Slide 1

Enterprise Information Services DAS-EIS-2021 Information Security Training

Table of contents:

Introduction
- Video Message with Transcript

Safe Computing – Threats
- Introduction
- Types of Threats
- Social Engineering Threats
- Summary
- Knowledge Check

Safe Computing Principles
- Electronic Communications
- Cloud Services
- I've Been Hacked
- Summary
- Knowledge Check

Safe Remote Computing
- Your Home Office
- Mixing Business and Personal
- Data Minimization
- Summary
- Knowledge Check

Safe Mobile Computing
- Password Best Practices
- Device Defender
- Remote Incident Reporting
- Summary
- Knowledge Check

Acknowledgement

Assessment

Slide 2

INTRODUCTION

Instructions:

Listen as Enterprise Information Services - Cyber Security Services, Chief Information Security Officer, Gary Johnson discusses the importance of Information Security to the State of Oregon. When you are finished watching the video, click **NEXT**.

Video Message with Transcript:

Hello and welcome to the DAS EIS Information Security: Foundations, annual Training.

I'm Gary Johnson, State Chief Information Security Officer at Cyber Security Services (CSS) within EIS.

While all agencies are collectively responsible for information security, the work of CSS supports and increases the collective impact and resilience of state agencies as a whole.

Information Security is a topic that is vital to our work environment but also and just as importantly, to our personal lives, our families and our communities. We encourage you to take the information gleaned from this training and use it to inform those close to you of the cyber risks they may encounter in their daily lives.

While cybersecurity has a strong focus on the technology tools we all use, it's our behavior and how we use the technology that determines the cyber security risk.

Security culture is most effective when everyone cooperates as a team to engage in good security practices as a matter of habit and routine. It is both a mindset and mode of operation.

Each time you do things, like log into your computer, check your email, use your phone or access our systems when working from home you connect to a network of assets that we depend on for our operations.

Your attention to security best practices is critical to reduce risk and keep our organization safe. Our number one defense against theft and loss is you.

Thank you for being an integral part of the state of Oregon's security team.

Slide 3

SAFE COMPUTING - THREATS

Introduction

We face a rising number of threats that could compromise the security of our information and resources. Threats and incidents may be caused by malicious attempts to steal information, but more often they are caused by simple inattention to policies and procedures. Either way, you have the power to stop most security threats.

Although the number of security threats is endless, the most common categories are:

- Loss: Misplacing a resource or device.
- Theft: Stealing information—electronically or physically—or resources.
- Cybercrime: Damaging electronic devices, files, or our organization's network.

We've developed security policies and procedures designed to help you combat these threats. Your

attention to these policies and procedures is critical to preventing actions that could lead to security breaches.

OBJECTIVES:

- Identify the types of security threats that put consumers' personal information at risk.
- Recognize the manipulative social engineering techniques that criminals use to access sensitive information.
- Identify the best methods for minimizing security risks in all forms of electronic communication.
- Identify the best practices for using cloud services.
- Identify the steps to take to regain access after you've been hacked.
- Recall the guidelines and best practices required for creating a secure home office.
- Recognize best practices that minimize the risks to sensitive data that are created when using a personal device for work activities.
- Identify ways to reduce risk to data through minimization.
- Identify the password best practices that keep our information secure.
- Identify ways to limit access to your mobile device and laptop computer while working remotely.
- Identify the need to report security incidents when working remotely.

Slide 4

SAFE COMPUTING - THREATS

Types of Threats

Your awareness and good security habits are key to stopping the nearly endless threats posed by loss, theft, and cybercrime.

Take a moment to learn more about how these threats may manifest.

Instructions: Read each scenario and answer the question.

Slide 5

SAFE COMPUTING - THREATS

EXAMPLES

CYBERCRIME

Any crime that involves a computer and a network. It can occur as a result of:

- Connecting to unsecure Wi-Fi networks.
- Neglecting to update computer software.
- Clicking links in a phishing e-mail.
- Sending sensitive or confidential information in an unencrypted e-mail.
- Opening e-mail attachments from unknown sources.
- Posting sensitive or confidential information to social networking sites.

THEFT

Theft can occur as a result of inattention to security procedures. Theft can occur as a result of:

- Leaving work resources in unlocked locations or unattended while in public places.
- Leaving work resources in briefcases, purses, clothes pockets, or on desks around the office.
- Leaving documents containing sensitive information in plain view for unauthorized individuals.
- Allowing unauthorized individuals to access our secure facilities.
- Being tricked by social engineering scams.

LOSS

Information that is transportable can be lost. Security breaches can occur as a result of losing:

- USB drives
- Laptops
- Documents
- DVDs
- Briefcases or purses
- Tablets
- Smart phones

Slide 6

SAFE COMPUTING - THREATS

Question 7: *"I'm so sick of these software updates that keep popping up on my work computer. I'll just keep clicking 'Update Later' until they go away!"*

This scenario represents which type of security risk? Loss, Theft or Cybercrime

Answer: Cybercrime can more easily affect our systems and networks when your work computer's software is out of date and unable to defend against the latest cyberattacks.

Slide 7

SAFE COMPUTING - THREATS

Question 1: "I handled sensitive consumer information yesterday while working from home ... and now the files are gone! My kid must have mixed them up with their homework and taken them to school."

This scenario represents which type of security risk? Loss, Theft or Cybercrime

Answer: Loss of important documents is a security threat that could compromise our data.

Slide 8

SAFE COMPUTING - THREATS

Question 5: *"It seems that a con artist talked their way past security this morning. The security video showed them leaving with something tucked under their arm, but we're still trying to assess what was taken."*

This scenario represents which type of security risk? Loss, Theft or Cybercrime

Answer: Theft can occur at our facilities if unauthorized individuals are allowed entry.

Slide 9

SAFE COMPUTING - THREATS

Question 6: *"I got up from my table at the café for just a minute and discovered that several important pages are missing from my business records."*

This scenario represents which type of security risk? Loss, Theft or Cybercrime

Answer: Theft of important documents is a security threat that could lead to the compromise of information.

Slide 10

SAFE COMPUTING - THREATS

Question 9: *"I've finally found an open Wi-Fi network. Time to connect with my work computer and get through some of these e-mails."*

This scenario represents which type of security risk? Loss, Theft or Cybercrime

Answer: Cybercriminals can use open Wi-Fi networks to spy on your actions, steal information from your device, or install malware which can spread to our systems or network.

Slide 11

SAFE COMPUTING - THREATS

Question 8: *"That e-mail said to click a link to verify my password, and now my computer is acting very strange. Is something wrong?"*

This scenario represents which type of security risk? Loss, Theft or Cybercrime

Answer: Cybercrime often depends on the unwitting installation of malware on our computers, which can then spread to our entire system or network.

Slide 12

SAFE COMPUTING - THREATS

Question 2: *"Drat! My files aren't on this USB drive either. I have way too many of these things and yet can't seem to find the one I need. The boss is going to be upset if that USB drive doesn't turn up soon!"*

This scenario represents which type of security risk? Loss, Theft or Cybercrime

Answer: Loss of electronic storage devices, like USB drives, is a security threat that could lead to the compromise of personal information.

Slide 13

SAFE COMPUTING - THREATS

Question 4: *"I need to talk to airport security. My work laptop was stolen out of the overhead compartment during my flight."*

This scenario represents which type of security risk? Loss, Theft or Cybercrime

Answer: Theft of devices, such as computers or mobile devices, incurs not only the expense to replace the device, but also the risk posed by compromised data.

Slide 14

SAFE COMPUTING - THREATS

Question 3: *"Oh no! I just realized that my secure entry badge must have fallen out of my pocket while I was on the train."*

This scenario represents which type of security risk? Loss, Theft or Cybercrime

Answer: Loss of organization resources, like a secure badge, is a security threat that could lead to the compromise of important personal information by giving unauthorized individuals access to our facilities.

Slide 15

SAFE COMPUTING - THREATS

Social Engineering Threats

Whether over the phone, through electronic communications, or even face to face ... social engineers are con artists that exploit our emotions to steal information.

No technological defense can truly protect us from social engineering, because you and your coworkers are the target.

It's up to you to spot the con and take the right actions to stop social engineering scams.

Introduction:

Click **SOCIAL ENGINEERING TECHNIQUES** to learn more. To begin the activity, enter your first name, then click **START**. When you are finished, click **NEXT**.

Slide 16

SAFE COMPUTING - THREATS

Social Engineering Techniques

These are examples of just some of the most common social engineering techniques. Remember that thieves may try these scams to target our organization or you personally.

