DEPARTMENT of REHABILITATION
Employment, Independence & Equality

Protecting Privacy in State Government

A SELF-TRAINING MANUAL FOR EMPLOYEES AND CONTRACTORS OF THE CALIFORNIA DEPARTMENT OF REHABILITATION

January 2017

Table of Contents

Instructions

The California Office of Privacy Protection created the self-training manual, “Protecting Privacy in State Government,” that the Department of Rehabilitation revised to meet its business needs.

This document is designed to be a self-assessment tool and does not require a specific percentage to pass. The review questions at the end of each section are an assessment of how well you have understood the training material.

If you choose to print the training manual, you can mark your answers to the review questions on the hardcopy document. If you choose instead to read the manual online, you may write the answers down on another piece of paper and then check them against the answers provided. For those utilizing a screen reader, you can open a blank document and place your answers on a separate screen, and then compare the answers to the questions by using Control F6 to move from screen to screen.

Each employee must complete this self-training, and print and sign the acknowledgement form. The form is located at the end of this document.

In this Manual

All state employees, contractors, and individuals who perform services for or on behalf of the Department of Rehabilitation (DOR) have a duty to protect the privacy for all Californians. Your job may require you to routinely work with personal information, or you may only occasionally come into contact with it on the job. In either case, you have the ability and the duty to handle it properly. Protecting personal information is essential to protecting the privacy of your fellow Californians.

This training is required pursuant to State Administrative Manual (SAM) Chapter 5300, and is intended for all DOR employees regardless of classification, as well as contractors and other individuals who perform services for or on behalf of DOR. The laws discussed apply to all state departments[1] and the practices recommended fit many different work situations.

The Manual will give you basic information on how to manage personal information responsibly in your job.

- You will learn about the basic information privacy laws that apply to state government.
- You will learn some good and bad practices for handling personal information in your job.
- You will learn how to recognize and report an information security incident.
- You will learn some of the consequences of mishandling personal information, both for you and for those whose information is involved.
- You will take quizzes at the end of each section to help you review what you've learned.

Reading through the Manual is one step towards developing a greater awareness of privacy. Think about what you can do to contribute to a culture that respects privacy in your workplace.

[1] The term department in this manual refers to any type of state government agency, such as departments, boards, commissions, bureaus, offices, and others.

Section 1: Why Protect Privacy?

IN THIS SECTION

You have various duties in your job with the State of California, or as a contractor or individual who performs services for or on behalf of the State of California. An important part of every State employee's, contractor's, or individual's job is protecting the personal information managed by your department, your business, or you. In this section, you will learn why protecting personal information - protecting privacy - is everyone's job.

It's the law!

Our State Constitution includes a specific privacy right among the inalienable rights of all Californians.[2] There are also other laws that require state departments to protect personal information.

The Information Practices Act of 1977 is the comprehensive privacy law for state government.[3] It sets out the basic requirements for all state departments, employees, and contractors on handling and protecting personal information.

Federal Agencies Require It

As a recipient of funds from the Social Security Administration, the DOR must certify that it has made every reasonable effort to ensure that its employees know the rules of conduct in protecting and reporting the suspected loss of personal information.

Security Breaches

In recent years, the news has been filled with stories about companies and government agencies notifying individuals that their personal information was on a stolen laptop or involved in some other kind of security breach. The law requires notifying people of such breaches in order to give them the opportunity to take steps to protect themselves from possible identity theft. Such incidents are expensive for a state department. In addition to the hard costs of mailing notices to large groups of people, the department also faces a loss of public confidence.

Identity Theft

Stealing personal information has become a popular way for dishonest people to make money. Law enforcement calls identity theft the crime of our times. It is a crime whose victims are harmed financially and in other ways. The growth of this crime in recent years puts an increased burden on all organizations, including state government, to protect the personal information in their care.

