

- “Can I verify who this person is?”
- “Is it ok to give out this information?”
- “What does this person need the information for?”

If you don't feel comfortable providing information to a person over the phone, you can offer to take their information and return their call later. This gives you the opportunity to ensure that the caller is genuine and to check with your supervisor to ensure the information is properly handled.

If you receive an email message warning of dire consequences or threatening circumstances, it is more than likely a “phishing” attack and should be immediately deleted. If the email “looks” genuine and you are not sure, your best option may be to simply call the organization in question and ask.

Don't let security hackers take advantage of you. Taking time to question and validate transforms you in to the **strongest** link in the information security chain!

Social networking websites such as Facebook and Twitter are used for people to connect with other people. Some people use these websites for business, social interaction or even romantic purposes. These websites allow you to provide information about yourself and offer a way to communicate quickly and easily with other users. Because of this active communication platform, all of the elements of Social Engineering become even easier with Social Networks. Much in the same way they are affected in email.

Many social networking attacks focus on impersonation or having a person pretend to be you, while attempting to gain information from your group of friends and family. And because an attacker is impersonating you... people are much quicker to provide information or help if the attacker pretends to be in trouble.

When using a DGS network social networking sites should only be visited for business purposes only.

And whether it is work related or in your personal home use, it is best to remain vigilant when visiting social networking websites.

Acceptable Use

Included in the security and privacy requirements is the Acceptable Use of DGS resources. Users are subject to compliance with the acceptable use standards.

The state reserves the right to monitor any and all usage and authorized users should expect no privacy while accessing DGS information assets.

Incidental personal use of state resources for email or internet is permitted, but such usage must not interfere with normal job performance and must not pose a security risk for the department. Furthermore, DGS assets must not be used for private gain, inappropriate, obscene or illegal activities.



DGS email is intended to be used for authorized business use only. As such, forwarding or sending email containing sensitive, or personal information from the DGS e-mail system to external email is prohibited. Creating or forwarding spam messages is prohibited. Also using email to harrass or threaten others is prohibited.

All software used by DGS employees is to be installed and managed by IT Services Division. Any unauthorized software will be immediately removed. Any copying of copyrighted material for which DGS does not have an active license is strictly prohibited. Certain software such as hacking tools and peer to peer file sharing software pose a specific security risk and will be immediately removed.

Security Incident Management

No matter how hard we work in avoiding the pitfalls of information security, sometimes things don't work as planned and data or information assets are lost or otherwise compromised. When this happens, a security event has taken place.

Policy states that a security incident is any intentional or unintentional event which may result in unauthorized access, loss, disclosure, modification, or destruction of information resources or assets.

For example,

- The loss or theft of a laptop, mobile phone, or briefcase whether it contains personally identifiable information or not.
- The accidental release of confidential information through a forward of a sensitive email.
- Visiting of inappropriate web sites
- Using State Resources to conduct a personal business
- Or sharing of a DGS user name and password.

These are just a few examples of security incidents that must be reported to the ISO. Failure to report such incidents does not comply with State requirements, and puts the department at risk and in violation of the law.

Security Incident Management

(Multimedia Video)

Security Incident Management

Any suspected, attempted, or actual security incident must be immediately reported.

In the event of a suspected or actual incident an employee must immediately inform their supervisor.

The Supervisor then reports to the ISO. The ISO will determine whether or not an actual security incident has occurred and appropriate actions to take. Once reported within DGS, the ISO reports to the appropriate external departments and manages the incident through the entire reporting process.

The supervisor is also responsible for completing the Security Incident Report Form and submitting it to the ISO within two days.

When in doubt, report it.

Measuring Success

We put our best foot forward by using good practices and tracking our security and privacy pitfalls through effective incident management.

As a department, we must take time to take score, measure our successes and our deficiencies.

Tracking allows us to identify potential problems that may exist in our department. It also brings to light issues that may or may not be working in support of how we conduct business. Through time, if we identify that a particular issue reoccurs time and time again, we can take steps to improve business processes or policies to make things work better.

Some ways DGS is measuring performance today, help ensure our department moves forward toward continued success...



- Conducting and tracking security and privacy training by employees to ensure all staff are trained in basic information security.
- Monitoring network traffic to ensure acceptable use policy requirements as well as eliminate potential technology threats.
- Scanning of personal computers to ensure that unauthorized software is not loaded without proper approval
- Monitoring projects and conducting risk assessment prior to going live or into production.
- The reporting of potential security or privacy violation events

By maintaining an effective monitoring and performance measurement process, the department will continue on track to achieve information security success.

Working together as a team, we will find ourselves transformed into a Security Aware Culture.

Security & Confidentiality Acknowledgement

After completing this training, be sure to print out and complete the Security and Confidentiality Acknowledgement form. The completed form shall be submitted to your supervisor. This form certifies that you have completed the training for this year.

Supervisors will maintain the form in the employee files and ensure the training is entered into ABMS.

Detailed instructions for employees and supervisors are available on the form's instruction sheet.

This concludes the Information Security Awareness training.

For any questions regarding this training presentation or information security issues or incidents, please feel free to contact the information security office directly.

We are located in the Ziggurat Building in West Sacramento

We can be reached by phone at 916 376 3940

By email at dgsinfosec@dgs.ca.gov

Or on the internet at www.iso.dgs.ca.gov.

information security office

707 Third Street
West Sacramento, CA 95605

(916) 376-3940

dgsinfosec@dgs.ca.gov
<http://www.iso.dgs.ca.gov>