Over the Phone

- Posing as a reputable service provider
- Impersonating a government or law enforcement official
- Pretending to be a customer to extract account info

In E-Mail

- Impersonating individuals of authority within our organization
- Messages threatening you with financial penalties
- Warnings of suspended accounts that require you to enter your credentials

In Person

- Individuals posing as service technicians or delivery persons hoping to enter our facility
- Pretending to be a potential client hoping to glean information from your computer screen
- A fake job interviewee assessing our organization

<u>Exploiting Emotions</u>

- Fear
- Sympathy
- Trust

Slide 17

SAFE COMPUTING - THREATS

Scenario: While doing some research for a project, you receive an alarming alert.

Uncertain of how to proceed, you call the phone number displayed...

Alert!
Virus detected.
To resolve call (555) 555-5555

To confirm your payment and allow access, please click "Accept" below.

ACCEPT

Hello, MS technical support hotline. Sorry you're experiencing this issue. Let's get you fixed up! I'll need you to navigate to the following website, confirm your payment information, and then click the "Accept" button. *This will give me access to your computer*, and I'll be able to remove the malware.
mssupport.xyz

Question: The social engineer is manipulating what emotion? Fear, Sympathy or Trust

Answer: The social engineer is exploiting you by manipulating your sense of **TRUST**. This website is a spoof of an official operating system alert. By impersonating a reputable business' technical support and posing as an authority, they might wear down your defenses to extract payment and information.

Question: What's the most professional response in this situation?

a. End the call
b. Report the incident to your manager or IT
c. Search for the error code and turn to official technical support channels

Answer: B. Whether or not you spot the scam, it's useful to report incidents like this to your manager or to IT. In general, it's best to close fake websites like this right away and to never click links you aren't sure about.

Slide 18

SAFE COMPUTING - THREATS

Scenario: You're enjoying lunch out with your coworkers.

RING *RING*

But you're pulled away by what may be an important call...

Hi, is this Jo? This is Claire from your bank's Fraud Alert team. Our systems have detected suspicious activity on your checking account. We're showing a charge for $11,750 to an unknown third party. Don't worry—we can stop this charge—but first I'll *need you to validate your identity by providing me with some account details*. Let's start with your date of birth and PIN code.

Question: The social engineer is manipulating what emotion? Fear, Sympathy or Trust

Answer: The social engineer is exploiting you by manipulating your sense of **FEAR**. Threats against finances are one of the most common ways to elicit an immediate and fearful reaction. This plays right into the scammer's ploy.

Question: What's the most professional response in this situation?

a. Ask for more information about the charges
b. Threaten the scammer and change your phone number
c. Verify the charges by calling your bank's official customer service number

Answer: C. Even if you suspect a scam, it's best to verify scenarios like this by contacting the relevant financial institution's official service number. Never divulge personal or financial information to inbound callers.

Slide 19

SAFE COMPUTING - THREATS

Scenario: You receive an e-mail from your good friend, Mary.

Unfortunately, it doesn't look like good news...

Jo, I need your help. My dog Scrapper, whom I just adopted, has just been diagnosed with a viral illness. There's no way that I can cover the expenses alone ... I've set up a charitable donation link via PayBuddy. Please help Scrapper by donating any amount you can. Thank you.

Question: The social engineer is manipulating what emotion? Fear, Sympathy or Trust

Answer: The social engineer is exploiting you by manipulating your sense of **SYMPATHY**. It's likely that your friend's e-mail address has been compromised and that scammers are sending this message to everyone in their contact list. The personal story could have been gleaned by looking at past e-mails or social media. All donations will go directly to the thieves' illicit account.

Question: What's the most professional response in this situation?

a. Contact your friend directly
b. Delete the e-mail
c. Find the real donation link directly on the payment website

Answer: A. Even if you suspect a scam, it's best to verify directly with the sender. Additionally, you can help prevent future scams by informing that individual so they can change their password and notify their contacts.

Slide 20

SAFE COMPUTING - THREATS

Scenario: On your way back from an afternoon walk, you come to our secure door to find a person you don't recognize waiting outside.

Oh, thank goodness. Could you help me with something? I'm running late for a meeting and forgot my badge. Would you mind getting the door for me?

Question: The social engineer is manipulating what emotion? Fear, Sympathy or Trust

Answer: The social engineer is exploiting you by manipulating your sense of **SYMPATHY**. It's easy to exploit our politeness when it comes to holding open doors, and everyone forgets their badge from time to time. Social engineers know this and will create any number of stories to gain access to our facility.

Slide 21

SAFE COMPUTING - THREATS

Scenario: On your way back from an afternoon walk, you come to our secure door to find a person you don't recognize waiting outside.

Oh, thank goodness. Could you help me with something? I'm running late for a meeting and forgot my badge. Would you mind getting the door for me?

Question: What's the most professional response in this situation?

a. Ask for more information about the reason for the person's visit
b. Close the door
c. Escort the individual to our reception area

Answer: C. It's always best to simply walk with the individual to the reception area so that they can sign in and be announced. Be polite, but firm in following our security policies.

Slide 22

SAFE COMPUTING - THREATS

Scenario: What a week! With Doug on vacation in Aruba, your team has been struggling to keep up with these personnel files. It doesn't help that the internet is painfully slow this time of day.

RING *RING*

A phone call brings a welcome break!

Hi, you must be Jo. This is Jerome from Acme Enterprise Solutions. I've been working with Doug on getting your servers updated. Techcast is just the slowest network, right? Ha ha! But I forgot to get some info from Doug before he left for Aruba. Jo, maybe you can help me? *I need some information about your network server*. Once you get me that info I'll boost your internet speed.

Question: The social engineer is manipulating what emotion? Fear, Sympathy or Trust

Answer: The social engineer is exploiting you by manipulating your sense of **TRUST**. Divulging this information could give the thief access to our systems and information. It's likely that this story was created by gleaning information from social media or other public sources.

Question: What's the most professional response in this situation?

a. Call Doug in Aruba for clarification
b. End the call and return to work
c. Report the call to your manager or IT

Answer: C. Whether or not you spot the scam, it's useful to report incidents like this to your manager or to IT. Never divulge information about our systems or resources to individuals if you can't verify their identity or if it's not your job to do so.

Slide 23

SAFE COMPUTING - THREATS

Scenario: You're running late for an errand after work, when your smartphone notifies you of an e-mail.

It's from your manager. Uh oh, this doesn't look good...

Strange. Your manager has never asked you to change our processes in the past.

Operations Manager MISSING INFORMATION: URGENT! Jo, we've got a problem. A prospect just reported that they're missing critical information necessary for us to get the contract. I need you to send me this information ASAP! Please share them to my cloud storage directly ... this can't wait until tomorrow. Here's the link:
httpz://real.contract.update

Question: The social engineer is manipulating what emotion? Fear, Sympathy or Trust

Answer: The social engineer is exploiting you by manipulating your sense of **FEAR**. By compromising or impersonating your manager, they hope to intimidate you into taking action without questioning their instructions. Social engineers use information about our organization, often picked out from public sources or employees oversharing on social media, to craft convincing messages.

Slide 24

SAFE COMPUTING - THREATS

Scenario: You're running late for an errand after work, when your smartphone notifies you of an e-mail.

It's from your manager. Uh oh, this doesn't look good...

Strange. Your manager has never asked you to change our processes in the past.

Operations Manager MISSING INFORMATION: URGENT! Jo, we've got a problem. A prospect just reported that they're missing critical information necessary for us to get the contract. I need you to send me this information ASAP! Please share them to my cloud storage directly ... this can't wait until tomorrow. Here's the link:
httpz://real.contract.update

Question: What's the most professional response in this situation?

a. Confirm with your manager directly
b. Contact the client or customer directly
c. Delete the e-mail

Answer: B. When it comes to important business processes, it's always best to verify unusual requests like this from the source. If something is amiss, contact the individual involved directly—not by responding to the e-mail message.

Slide 25

SAFE COMPUTING - THREATS

Summary

In this lesson, you learned that we face various computer threats that compromise the security of our information and resources. Your attention to safe computing practices is the best way to combat these threats.

Take a moment to review the key points covered.

- Be aware of varying security threats that can put our information and resources at risk.
- Social engineers use a variety of manipulation techniques to access sensitive information, usually by exploiting fear, sympathy, or trust.