Public Trust

People entrust their most sensitive personal information – tax, financial, and medical information to state agencies. In most cases, they have no choice. Consumers can choose another bank or store if they're not happy about how their personal information is handled, but they can't go to another Department of Motor Vehicles (DMV) to get a driver's license, or to another Franchise Tax Board to pay their state taxes.

---

[2] California State Constitution, Article 1, Section 1.
[3] California Civil Code Section 1798 and following.

This places a special obligation on government employees, contractors, and other individuals. If we fail to protect personal information or to use it properly, we can undermine our citizens' faith in government. Protecting personal information means protecting people. It's a matter of public trust.

Section 2: Identity Theft and Its Impact

IN THIS SECTION

Identity theft is taking someone else's personal information and using it for an unlawful purpose.[4] It is a crime with serious consequences. In this section, you will learn about the different types of identity theft and what they cost victims and businesses.

Types of Identity Theft

Government Documents and Benefits

There are several types of identity theft. The most common type of reported identity theft is government documents/benefits fraud, which represents about 39% of reported identity theft.[5] Government documents fraud, also known as identity fraud, is the manufacture, sale or use of counterfeit identity documents (e.g., fake driver's licenses, birth certificates, Social Security cards or passports) for immigration fraud or other criminal activity. Government benefits fraud is the misrepresentation or omission of facts on an application to obtain government benefits one is not entitled to (e.g., U.S. citizenship, a valid visa, unemployment insurance, disability insurance, Medi-Cal).

Existing Accounts

Another common type of identity theft is the fraudulent use of an existing credit account. Recovering from this type of identity theft has become fairly easy. If you discover a purchase you didn't make when reviewing your monthly credit card statement, you simply call your bank and follow up with a letter disputing the charge. Your dispute generally leads to the charge being removed. Federal law limits liability for an unauthorized credit card charge to $50 when you report it, and often there's no charge at all.[6]

New Accounts

New account identity theft is when a thief uses information like your name and Social Security number to open new credit accounts. This type of identity theft can be much more difficult to deal with. The victim often doesn't find out for many months, perhaps when contacted by a debt collector. It takes many phone calls, letters, and hours of work to clear up this type of identity theft.

Employment and Medical Identity Theft

An identity thief may use a victim's Social Security number when applying for work. This can lead to increased tax obligations for the victim. A thief may also get medical treatment in the victim's name. Medical identity theft not only means unauthorized

---

[4] Penal Code Section 530.5

[5] Federal Trade Commission's *Consumer Sentinel Network Data Book for January – December 2014*, which was published in February 2015.

[6] Fair Credit Billing Act, 15 U.S. Code Section 1666

payments, but it can also pollute the victim's medical records with inaccurate information. This can put the victim at risk of receiving inappropriate medical treatment.

Criminal Identity Theft
Criminal identity theft is often the most difficult type to resolve. All identity theft is a crime, but the term criminal here means using someone else's identifying information when arrested or charged with a crime, thereby creating a criminal record for the victim. The victim may be arrested and not released until after a fingerprint check. The victim may be unable to find work because of inaccurate information in a background report.

Identity Theft Facts
In 2014, 12.7 million U.S. adults were victims of identity theft.[7] According to law enforcement, identity theft is a low-risk, high-reward crime. The risks are low because a thief doesn't have to face his victim and because it's a non-violent crime with lower penalties than armed robbery.

Cost of Identity Theft
To repair the damage done by an identity thief, a victim incurs costs such as unreimbursed monetary losses, lost wages as a result of time spent to resolve the identity theft, and any related legal and credit monitoring costs.

The time a victim must spend to clear up an identity theft situation can range from a few hours to many days. New account or criminal identity theft can require hundreds of hours of phone calls, letter writing, and even court appearances spread over many months or years.

The total cost of identity theft in 2014 was $16 billion. Because consumers ultimately pay the business costs through higher prices for goods and services, we all pay for identity theft.