Slide 26

SAFE COMPUTING - THREATS

Knowledge Check

Now it's time to check your knowledge of safe computing. Take a moment to answer the following questions.
Instructions: Read the questions and then click the best answer from the choices provided. When you are finished, click **NEXT QUESTION**. To continue, click **NEXT**.

Question: The most common categories of security threats are:

a. Access, loss, and theft
b. Access, theft, and misuse
c. Loss, theft, and cybercrime
d. Loss, theft, and misuse

Answer: C. Although the number of security threats is endless, the most common categories are loss, theft, and cybercrime.

Slide 27

SAFE COMPUTING - THREATS

Knowledge Check

Now it's time to check your knowledge of safe computing. Take a moment to answer the following questions.
Question: Which statement best describes social engineering?

a. Studying human behavior with the intent to create more collaborate workplaces.
b. Using deceptive techniques to access information.

c. Gaining notoriety on social media platforms.

Answer: B. Social engineering is the use of manipulative, deceptive techniques to access information.

Slide 28

SAFE COMPUTING PRINCIPLES

Electronic Communications

Electronic communications—such as e-mail, instant messenger, texting, and social networking services like Facebook, Twitter, and LinkedIn—make it easy to communicate. However, along with the convenience comes the risk of a security breach. Once information reaches the Internet, it is virtually impossible to recall or delete.

You are the first line of defense in ensuring the security of personal and sensitive information that we handle. Your actions have far-reaching consequences, which is why it's so important that you follow our processes when using electronic communication technologies.

Take a moment to learn how your decisions in using electronic communications help keep information secure.

Slide 29

SAFE COMPUTING PRINCIPLES

Electronic Communications

E-Mail Defender

Question: You need to send an e-mail that contains personal information to a coworker. Though they are connected to our network, they work at another worksite across the country. What action should you take?

a. Flag the e-mail as high importance.
b. Encrypt the e-mail.

Answer: B. Just because the coworker's computer is on our network, that doesn't guarantee the message will remain secure. Always encrypt e-mails that contain personal or sensitive information!

Slide 30

SAFE COMPUTING PRINCIPLES

Electronic Communications

Attachment Issues

Question: You just received a message from a coworker that includes an attached document that you were not expecting. The content seems a bit unusual. What's the best action to take?

a. Send your coworker a new e-mail asking for verification.

b. Immediately delete the message.

Answer: A. Even if you know a sender very well, always be skeptical if something seems unusual; however, this doesn't mean that you should make assumptions and delete it right away. It's best to verify with your coworker first by sending a new e-mail. Never click **Reply** to verify if the e-mail is from the sender!

Slide 31

SAFE COMPUTING PRINCIPLES

Electronic Communications

Social Experiment

Question: Your organization's new product is about to be released and you're pumped! Time for a LinkedIn post. But wait! What should you do before posting?

a. Make sure you have your facts right.
b. Confirm that the information is not sensitive, personal, or proprietary.

Answer: B. Never assume that work information is public knowledge. Never send or post any sensitive, personal, or proprietary information. Once information is released on the Internet, it is impossible to call it back.

Slide 32

SAFE COMPUTING PRINCIPLES

Electronic Communications

LOL Link

Question: You receive an e-mail from a friend with a link to a hilarious video. Who doesn't like a good laugh, but what should you do before clicking the link?

a. Verify the source of the link.
b. Use your browser's "private" mode so it doesn't cache harmful files.

Answer: A. Verify the source of any electronic communication—e-mail, instant messenger, texting, or social networking—that contains a hyperlink. Once verified, do not click the hyperlink; instead, type the URL into the Search bar. A hyperlink could initiate a dangerous download.

Slide 33

SAFE COMPUTING PRINCIPLES

Cloud Services

Cloud services and apps give us the ability to instantly share content between coworkers, customers, and vendors; but they also expose us to increased risk of data leakage or information compromise. Though we do review the security practices of approved vendors, it's always best to be cautious and

keep security in mind when exchanging any business information with external parties.

Take a moment to explore some of the potential pitfalls involved in sharing information via cloud services.

Slide 34

SAFE COMPUTING PRINCIPLES

Cloud Services

SOCIAL ENGINEERING

The following message just showed up in your CloudMax inbox, but something's phishy. What gives the message away as a social engineering attempt?

> Dave Gilbert
> TECH SUPPORT, Available
>
> Attention CloudMax user. We've detected unauthorized access to your file, FILENAME_12345.EXT. The outside user's attempt was thwarted, and the file has been locked down for your security. Unlock it by responding to this message with your ChatMax username and password. We're sorry about the inconvenience!

a. The time stamp seems out of place.
b. The message is asking for your username and password.
c. The message reference a specific file.

Answer: B. This message is using social engineering to trick you into disclosing your credentials. Be on your guard for phishing when using a cloud service, which could come disguised as a message from our organization, or from a third party using the service.

Slide 35

SAFE COMPUTING PRINCIPLES

Cloud Services

COMPLIANCE CONSIDERATIONS

A vendor asks you to use their cloud-based chat to help associate a customer's mailing address with an account number in order to complete an approved business transaction. Which of the two possible messages below is the best version to send?

a. Account#: 97564100
   Mailing Address: 742 Evergreen Terrace, Springfield

b. Name: Mikel Goodman
   SS#: 431-86-4775
   Account #: 97564100

Mailing Address: 742 Evergreen Terrace, Springfield
Credit Score: 723
Customer_Profile_97564100.pdf
103kb
Download

Answer: A. The message limits the information to those with a defined need to know. Limiting information this way ensures that we and all third parties maintain compliance with regulations concerning the use of personal or sensitive information.

Slide 36

SAFE COMPUTING PRINCIPLES

Cloud Services

CLOUD SERVICE PASSWORDS

While some cloud services utilize single sign-on (SSO) or multi-factor authentication, many require traditional passwords. When it comes to creating a password for an approved cloud service, which statement describes the best approach?

a. Use the same password for the cloud service as for your employee account.
b. Use a password that meets the minimum security requirements as required by the cloud service.
c. Use a unique password for the cloud service that is not shared with another personal or professional account.

Answer: C. Always use a unique password for your cloud services account. That way your work and personal accounts are safe in the event that our third-party cloud provider experiences a security breach.

Slide 37

SAFE COMPUTING PRINCIPLES

Cloud Services

SHADOW APPS

Select the application installed on this computer that could be a security risk if it interfaces with the business data used in our cloud service, "CloudMax." Click each application for a description of its function.

a. **InStone:** This application is installed by default on each employee's computer by IT. It gives our cloud service access to our company records, which is required for our operations.
b. **ScheduleMaster:** This third-party application is great! You've used it successfully at home for years. It automatically accesses other applications and aggregates schedule information from any account. With it, you can see information from your work e-mail, cloud service appointments, and personal contacts all in one place.

c. **Microsoft Excel:** The standard application used by all employees to organize data. Installed by default on all employees' computers. You can use it to save spreadsheets directly to our cloud service.
d. **Q2_Earnings.pdf:** This is a document you downloaded from our cloud service's message board.
e. **NetDefend:** A firewall application installed by IT on each employees' computer. It interfaces directly with our cloud service to perform security scans.

Answer: B. This application may be useful; however, if not approved by IT, it could interface with the business data stored in our cloud service. We have no way of knowing if these applications meet our organizational standards for confidential information, so always check with IT before installing any software on your work computer or mobile device!

Slide 38

SAFE COMPUTING PRINCIPLES

I've been hacked!

Even if you've taken all the recommended precautions to protect your information and your devices, you can still fall victim to hacking. If you think you've been hacked, there are several important steps you should take to ensure you can regain access to your accounts and keep hackers out!

Take a moment and learn about hacking and some techniques to regain control.

Slide 39

SAFE COMPUTING PRINCIPLES

I've been hacked!

DETERMINE HOW THEY GOT IN

Which of the following can hackers use to access your account?

a. Malware: Malicious software that can infect your computer or network
b. Phishing: Fraudulent messages sent by scammers
c. The Internet: Stealing information that you've entered on unprotected sites
d. Any of the above

Answer: D. Hackers use several techniques—including malware, phishing, social engineering, and attacking Internet sites—to access your information.

Slide 40

SAFE COMPUTING PRINCIPLES

I've been hacked!

RESET YOUR PASSWORD

The easiest step to take in regaining access to your account is to reset your password. Be sure your new password is:

a. A combination of symbols and numbers
b. Not similar to any old passwords
c. Frequently changed
d. All of the above

Answer: D. Password reuse creates liability for your computer and information. Because you've been hacked, it's more urgent that you change your password for all accounts that may have been hacked or affected.

Slide 41

SAFE COMPUTING PRINCIPLES

I've been hacked!

REVIEW YOUR RISK PROFILE

Which of the following actions make your accounts and information vulnerable to attack?

a. Updating the antivirus software on your computer
b. Using the same password for all of your accounts
c. Shutting down your computer
d. Connecting to the Internet

Answer: B. Hackers often use malware and phishing to get your information, but they also attack Internet sites and steal information from accounts where you've reused your password.

Slide 42

SAFE COMPUTING PRINCIPLES

I've been hacked!

MONITOR OTHER ACCOUNTS

Hacking puts both you *and* your contacts at risk. After an attack, you should:

a. Remove all saved contacts
b. Deactivate your social media accounts
c. Post a funny anecdote on your blog
d. Alert your contacts

Answer: D. Some hackers assume your identity and contact your friends and family to request money and maybe more. Once you've regained access, let your contacts know you've been hacked—this will put them on high alert for any suspicious activity that comes from you or your account.

Slide 43

SAFE COMPUTING PRINCIPLES

I've been hacked!

PUT YOUR ANTIVIRUS SOFTWARE TO WORK

During any attempt to regain control of your account, you should:

a. Update and run antivirus software on your computer
b. Disconnect from the Internet
c. Close all browser windows
d. Reset your network settings

Answer: A. Make sure you have a good antivirus program installed and make sure you keep it up-to-date. Regularly scanning your computer for viruses and malware will alert you to most threats.

Slide 44

SAFE COMPUTING PRINCIPLES

I've been hacked!

KNOW WHO YOU PUT AT RISK

Oftentimes the hacked account provides a path to other accounts that may be vulnerable. After an attack, which of the following should you monitor?

a. Bank accounts
b. Any sites where you make online purchases
c. Your credit
d. All of the above

Answer: D. Treat all other accounts as though they've been compromised. Monitor your bank accounts for unauthorized purchases or transfers, double check all shipping addresses and payment methods, and lock down your credit to prevent identity theft.

Slide 45

SAFE COMPUTING PRINCIPLES

I've been hacked!

LOOK FOR BACKDOORS

Once you've regained access to your accounts, check for backdoors designed to let a hacker back in. Which of the following might be a red flag?

a. Your security questions have changed
b. You have no new messages
c. Your network settings need to be reset
d. All of the above

Answer: A. Smart hackers set up tools to make sure they can access your account even after you've gotten them out. Be sure to check (and update) your e-mail rules, filters, and security questions and answers.

Slide 46

SAFE COMPUTING PRINCIPLES

Summary

In this lesson, you learned that we face various computer threats that compromise the security of our information and resources. Your attention to safe computing practices is the best way to combat these threats.

Take a moment to review the key points covered.

• Apply our electronic communications guidelines, such as encrypting e-mails and verifying the source of hyperlinks you receive, to keep both our customers' and your information secure.

• Cloud services must be used with best practices in mind, such as being on guard for phishing attempts and maintaining compliance requirements when sharing data, to prevent the compromise of sensitive information.

• If you fall victim to hacking, there are several important steps you should take to ensure you can regain access to your accounts.

Slide 47

SAFE COMPUTING PRINCIPLES

Knowledge Check

Now it's time to check your knowledge of safe computing. Take a moment to answer the following questions.

Question: You receive an e-mail from a coworker who you know very well. The e-mail includes a hyperlink for an unusual but interesting topic. What should you do?

a. Click the hyperlink because the e-mail is from someone you know very well.
b. Delete the e-mail because you do not understand why your coworker sent you the hyperlink about that topic.
c. Send a **New** e-mail to your coworker asking if she sent you the e-mail with the hyperlink.
d. Use **Reply** to respond to your coworker and ask if she sent the e-mail with the hyperlink.

Answer: C. Whenever you receive an e-mail with a suspicious hyperlink, always send a **New** e-mail to verify the authenticity of the sender. Never click **Reply** in this situation.

Slide 48

SAFE COMPUTING PRINCIPLES

Knowledge Check

Question: When it comes to cloud services, what's the most important risk to keep in mind?

a. Our information is being shared with a third party, so think twice before any communication.

b. Without an e-mail, there is no longer a "paper-trail" tracking business communication.
c. Using real-time chat features can frequently be misunderstood by the recipient.

Answer: A. Using cloud services require us to give a third-party vendor access to our confidential data. This makes your adherence to security best practices all the more essential!

Slide 49

SAFE COMPUTING PRINCIPLES

Knowledge Check

Question: Jack's e-mail account was recently hacked. Although he was able to regain access to the account quickly, what other steps should Jack take to minimize the risk of being hacked again?

a. Close all of his browser windows.
b. Update and run his antivirus software.
c. Deactivate his social media account.
d. All of the above.

Answer: B. If you suspect that an account has been hacked, it is always a good idea to make sure you have a good antivirus program installed and make sure you keep it up-to-date. Regularly scanning your computer for viruses and malware will alert you to most threats.

Slide 50

SAFE REMOTE COMPUTING

Your Home Office

Working from home has some great advantages. You can skip the commute, avoid office distractions, and stay in your pajamas; however, it can also expose our company information to increased risk because your home office doesn't benefit from the numerous electronic and physical security controls of our corporate location. We trust you to be productive when working at home, and also trust you to think carefully about making your home office as secure as possible.

Slide 51

SAFE REMOTE COMPUTING

Your Home Office

Working from home has some great advantages. You can skip the commute, avoid office distractions, and stay in your pajamas; however, it can also expose our company information to increased risk because your home office doesn't benefit from the numerous electronic and physical security controls of our corporate location. We trust you to be productive when working at home, and also trust you to think carefully about making your home office as secure as possible.

SECURE YOUR HOME

Take common-sense measures to ensure that your home is secure from unauthorized entry.

- Lock your doors and windows before leaving.
- Do not leave your computer or other valuable equipment in plain sight.
- Place work devices in a concealed and preferably locked location when not in use.
- Do not post your status as working from home on social media accounts.
- Engage in voice conversations where others cannot overhear.

Slide 52

SAFE REMOTE COMPUTING

Your Home Office

Working from home has some great advantages. You can skip the commute, avoid office distractions, and stay in your pajamas; however, it can also expose our company information to increased risk because your home office doesn't benefit from the numerous electronic and physical security controls of our corporate location. We trust you to be productive when working at home, and also trust you to think carefully about making your home office as secure as possible.

HOME LIFE

Whenever possible, distance your work duties from domestic responsibilities.

- Do not allow children, your spouse, or even your cat to touch your work devices.
- While working, limit other devices, such as various "smart" appliances or other computers, from connecting to your home network.
- Do not leave important company documents where they could be accidentally thrown away or damaged.
- Use a cross-cut shredder to dispose of any documents that contain sensitive information—never your family garbage can.
- Do not insert personal peripheral devices, like USB drives, smartphones, cameras, or other gadgets into your company computer.

Slide 53

SAFE REMOTE COMPUTING

Your Home Office

Working from home has some great advantages. You can skip the commute, avoid office distractions, and stay in your pajamas; however, it can also expose our company information to increased risk because your home office doesn't benefit from the numerous electronic and physical security controls of our corporate location. We trust you to be productive when working at home, and also trust you to think carefully about making your home office as secure as possible.

PROTECT YOUR ROUTER

Take the time to configure your home router's settings to maximize security.

- Change the administrative password from the manufacturer's default.

- Turn off SSID broadcast to limit who can detect your network.
- Use WPA2 or better encryption.
- Turn on MAC filtering so that only specified devices can connect to the router.
- Disable remote management features, if available.
- Regularly check for updates to the router's firmware.

Slide 54

SAFE REMOTE COMPUTING

Your Home Office

Working from home has some great advantages. You can skip the commute, avoid office distractions, and stay in your pajamas; however, it can also expose our company information to increased risk because your home office doesn't benefit from the numerous electronic and physical security controls of our corporate location. We trust you to be productive when working at home, and also trust you to think carefully about making your home office as secure as possible.

FOLLOW OUR ORGANIZATION'S CONTROLS

Treat your work computer with the same level of security consciousness when at home as you are expected to when at work.

- Use a password and lock your computer's screen when away.
- Access only the information you need to complete the work for which you are currently responsible.
- Keep antivirus and firewall software up to date and running.
- Use a VPN to connect to our network.
- Save files to our designated cloud server.
- Encrypt files and messages when appropriate.