Section 3: State Government Privacy Laws

IN THIS SECTION
This section gives an overview of the main privacy laws that apply to all California state agencies. These are not the only laws on protecting personal information in government. There are also state laws that protect specific kinds of personal information, such as HIV diagnoses, tax information, and driver's license information. There are also federal laws that apply to certain state agencies.

Information Practices Act

The basic privacy law that applies to all state agencies is the Information Practices Act of 1977.[8] This law sets the requirements for agencies on the management of personal information.

---

[7] Statistics cited in the "Identity Theft Facts" and "Cost of Identity Theft" sections of this training manual are from the Javelin Strategy & Research's *2015 Identity Fraud Report*, which was released in March 2015.
[8] Civil Code Section 1798 and following

The Information Practices Act defines personal information as any information that is maintained by a department that identifies or describes an individual. The broad definition includes information such as the following:

- Name
- Social Security number
- Physical description
- Home address
- Home telephone number
- Education
- Financial matters
- Medical or employment history

The Information Practices Act allows agencies to collect only the personal information they are legally authorized to collect. It gives individuals the right to see their own records and to request that any errors be corrected. It also requires agencies to establish appropriate and reasonable administrative, technical and physical safeguards to protect personal information from a wide spectrum of threats and risks such as unauthorized access, use, disclosure, modification, or destruction. The next section of this manual will cover some examples of practices for safeguarding personal information.

Public Records Act

The Information Practices Act interacts with the Public Records Act.[9] The Public Records Act makes most state records open to the public, with certain exceptions. The Information Practices Act requires protecting personal information, even when it is part of a record that is open to the public. That's why state agencies routinely redact or otherwise delete personal information before releasing public records. Check with your department's Public Records Act coordinator, Public Information Officer, external affairs office, or legal office when responding to requests for information pursuant to the Public Records Act.

Consequences

There are penalties for violating the Information Practices Act, both for a department, which may be sued, and for an employee, who may be disciplined.

- An individual may bring a civil action against a department that violates the Information Practices Act if the violation results in an adverse impact on the individual.

- An employee who intentionally violates the Act may be subject to disciplinary action, including termination.

- An employee who willfully obtains a record containing personal information under false pretenses may be guilty of a misdemeanor, with a penalty of up to a $5,000 fine and/or one year in prison.

[9] Government Code Sections 6250-6270

Notice of Security Breach Law
The Information Practices Act requires departments to notify people promptly if an unauthorized person acquires certain personal information. Such a breach might be the loss or theft of a laptop containing personal information, an intrusion into a state computer system by a hacker, or the mailing of a disk or letter containing information to the wrong person.

The law was passed to alert people when their personal information may have fallen into the wrong hands, thus putting them at risk of identity theft. People who receive a notice of a breach can take steps to protect themselves against the possibility of identity theft. For example, if your Social Security number is involved in a breach, you can place a fraud alert or a security freeze on your credit files, which will protect you from new accounts being opened using your information.[10]

The personal information that triggers the notice requirement is the kind that identity thieves want. It is a name plus one or more of the following:

- Social Security number
- Driver's License or California Identification Card number
- Financial account number, such as a credit card or bank account number
- Medical information
- Health insurance information

If the information is encrypted, or scrambled so that it is unreadable, there is no requirement to notify individuals.[11]

State Policy on Notification
State policy requires agencies to notify individuals whenever an unauthorized person has acquired unencrypted personal information of the type listed above. This policy applies whether the information is in digital format, such as on a computer or CD, or in paper format, such as on an application or in a letter.[12]

Social Security Number Confidentiality Act
The Social Security Number Confidentiality Act seeks to protect against identity theft using Social Security numbers.[13] With a name and a Social Security number, an identity thief can open new credit accounts and commit other financial crimes in the victim's name. Therefore, this law applies to state agencies and to other entities in California by prohibiting the public posting or display of Social Security numbers (SSN). It also specifically prohibits a person or entity from doing any of the following:

[10] Refer to page 33 (Section 5, Subsection "Information for Consumers") for sources of consumer information on identity theft.
[11] Refer to pages 22-23 (Section 4, Subsection "Protect Personal Information on Portables") for the State policy on encryption of personal information on portable devices.