Slide 55

SAFE REMOTE COMPUTING

MIXING BUSINESS AND PERSONAL

When you use your personal device for both work and personal activities, it's important to ensure that your personal use doesn't compromise our business information. Inappropriate use of your device—like ignoring our security procedures—turns it into a skeleton key for data thieves. Without the proper security controls, your mobile device can be used by cyber-criminals to access both your personal information and our proprietary data.

To learn more about safely using your mobile device for work responsibilities, click each **IMAGE**. When you are finished, click **NEXT**.

Slide 56

SAFE REMOTE COMPUTING

MIXING BUSINESS AND PERSONAL

ACCOUNTS

Modern web services have no shortage of accounts that require sign-in. Keep the following best practices in mind:

- Never use your personal username and password as the credentials for a professional account, and vice versa.
- Never use your personal device for business use.

Slide 57

SAFE REMOTE COMPUTING

MIXING BUSINESS AND PERSONAL

CLOUD STORAGE

Remote storage is a great way to extend the space on your device or back up your data; however, keep the following practices in mind before you start using a cloud service:

- Never backup our organization's information to unapproved cloud-based services, such as Dropbox, Google Drive, or iCloud.
- Never use our organization's cloud-based service to store and/or backup your personal information.

Remember: backing up your personal data is exclusively your responsibility. If your device is lost or compromised, you must report it immediately. IT will remotely wipe your device and information that has not been backed up may be lost.

Slide 58

SAFE REMOTE COMPUTING

MIXING BUSINESS AND PERSONAL

APPS

There may be an app for just about everything, but that doesn't mean you should use the same app for both personal and work purposes. For example:

- Refrain from downloading apps that have not been approved by IT.
- Use different apps for work e-mail and personal e-mail.

Check with IT to see if third party applications can be implemented to further isolate our organization's data from your day-to-day use of the device.

Slide 59

SAFE REMOTE COMPUTING

Data Minimization

Data minimization is all about reducing risk to the information we handle. This means thinking carefully about collecting, accessing, and retaining the least amount of data necessary. Keep an eye out for opportunities to minimize data exposure, and help your coworkers do the same.

To begin, click **START**. Read each scenario and identify whether the actions taken by your coworkers are **SAFE** or **RISKY**. When you are finished, click **NEXT**.

Slide 60

SAFE REMOTE COMPUTING

Data Minimization

SAFE or RISKY?

I just discovered our office copier's "memory" feature. It automatically caches a copy of each document scanned so it can be easily pulled up for later use. I will use this feature on my next project to save me time!

Slide 61

Answer: Risky - Cached data might keep copies without our knowledge. Be aware of hidden places that sensitive data might reside in our systems, devices, or facilities. When it comes to sensitive data, out of sight should never be out of mind!

Slide 62

SAFE REMOTE COMPUTING

SAFE or RISKY?

My computer desktop looks chaotic with old files, but I've got a system to stay organized. If you need to look up financial records from the past 5 years—I'm your guy!

Slide 63

Answer: Risky - Devices should never have too much information saved to their local storage. If the device is compromised, that data is immediately at risk. Delete unnecessary information as soon as it's appropriate to do so.

Slide 64

SAFE REMOTE COMPUTING

SAFE or RISKY?

I routinely receive alerts that contain patient healthcare information. After I read them, I always delete the messages from my phone's e-mail app.

Slide 65

Answer: Safe - Devices should never have too much information saved to their local storage. If the device is compromised, that data is immediately at risk. Delete unnecessary information as soon as it's appropriate to do so.

Slide 66

SAFE REMOTE COMPUTING

SAFE or RISKY?

Our new mobile app is working great! In fact, it's collecting more data than we know what to do with right now. We'll be ready when it comes time to add new features.

Slide 67

Answer: Risky - Always consider what personal data is necessary to collect, and never collect more. Collecting now with the intent of using later is a serious breach of many privacy regulations.

Slide 68

SAFE REMOTE COMPUTING

SAFE or RISKY?

I take down customer payment data all the time. So much in fact that I make it a habit to clear my browser's history at the end of each day to ensure it's not retaining information without my knowledge.

Slide 69

Answer: Safe - Cached data might keep copies without our knowledge. Be aware of hidden places that sensitive data might reside in our systems, devices, or facilities. When it comes to sensitive data, out of sight should never be out of mind!

Questions are random and could also include any of the following:

SAFE REMOTE COMPUTING

SAFE or RISKY

My coworker asked me for a copy of an upcoming report. Rather than e-mailing her a duplicate, I pointed her towards the location of the shared file saved in our cloud.

Answer: SAFE - Think carefully each time you duplicate data. The more copies that exist, the more that data becomes at risk.

SAFE or RISKY?

Looks like my team just published research data to our cloud storage. I'll save a local copy on my computer just in case.

Answer: Risky - Think carefully each time you duplicate data. The more copies that exist, the more that data becomes at risk for accidental exposure, loss, or theft.

SAFE or RISKY?

I clarify with my team what information is safe for them to access with their administrator credentials, and what information access is off-limits.

Answer: Safe - Each employee should have access to the minimum amount of information necessary to complete their jobs. If you notice that you or another employee has more access than they need, report it to IT right away.

SAFE or RISKY?

It turns out that my credentials give me access to our HR system. I won't cause any mischief, but since I'm here, I'll take a peek at that new person's salary.

Answer: Risky - Each employee should have access to the minimum amount of information necessary to complete their jobs. If you notice that you or another employee has more access than they need, report it to IT right away.

SAFE or RISKY?

We're about to launch our next marketing survey. We had numerous discussions about how much information we needed to collect from customers. In the end I think we got it down to the bare minimum.

Answer: Safe, Collecting now with the intent of using later is a serious breach of many privacy regulations. Always consider what personal data is necessary to collect, and never collect more.

Slide 70

SAFE REMOTE COMPUTING

Summary

Security threats—actions that put our information at risk—can be caused by malicious activity, but are more often caused by inattention to policies and procedures. Our policies and procedures are designed to protect our information, our resources, and our reputation, but they only work if we all follow them.

Remember, you are our best defense against information theft and loss, so be sure you know and follow our policies and procedures. Now, take a moment to review the key points covered.

- If working from home, you must take steps to ensure that your office is secure.
- You can reduce risk posed to sensitive data by minimizing the amount of data you collect, access, and retain.

Slide 71

SAFE REMOTE COMPUTING

KNOWLEDGE CHECK

Now it's time to check your knowledge of safe computing. Take a moment to answer the following questions.

1. Which are security risks when working from a home office?
    a. Theft of company equipment.
    b. Accidental destruction of documents.
    c. Network security.
    d. All of the above.

Answer: D. Your home office doesn't benefit from the numerous electronic and physical security features of our work location.

Slide 72

SAFE REMOTE COMPUTING

KNOWLEDGE CHECK

2. Options for keeping work and personal activities separate when using one device include using
    a. Different apps for work and personal e-mail.
    b. Third-party apps installed by IT to isolate our organization's data.
    c. Different user profiles for personal and business.
    d. All of the above.

Answer: D. Without the proper security controls, your mobile device can be used by cyber-criminals to access both your personal information and our organization's data.

Knowledge check could also include the following:

3. What's the best keyword to remember when it comes to reducing risks to sensitive data?
    a. Deletion
    b. Minimization
    c. Nominal

Answer: B. Keep the word "minimization" in mind and you can help reduce risk to sensitive information. Always collect, access, and retain the least amount of information necessary.

Slide 73

SAFE MOBILE COMPUTING

Password Best Practices

So you've created a strong password? Well, password security doesn't stop there! Every day you and your coworkers make password-related decisions that either keep your password safe, or put it—and our data—at risk.

Slide 74

SAFE MOBILE COMPUTING

HINT

PASSWORD BEST PRACTICES

- Don't use the same passwords for work and home accounts. Variety is better.
- Never share your password.
- If you suspect your password has been compromised, change it immediately.
- Don't write down your passwords or store them electronically.
- Use a password manager if available.
- Set your devices to unlock only by entering a password or PIN.

Slide 75

SAFE MOBILE COMPUTING

"My personal e-mail account was just hacked. I don't understand how. The password is the same secure password I use for work!"

What should your coworker do?

a. Change her personal e-mail account password
b. Change her work account password
c. Change the password to each of her accounts

Answer: C. If your password has been compromised at any point it's essential that you change it right away. As an added precaution, if you use the same password at home and at work, notify IT if your personal account is compromised.

Slide 76

SAFE MOBILE COMPUTING

"This facial recognition technology is amazing, much faster than entering my password every time I need to check a message."