[12] State Administrative Manual Chapter 5300.
[13] California Civil Code Sections 1798.85-1798.89.

- Printing a SSN on identification/membership cards (e.g., health plan cards, student ID cards),
- Requiring an individual to transmit his or her SSN over the Internet (e.g., email) unless the connection is secure or the SSN is encrypted,
- Mailing documents with SSN to an individual unless required by law, or
- Requiring an individual to use his or her SSN to access a website unless a password is also required.

California Code of Regulations (CCR)
Current DOR regulations contain specific "Confidentiality" provisions applicable to the collection and disclosure of personal information, and to releases. These provisions are set forth in California Code of Regulations, Title 9, Sections 7140 through 7143.5.

Section 4: Recommended Privacy Practices

IN THIS SECTION
Protecting personal information from unauthorized access, use, disclosure, modification, or destruction is one way to protect individuals' privacy. In this section, you will learn about good - and bad - practices for protecting personal information.

The practices described are recommended for all state employees, contractors, and other individuals who handle personal information. They are for the person in the cubicle, the office, the mailroom and the warehouse, and at an authorized telework or other remote location - wherever state workers and contractors do their jobs.

Some of these practices may not be appropriate for a particular work situation. If you think that is the case for your job, contact your department's Information Security Officer or Privacy Officer. They can help you with procedures that will allow you to work efficiently, while protecting personal information.

These practices are intended to protect personal information - but they would also protect other kinds of confidential information. In addition to personal information, your department has other kinds of confidential and sensitive information that it must protect. This may include security-related information such as descriptions of your department's computer network configuration, some financial information, or drafts of policy documents.

Personal Information = Money
Law enforcement tells us that personal information – especially information such as names and Social Security numbers, is worth money. There's a black market for it and identity thieves use the information to steal money.

If you thought of personal information as cash, you would probably handle it differently, wouldn't you? For example, would you leave a stack of $100 bills lying on your desk, even if you were away just for a short meeting or a break?

This is how we should all think of the personal information in our care.

Know Where Personal Information Is

Where do you keep personal information at your workplace? Pay particular attention to information such as Social Security numbers, driver's license numbers, California Identification Card numbers, financial account numbers, and medical information.

The first step to protecting personal information is to know where it is. Take a look around your workstation. Remember to look for information on employees, as well as consumers, licensees, and others. Personal information can be on different types of media (e.g., electronic, paper). Places to look include, but are not limited to, the following:

- Your desk or countertop
- Your desktop computer
- Your workstation file drawers, cabinets, shelves, and bookcases
- Your laptop, tablet, smartphone, and other mobile computing devices
- Your disks, CDs, DVDs, USB flash drives, hard drives, and other portable electronic storage media
- Your cell phone, digital voice recorder, printer, scanner, and other electronic devices

Do you download personal information onto your computer and other electronic devices? Do you put printouts containing personal information in file folders while you're working on them, and then leave the file in an unlocked drawer in your workstation? Do you have CDs, DVDs, USB flash drives, or disks with personal information on them?

Keep Personal Information Only As Long As Necessary

Once you've located where you keep personal information in your workstation, consider whether you really need to keep it all. There are some kinds of records that we are required to keep for legal and policy reasons. But there are probably lots of other files - paper and digital, that we don't need to keep beyond the period when we are working on them. Refer to your Records Retention requirements for specific time periods.

- Develop the habit of regularly purging documents with personal information from individual file folders.

Pursuant to DOR policy, do not download personal information onto your computer hard drive, USB flash drive, or other portable devices/media.

Dispose of Records Safely

One way that identity thieves steal personal information is by going through trash. It's called "dumpster diving." Shred documents with personal and other confidential information before throwing them away. Always use a cross-cut or confetti-cut shredder to destroy documents containing personal, confidential, or sensitive information. You can shred CDs, DVDs, and credit cards in most cross-cut or confetti-cut shredders, too. A straight-cut shredder should never be used, since it does not adequately destroy the documents.

- Don't throw documents containing personal information into your wastebasket or recycling bin - shred them.

- Use Confidential Destruct boxes/bins and an onsite shredding service (approved vendor shreds the documents at your worksite) for large quantities of documents containing personal, confidential, or sensitive information.

- Be sure to watch the onsite shredding service actually shred the documents.

- Be sure to protect Confidential Destruct boxes/bins. It's as if they're labeled, "Here's the good stuff - steal this first!" If the Confidential Destruct boxes/bins are not locked, don't leave them unattended during the day, and be sure to lock them up overnight.

- Deleting files from your computing devices (e.g., computers, tablets, smartphones) doesn't completely remove it from your computing devices. To protect personal information, computing devices must be sanitized using an approved destruction method before disposal, surveying, repairing, returning, replacing, upgrading, or other activities/services involving individuals not authorized to access the personal information. Sanitization is the process of wiping, overwriting, or destroying data and information in a special manner so that the data and information cannot be restored/recovered.

- Portable electronic storage media (e.g., USB flash drives, hard drives, CDs, DVDs, disks, SD cards) and other electronic devices (e.g., servers, printers, routers, copiers, fax machines, scanners, digital voice records, notetakers) must also be sanitized using an approved destruction method.

Protect Personal Information from Unauthorized Access

Not everyone in an office needs to have access to all files and databases containing personal information. Access to personal information - especially information like Social Security numbers, driver's license numbers, financial account numbers, and medical information - should be limited to only those who need to use it to perform their duties.

- Don't give access to coworkers who are not authorized.

- Don't share your user IDs or passwords or your keys to the file cabinet with others.

- Keep private and not share any of your user IDs, passwords, keys, codes, or other methods that are used to access the network, computers, tablets, smartphones, systems, applications, databases, voicemail, records, offices/rooms, files cabinets, and other information assets.

- When in doubt about someone's access privileges, check with your supervisor/manager.

Protect Personal Information in Workstations

Store documents, media, and devices containing confidential, sensitive, or personal information in secure places (e.g., locked cabinets and drawers) when not actively using.

Protect your computing devices (e.g., computers, tablets, smartphones) from unauthorized access or use.

- Lock your device/screen when not actively using your computer, smartphone, or tablet. For computers, a good way to remember this is to think "Ctrl-Alt-Delete," before you leave your seat.

- Use strong passwords. Don't use obvious facts or numbers as your password - not your Social Security number, your spouse's, child's or pet's name, and not a birth date or anniversary.

    - Stronger passwords are made up of at least eight characters, including letters, numbers, and symbols. One way to create a memorable password that others can't guess is to use the first letters of a sentence that has meaning to you, then substitute numbers or symbols for some letters.

    - For example, "How much wood could a woodchuck chuck?" could be HMWC1WC2? (Don't use this example as your password.)

  Remember, your password is like your toothbrush: Change it often, and don't share it!

  The DOR's policy is for all employees to regularly change their passwords.

- Don't download any software onto your computing devices, especially from unknown or untrusted sources (e.g., websites). It could contain hidden spyware or malware. Spyware and malware can slow down the operation of your computing devices, send annoying pop-up ads, or introduce a virus into the department's network. One kind of spyware and malware, called a "keylogger," can record all your keystrokes, sending your user ID, password, and other confidential information to someone else. Check with your department's Help Desk (information systems/technology support) or Information Security Officer before downloading any software.

  The DOR's policy is that employees are not allowed to download and install any software. Requests can be submitted to the Help Desk if any software has to be downloaded and installed for departmental business.

Protect Personal Information on Portables

It is state policy that departments must use encryption to protect personal, confidential, and sensitive information that is transmitted or accessed outside the secure internal network of the department (e.g., email, remote access, file transfer, Internet/website communication tools), or stored on portable electronic storage media (e.g., USB flash drives, tapes, CDs DVDs, disks, SD cards, portable hard drives), mobile computing devices (e.g., laptops, tablets, smartphones), and other mobile electronic devices.