Yes

No

Answer: No, Alternative methods for securing devices, like facial recognition and thumb print scans, are not as secure as using a lengthy password or PIN. In fact, these methods can be thwarted by skilled criminals.

Slide 77

SAFE MOBILE COMPUTING

"I try hard to create new passwords for each account, but it's getting tough to remember them all!"

What would you suggest to your coworker?

a. Try an approved password manager tool
b. Use a single, highly complex password
c. Keep track of your passwords in a notebook

Answer: A. Password managers keep track of the passwords for your various accounts, allowing you to maximize length, complexity, and diversity across accounts without worrying about remembering each password. Many are available for free and can be used on computers and mobile devices.

Slide 78

SAFE MOBILE COMPUTING

"Thanks for showing me how to use this system. Let me just type my password into my phone's note-taking app so I don't forget."

What would you say?

a. Great idea!
b. Save that password to your cloud storage.
c. Keep that password in your memory only.

Answer: C. Writing down passwords, or storing them electronically, makes them much more vulnerable. If your password is so complex that you can't remember it, consider using an easy-to-recall passphrase.

Slide 79

SAFE MOBILE COMPUTING

"Dude, I got locked out ... again. Let me borrow your password to get logged in real quick."

Will you share your password with him?

Yes

No

Answer: No, Never share your password with another coworker, even if that person is your manager or a member of our IT team. Your password is yours alone. Forgotten passwords or locked accounts should be reset by IT.

Slide 80

SAFE MOBILE COMPUTING

Device Defender

Do you have what it takes to defend your work devices—and the sensitive information they access? Test your knowledge by playing "Device Defender." This game asks you to decide if certain actions related to working remotely are safe or risky. Make the best decisions to raise your device's protection; make too many mistakes, and the cyber crooks will break through and compromise our data. Good luck!

Click **START** to begin. For each security topic, determine which actions are **SAFE** or **RISKY**. When you're ready, click **ACTIVATE DEFENSES** to see how you did. Make three mistakes and its game over!

Slide 81-2

SAFE MOBILE COMPUTING

Device Defender

Actions: Safe/Risky

TOPIC: PASSWORDS

1. Set a screen lock for your smartphone that uses the same password as your laptop.
    a. RISKY, Use a unique password for each device.
2. Conceal passwords as contacts in a smartphone's address book for easy recall later.
    a. RISKY, Never document a password, especially not somewhere on or near your devices.
3. Use two-factor authentication whenever it's available.
    a. SAFE, Two-factor authentication is a great way to create an additional layer of defense to control access to your devices.

Slide 83-4

SAFE MOBILE COMPUTING

Device Defender

Actions: Safe/Risky

TOPIC: MONITORING YOUR DEVICE

1. Keep your device nearby at all times.
    a. SAFE, You should never be far from your device. Keep it on you as much as possible.
2. Hire a qualified repair person to service your device should it break while working remotely.
    a. RISKY, Allow only our IT department to facilitate repairs.
3. Allow others, such as clients, vendors, or coworkers from other sites to access your device.
    a. RISKY, Never let another person access your device, even when under your supervision.

Slide 85-6

SAFE MOBILE COMPUTING

Device Defender

Actions: Safe/Risky

TOPIC: PROTECTING INFORMATION

1. Use cached information to recall passwords and other information.
    a. RISKY, Clear your device's application caches and adjust settings so that they do not remember information like passwords and usernames.
2. Implement your device's built-in data encryption.

    a. SAFE, Encryption should be implemented to protect data saved to your device. Check with IT for more information on implementing this feature.
3. Back up both personal and work information as appropriate.
    a. SAFE, Regularly back up information to the appropriate locations. Do not use work storage to back up personal information, and vice versa. Check with IT for more information on how to perform a backup.

Slide 87-8

SAFE MOBILE COMPUTING

Device Defender

Actions: Safe/Risky

TOPIC: APPLICATION ACCESS AND PERMISSIONS

1. Carefully consider app permissions before installing.
    a. SAFE, Smart phone apps display what information that app is allowed to access. Disable or refrain from downloading apps that seem to access more information than is required.
2. Download third-party applications to your device prior to gaining confirmation from IT.
    a. RISKY, We have no way of knowing if third-party applications meet our organizational standards for confidential information, so always check with IT before installing any software on your work computer or mobile device!
3. Monitor applications that may be using system resources or mobile data in the background without your knowledge.
    a. SAFE, Malicious apps may be using your system resources or mobile data. Most devices have tools that allow you to easily view this information.

Slide 89

SAFE MOBILE COMPUTING

Remote Incident Reporting

When you're working remotely, you're even more vulnerable than usual to cybercrime. If you notice something unusual or even if you only suspect that an incident has occurred, it's vital that you contact our IT department right away.

Read each statement and answer the question; then click **NEXT QUESTION**. To see examples of incidents, click **HINT**. When you are finished, click **NEXT**.

Slide 90

HINT

WHAT IS AN INCIDENT?

An incident is any actual or potential compromise of our organization’s information or devices.

Common examples include:

- Stolen laptop or mobile device.
- Unauthorized access to your hotel room, home office, or home network.
- Erratic behavior of laptop or mobile devices.
- Sensitive information overheard during a private conversation by an unauthorized individual.
- Sending or receiving information over an unsecure network.

Slide 91

SAFE MOBILE COMPUTING

Remote Incident Reporting

> *Did I seriously just delete that e-mail? Whose idea was it to make this phone's "delete" icon look like that!*
> Should this be reported to IT?
> Yes
> No

Answer: No, A simple mistake, like accidentally deleting an e-mail, doesn't require immediate reporting to IT as a security incident.

Slide 92

SAFE MOBILE COMPUTING

Remote Incident Reporting

> *I just finished up a day at the convention and need to send an update to my manager. I'll use a VPN to connect back to my organization's network.*
> Should this be reported to IT?
> Yes
> No

Answer: No, Using a VPN is the safest way to connect to networks outside of our own, so informing IT of their implementation is not necessary.

Slide 93

SAFE MOBILE COMPUTING

Remote Incident Reporting

> *Hmmm ... I don't remember downloading this app. Come to think of it, I've been seeing some other strange pop-ups lately, too. Where are these coming from?*
> Should this be reported to IT?
> Yes
> No

Answer: Yes, Mysterious apps, processes, or pop-ups showing up on your device are an indicator of malware, which should be reported to IT immediately.

Slide 94

SAFE MOBILE COMPUTING

Remote Incident Reporting

> *I can't believe I almost lost my smart phone in the airport! It's a good thing that the airline staff was able to find it, even if it took a few hours. Now to make sure I didn't miss any important work e-mails!*
> Should this be reported to IT?
> Yes
> No

Answer: Yes, A lost device that possesses work information should be reported to IT right away, even if it is later recovered.

Slide 95

SAFE MOBILE COMPUTING

Remote Incident Reporting

> *I think my home Internet is broken. Ever since I downloaded those files from my e-mail it feels like my whole network has shut down. How am I supposed to get any work done?*
> Should this be reported to IT?
> Yes
> No

Answer: Yes, Changes in your home network's performance may not be a security incident, but if it affects your work device, it should still be reported, especially if you can trace the change to actions taken while using your work device.

Slide 96

SAFE MOBILE COMPUTING

SUMMARY

In this lesson, you learned that we face various computer threats that compromise the security of our information and resources. Your attention to safe computing practices is the best way to combat these threats.

Take a moment to review the key points covered.

- Follow password best practices to keep our organization's information secure.
- You are responsible for limiting access to your mobile devices and laptop computer while working remotely.

- Security incidents, actual or suspected, that are encountered while working remotely must be reported immediately.

Slide 97

SAFE MOBILE COMPUTING

Knowledge Check

Now it's time to check your knowledge. Take a moment to answer the following questions.

Read the questions and then click the best answer from the choices provided. When you are finished, click **NEXT QUESTION**. To continue, click **NEXT**.

Questions

Which of the following is a password best practice?

a. Documenting your passwords in a secret document in your personal cloud storage.
b. Setting your screensaver to unlock with a password.
c. Using a short password such as the name of your pet so you can remember it.

Answer: B. Setting your screensaver to unlock with a password is a password best practice.

Slide 98

SAFE MOBILE COMPUTING

Knowledge Check

Now it's time to check your knowledge. Take a moment to answer the following questions.

When working remotely, the first line of defense in protecting your devices is

a. Information Technology (IT)
b. You
c. Third-party software

Answer: B. While working remotely, your first line of defense is to ensure that you, and only you, can access the information stored on your devices.