Several of the security breaches requiring notification have involved lost or stolen laptops, portable electronic storage media, or other mobile electronic devices. We can protect this information by encrypting it, or scrambling it so that it's unreadable.

When personal information on portable devices is encrypted, it cannot be accessed or used by an unauthorized person. If the data is encrypted, the department will not be legally required to notify individuals of the incident.

In addition to protecting the information on a device, employees should take care to protect the devices themselves. Don't leave a laptop or a smartphone device visible in an empty vehicle, in a locker at the gym, or unattended in a public location. It only takes a few seconds for a thief to smash a window or break a lock and take what they want.

Protect Personal Information in Transit
Transmitting information electronically can make our work easier and more efficient. But some transmission methods, as well as some traditional means, can pose privacy risks if not used properly.

Email
Think of email as a postcard. It isn't private. It's also very easy to mistype an email address and send the message to the wrong person. Don't use email to send or receive personal information like Social Security numbers, driver's license or California Identification Card numbers, financial account numbers, medical information, or health insurance information. Before sending emails, check the email addresses to ensure that the message is being sent to the correct individuals and that these individuals are authorized to have access to any personal information contained in the message.

Voice Mail
Don't leave personal information in a voice mail message. You don't know who will pick up that message. Instead simply leave a message to call you back. This precautionary measure also applies to leaving messages with an individual who may not be authorized to have access to the personal information. This individual may also put the message where it is visible or readable by other individuals who may not be authorized to have access to the personal information.

Regular Mail
Use secure procedures for regular mail, which often contains personal information. Mail thieves are after personal information to commit identity theft. Don't leave incoming or outgoing mail in unlocked or unattended receptacles. Also, be sure to include the name of the intended recipient in the address rather than just the name of a business organization. Without a name, mailroom staff must open and read mail to determine the appropriate recipient.

Delivery Services
"Track" packages and large envelopes when authorized to send a large amount of personal information (e.g., paper files for one or more individuals). Provide the estimated date of delivery to the recipient and request independent confirmation of the delivery from the recipient once the item has been actually received.

Fax
Don't send personal information by fax, unless you use security procedures. You don't know how long a fax will remain on a machine or who might see it or pick it up. If you need to fax personal information, make special arrangements with the recipient.

Arrange for and confirm prompt pick-up of the fax. Also check the accuracy of the fax number and take care when keying it in.

Wireless
Don't use wireless networks to access, communicate, or transmit personal information, unless you ensure that the wireless network is managed and secured by a known and trusted source, and that sufficient safeguards are in place (e.g., strong encryption, password protection) to comply with the security requirements described in State policies and standards (e.g., Telework and Remote Access Security Standard [SIMM 5360-A]).

Internet
Don't share or disclose personal information on the Internet (e.g., websites), unless you have obtained a signed release from the affected individual, and written authorization from your supervisor/manager and your department's Public Information Officer, Privacy Officer, and/or Information Security Officer.

Protecting State Information at Home and Away
Don't take or send state records containing personal or other confidential information out of the office unless you are authorized to do so by your supervisor/manager.

Securely store state records, laptops, smartphones, and other state information assets in your home or other authorized work location and not in a vehicle during the night or for an extended period of time (e.g., shopping). Individuals at your home or other authorized work location must not have access to the state records, laptops, smartphones, or other state information assets.

Ensure that individuals who use your personally-owned computers or smartphones do not have access to state records, which may contain personal, confidential, or sensitive information.

Only use computing devices (e.g., computers, tablets, smartphones) that are not available to the general public, and are approved by your supervisors/managers to make remote connections in a secure manner.