Slide 99

ACKNOWLEDGMENT

Now that you have completed the course, you must check the box below to acknowledge that you have read, understood, and will comply with the material covered in this training.

I acknowledge that I will comply with the material covered in this training, including all related policies and procedures.

To confirm course completion, click the **CHECK BOX**, and then return to the **MENU** and click **ASSESSMENT**.

Slide 100

RESOURCES

Cloud and Hosted Systems Policy with Exhibit

PURPOSE: This policy establishes standards to ensure that state agencies:

- Appropriately analyze and document the benefits, costs, and risks to the state before contracting for a Cloud or Hosted Service.
- Assess the readiness of a Cloud or Hosted Service Provider to deliver a solution that meets the state's requirements.
- Conduct planning to ensure that state information and financial assets are appropriately protected when adopting a Cloud or Hosted Service.

APPLICABILITY: This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division, or office within the Oregon Executive Branch. The following agencies and boards are excluded:

- Secretary of State.
- State Treasurer.
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery.
- State Board of Higher Education or any public university listed in ORS 352.002.

FORM(S), EXHIBIT(S) & INSTRUCTIONS: These governing statutes, policies and rules must be reviewed prior to contracting for a Cloud or Hosted Service:

- Information Technology Investment Oversight Policy: 107-004-130.
- Information Security Policy: 107-004-052.
- Information Security Incident Response Policy: 107-004-120.
- Information Asset Classification Policy: 107-004-050.
- Cloud and Hosted Systems Procedure: 107-004-150_PR.
- ORS 291.047; 192.005; 192.311 to 192.478; and 279A.157.
- ORS 165.800; and 646A.600 to 646A.628.
- ORS 276A.300; and OAR 125-800-0005 to 125-800-0020.
- SB 1538 (Chapter 110, 2016 Laws).

Exhibit A attached, Cloud and Hosted Systems Workbook Guide supports the Cloud or Hosted Service purchasing process. Fillable form available at: https://www.oregon.gov/das/Policies/107-004150_PR_Attachment.docx .

DEFINITIONS

- "Cloud or Hosted Service": an Internet-based computing solution that provides shared processing resources, applications and access data on demand, made available to state agencies through various contracting models.
- "Cloud or Hosted Service Provider" or simply "Provider": the entity providing a Cloud or Hosted Service.
- "Service Contract": all of the documents that comprise a contract for a Cloud or Hosted Service between a Cloud or Hosted Service Provider and an agency.
- "Information Asset Classification Level": the classification of information by value, criticality, sensitivity, and legal implications to protect the information through its life cycle. Classification Levels are defined in DAS Policy 107-004-050 and referred to in statewide information security standards.
- "Public Record": has the meanings established in ORS 192.005 and ORS 192.311. In general it refers to information that is prepared, owned, used or retained by a state agency; relates to an activity, transaction or function of a state agency; and is necessary to satisfy the fiscal, legal, administrative or historical policies, requirements or needs of the state agency. It includes any writing that contains information relating to the conduct of the public's business, including but not limited to court records, mortgages, and deed records, prepared, owned, used or retained by a public body regardless of physical form or characteristics.

EXCLUSIONS AND SPECIAL EXCEPTIONS: Request exclusions to this policy by email to the Office of the State CIO (ITInvestment.Review@oregon.gov). The request should state the policy section and the exact wording to which the exclusion would apply if approved. State the limitations of the exclusion and the reasons why it is necessary and beneficial in the situation. The State CIO or designee will reply in writing with approval, denial, or limitations to the exclusion.

GENERAL INFORMATION

Strategic Considerations:

(1) The choice of a Cloud or Hosted System over an agency-managed system can have substantial, long-term impact on agency and enterprise capabilities, business processes and investments. Agencies should carefully consider the strategic implications of this sourcing decision, including how it will affect the organizational capabilities of the agency; whether the service is likely to serve the agency's long-term goals, and how the service and data will integrate with other state services and data to support service delivery and ongoing innovation.

(2) Cloud or Hosted Systems and Services may present limitations or challenges for integrating data or services with other agency, state or partner data or services. Agencies should consider how future business needs may create demands for data and service integration, and how these demands will be

met. Contractual terms may be helpful in ensuring that data and services are available for integration, for example through documented and supported Application Programming Interfaces (APIs).

Requirements:

(1) The selection and use of Cloud or Hosted Systems and Services must comply with all applicable laws, policies, procedures and standards including without limitation: privacy laws and regulations, statewide and agency-specific IT security policies and standards, internal audit controls, risk management standards, records management standards, and applicable DAS policies and procedures.

(2) Before contracting for a Cloud or Hosted Service, the agency must complete the planning and preparation necessary to appropriately manage the associated risks. Planning should be started as soon as a Cloud or Hosted Service is considered, and must be carried out with diligence and rigor appropriate to the size, business impact and risk of the proposed solution. Details of required documentation and timing are provided in the Cloud and Hosted Systems Procedure.

Use the Cloud and Hosted Systems Workbook (form), published by the State CIO, to document the results of this planning. The completed, signed workbook must be retained as part of the procurement file and submitted with supporting documentation as required by this policy and its associated procedure when seeking approval from the State CIO. When required, such approval must be obtained before continuing with the initiative.

The following risk areas must be addressed:

(a) Confidentiality, availability and integrity: Agencies must develop information security plans and Service Contract terms to protect information to all applicable standards. Among other guidance, the following apply to every information technology initiative:

- Information Security Policy: 107-004-052, which requires agencies to develop and implement information security plans, policies and procedures to protect their information.
- Statewide Information Security Standards, which the Enterprise Security Office (ESO) publishes and maintains as minimum standards for protecting information.

(b) Business continuity and disaster recovery: Agencies must document their business continuity (BC) and disaster recovery (DR) needs, and must develop plans and Service Contract terms to meet those needs. The impact of this IT investment must be reflected in the agency's BC/DR plan.

(c) Exit planning: Agencies must develop plans for both anticipated exit from the Cloud or Hosted Service (such as at the end of the Service Contract term) and unanticipated exit (in case the Provider becomes unwilling or unable to provide the Service).

(d) Service management: Agencies must document their required service levels and metrics and ensure that they are appropriately represented in the Service Contract.

(e) Incident management: ESO (Security Operation Center) will assist agencies in the development of security incident response plans and Service Contract terms that meet their needs for incident monitoring, notification and response. At a minimum, the following applies to every Cloud or Hosted Service:

• Information Security Incident Response Policy: 107-004-120 which requires agencies to establish capabilities to respond to information security incidents and requires the timely reporting of certain incidents.

(f) Data ownership and rights: Agencies must document their requirements in regards to data and metadata ownership and rights and ensure that those rights are appropriately secured and allocated in the Service Contract.

(g) Data retention and destruction: Agencies must document the retention and destruction schedules that apply to the information stored in the Cloud or Hosted System, and the required ability to retrieve records as needed. Agencies must develop plans and Service Contract terms to meet these needs and to ensure the ability to comply with Oregon Public Records laws and with all other applicable federal and state statutes, rules, and policies.

• The State Archivist is responsible for the management of public records from creation until final disposition. Agencies are required to develop policies for public records management that define the use, retention and ownership of public records and to obtain approval of those policies from the State Archivist.

(h) Audits and Controls: Agencies must determine how they will ascertain that the Provider has appropriate controls in place to meet agency needs as described in sections A-G above, and to comply with applicable legal, regulatory, and contractual commitments. Each Service Contract must include terms ensuring that appropriate audits are carried out and reports are made available, and that Provider cooperation is appropriately secured for audits by or on behalf of the agency.

(3) If the Cloud or Hosted Service meets or exceeds any of the triggering risk thresholds described below, the agency must obtain approval from the State CIO before contracting for the Cloud or Hosted Service. This approval is required in addition to any other oversight that the State CIO may impose, such as through the Stage Gate or Non-Stage Gate oversight processes. Agencies must submit proposals for oversight if any one or more of the following risk thresholds apply to the proposed Cloud or Hosted System or Service:

• It will store, process, or transmit data of Information Asset Classification Level 3 (Restricted; reference Policy 107-004-050) or higher, or information for which special protection standards apply by law or contract.

• It will be the authoritative source for information that is difficult, expensive, or infeasible to replace or recreate.

• A sustained interruption of the Service would have a significant impact on agency operations and/or those served by the agency.

(4) Agencies must also follow the IT Investment Oversight Policy: 107-004-130.