Implement and maintain fundamental security controls and practices when remotely accessing state information assets, and use the same safeguard requirements as at DOR offices when authorized to use an alternative work site, such as your home or other non-traditional work sites. The fundamental security controls and practices include, but are not limited to, strong passwords, two-factor authentication, device and data encryption, antivirus/malware protection software, personal firewalls, automatic updates, and secure configurations of web browsers, operating systems, and personal networks (wired and wireless).

Beware of Social Engineering Schemes
Social engineering is stealing personal information by deception. Identity thieves try to trick people into disclosing personal information. One common form is what's known as "phishing" - an email that looks like it's from a bank, a government agency, or a Help Desk/IT Support. It may ask you to confirm your password, account number, or Social Security number. It often claims to be part of an effort to protect you from fraud. It also

may ask you to open an attachment containing malware, or click on a link to a fraudulent or malicious website. The advice to consumers on phishing, which can take place over the phone or by email, is **never give out any personal information unless you initiated the contact**.

As a state employee, you may find yourself the target of this type of identity theft attempt. It may be part of your job to give information, including personal information, to people who call and ask for it. Social engineering schemes also target businesses and government agencies, relying on workers' desire to provide good customer service.

How do you know that people who ask you for personal information are authorized to have it? Because of concerns about social engineering, it's important to verify the identity and the authority of anyone who requests personal information. When the request is made in person, verification is usually done by asking to see a photo ID card. When the request is made by phone, other procedures must be used for verification before giving out personal information. If you're not sure how to verify someone's identity or authority to receive information, ask your supervisor/manager.

Report Information Security Incidents

In order to be able to maintain good information security – to protect the information people give to us – employees must recognize and report promptly information security incidents.

Be alert to incidents that could expose personal, confidential, or sensitive information to unauthorized access, use, disclosure, modification, or destruction. Some examples of disclosure methods are electronic, paper, and verbal. Incidents that must be reported to your supervisor/manager and the DOR Information Security Officer include, but are not limited to:

- Loss or theft of a computing device (e.g., computer, tablet, smartphone), BlackBerry, cell phone, or other electronic devices
- Loss or theft of a CD, DVD, disk, USB flash drive, or other storage media containing personal information
- Loss or theft of paper records containing personal information
- Mailing or faxing documents containing personal information to the wrong person
- Hacking into state computer systems

When in doubt, report it!

The DOR's policy requires employees to immediately notify their supervisors/managers and the DOR Information Security Officer of any actual or suspected information security incidents. Supervisors/managers are responsible for notifying the District Administrator or Section Chief, and for ensuring that the DOR Information Security Officer has been notified.

A Matter of Respect

Protecting privacy is a matter of respect - respect for our fellow citizens and others who entrust us with their personal information, and respect for our co-workers, whose information is also in our care.

Protecting personal information is not something an Information Security Officer or a Privacy Officer can do alone. We all touch some personal information in our offices and we are all responsible for protecting it. Protecting personal information is protecting people.

Section 5: Additional Security and Privacy Resources

Information for State Government and Other Organizations

- Privacy practice recommendations for organizations from the California Department of Justice, Privacy Enforcement and Protection Unit are available at the following link: http://www.privacy.ca.gov/.

- Information privacy and security policies and resources, including security and privacy training, incident management, disaster recovery, risk management, and other topics from the California Information Security Office are available at the following link: http://www.infosecurity.ca.gov/.

Information for Consumers

Information sheets on identity theft, financial and health information privacy, protecting your home computer, and other privacy topics from the California Department of Justice, Privacy Enforcement and Protection Unit are available at the following link: http://oag.ca.gov/privacy/info-sheets.

Information for Everyone

Security awareness, safeguards, tips, and advisories are available at the following links.

- StaySafeOnline.org
- MS-ISAC Daily Cyber Security Tip
- MS-ISAC Cyber Security Advisories
- US-CERT Tips
- US-CERT Current Activity

Privacy Laws

State and federal privacy laws from California Department of Justice, Privacy Enforcement and Protection Unit are available at the following link: http://oag.ca.gov/privacy/privacy-laws.