(5) Service Contracts must include terms and conditions required by the Attorney General in order for the contract to be approved for legal sufficiency according to ORS 291.047. Service Contracts must use available forms and templates developed by DAS and the Department of Justice according to ORS 279A.

(6) Service Contracts must require the contractor to carry insurance appropriate for the proposed transaction, as informed by the tools and guidance provided by DAS Risk Management.

Guide

Cloud and Hosted Systems Workbook Guide Exhibit A

Version 2.0 Date: 25 APRIL 2019 For the latest version, visit:
https://www.oregon.gov/das/OSCIO/Pages/OSCIO-templates-and-forms.aspx

For additional information, please contact: Your Senior IT Portfolio Manager, or
ITinvestment.Review@oregon.gov Enterprise IT Governance office

Cloud and Hosted Systems Workbook Guide Office of the State CIO

V2.0 1 of 21 4/25/2019

Table of Contents

Introduction..... 2
How to use this guide 2
General Information 3
Work Reduction and Reusability 4
OSCIO-approved boilerplate language..... 4

Re-use of completed workbooks..... 4
Fast-Lane Renewals..... 4
First-time review of existing contracts 4
Question-by-question guidance 5
Guidance on Section A: Risk FACTORS Determination 6
Guidance on Section B Sub-Section 1: Requirements 12
Guidance on Section B Sub-Section 2: Contract and related planning 16
Guidance on Section C: (Renewal/Reuse) 20
Document revision history 22

Cloud and Hosted Systems Procedure

PURPOSE: This cloud computing procedure describes how agencies must show that they have exercised due diligence in the consideration and acquisition of cloud technology and services.

APPLICABILITY: This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division, or office within the Oregon Executive Branch. The following agencies and boards are excluded:

Secretary of State. State Treasurer. The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice. Oregon State Lottery. State Board of Higher Education or any public university listed in ORS 352.002.

FORM(S), EXHIBIT(S) & INSTRUCTIONS

Cloud and Hosted Systems Policy: 107-004-150. Information Technology Investment Oversight Policy: 107-004-130. Cloud and Hosted Systems Workbook Guide, Exhibit A to Policy: 107-004-150. Cloud and Hosted Systems Workbook (form)

DEFINITIONS Refer to the Cloud Computing Policy: 107-004-150.

PROCEDURE: FIRST-TIME APPROVAL An agency must complete the actions in this procedure before contracting for a Cloud or Hosted Service, or as required during the Stage Gate process. Agencies are encouraged to engage with the Office of the State Chief Information Officer (OSCIO) through their assigned Senior IT Portfolio Manager early in the planning process. SIPM contact information is available on the State CIO web site, https://www.oregon.gov/das/cio .

RESPONSIBILITY STEP ACTION Agency project manager

(1) As soon as a Cloud or Hosted System is under consideration, complete Section A: "Risk Determination" of the Cloud and Hosted Systems Workbook to determine if the proposed investment entails significant risk.

Approving Business Owner and Approving Technology Manager

(2) Review and sign the completed Section A of the Workbook. Agency CIO (or executive responsible for IT)

(3) Low risk: If completion of Section A of the Workbook indicates that the investment is low risk, submit Section A of the Workbook to the State CIO through the PPM tool and retain a copy with the agency's procurement file. This completes the process for low-risk investments.

Significant risk: If the agency determines that the investment entails significant risk, continue to Step 4.

Agency project manager, ESO BISO

(4) Before releasing a procurement document or selecting a solution, complete Section B, Sub-Section 1: "Requirements" of the Workbook.

Approving Business Owner, Approving Technology Manager and ESO BISO

(5) Review and sign the completed Section B, Sub-Section 1 of the Workbook.

Agency project manager

(6) If the investment is under Stage Gate or Non-Stage Gate oversight per the IT Investment Oversight Policy: 107-004-130, submit the Section A and Section B, Sub-Section 1 of the Workbook to OSCIO through the PPM tool, and obtain approval before continuing.

If the investment is not under Stage Gate or Non-Stage Gate oversight, yet procurement approval is needed, submit Section A and Section B, Sub-Section 1 of the Workbook to OSCIO by email to ITInvestment.Review@oregon.gov and obtain approval before continuing.

If neither of the above conditions apply, continue with Step 8.

State CIO

(7) As necessary, review submissions, update project checklist and provide written documentation of oversight approval, conditional approval, or rejection. Agency project manager

(8) Before the agency commits to a particular Cloud or Hosted System or Service (i.e. before signing a Service Contract, purchase order or other binding document), complete Section B, Sub-Section 2: "Contract and Related Planning" of the Workbook. Approving Business Owner, Approving Technology Manager and ESO BISO

(9) Review and sign the completed Section B, Sub-Section 2 of the Workbook.

Agency project manager

(10) If the investment is under Stage Gate or Non-Stage Gate oversight per the IT Investment Oversight Policy: 107-004-130, submit Section B, Sub-Section 2 of the Workbook to OSCIO through the PPM tool, and obtain approval before continuing. Section A and Section B, Sub-Section 1 of the Workbook need not be resubmitted if they were previously approved; otherwise include them with this submission.

If the investment is not under Stage Gate or Non-Stage Gate oversight submit Section B, Sub-Section 2 of the Workbook to OSCIO by email to ITInvestment.Review@oregon.gov and obtain approval before continuing. Section A and Section B, Sub-Section 1 of the Workbook need not be resubmitted if they were previously approved; otherwise include them with this submission.

State CIO

(11) As necessary, review submissions, update project checklist and provide written documentation of oversight approval, conditional approval, or rejection. Agency project manager 12 Submit the completed, signed Cloud and Hosted Systems Workbook to OSCIO and the agency's designated procurement office via email. Procurement office 13 Ensure that the approved Cloud and Hosted Systems Workbook is retained as part of the procurement file.

Controlling Portable and Removable Storage Devices Policy

https://www.oregon.gov/das/Policies/107-004-051.pdf

Purpose: The purpose of this policy is to ensure the confidentiality, integrity, and availability of state information assets stored on portable or removable storage devices. Security controls are necessary to protect against theft of equipment, unauthorized disclosure of information, misuse of equipment, or unauthorized access to information assets.

Policy: Each agency will physically control and protect portable and removable storage devices, and protect and manage any sensitive information stored on them.

Controlling Portable and Removable Devices

Portable and removable storage devices may include, but are not limited to palmtops, laptops, mobile phones, flash drives, floppy diskettes, CDs, or DVDs.

Due to the portability of these devices, care needs to be taken to ensure the physical security of the device to prevent potential compromise through loss or theft of the device. To properly manage portable or removable storage devices agencies must know what devices they have, where they are, who has them, how they are being used, and what information is stored on them.

Each agency will adopt policy and procedures identifying types of approved devices, govern use of personally-owned devices, and establish methods for tracking the devices.

Securing Information Stored on Portable and Removable Devices

Each agency will adopt policies and procedures identifying what agency information assets may or may not be stored on portable or removable devices and approved methods for securing that information, as needed, appropriate to the information's sensitivity.

Compliance

Each agency may, based upon its individual business needs or legal requirements, exceed the security requirements put forth in this document but must, at a minimum, achieve the security objectives defined in this document.

State agencies have one (1) year from effective date of this policy to comply with this policy.

Authority:

This policy is established under the authority of 2005 Oregon Laws Chapter 739, OAR 125-800-005, 125-800-0010 and 125-800-0020.

Applicability:

This policy applies to all Executive Branch agencies as defined in ORS 17 4.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b) and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

Attachments: None

Definitions:

Asset: Anything that has value to the organization.

Availability: The reliability and accessibility of data and resources to authorized individuals in a timely manner.

Confidentiality: A security principle that works to ensure that information is not disclosed to unauthorized subjects.

Controls: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.

Sensitive Information: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled.

Sensitivity: A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

Guidelines:

Portable and Removable Storage Devices

State agencies should implement security controls in proportion with risk and exposure. These security controls are to protect against theft of enterprise equipment, unauthorized disclosure of information, misuse of equipment, or unauthorized access to information assets. Controls could include:

- Employees should only be given the necessary level of privileges for them to do their jobs.
- Equipment, information or software should not be taken off-site without prior authorization.
- Appropriate methods of transport should be implemented depending on the value of the information.

Protect Information Assets

No portable storage device should store any sensitive information without suitable physical and technical protective measures in place. Access control mechanisms should provide appropriate safeguards to preserve the confidentiality, integrity, and availability of the information asset. Security mechanisms could include:

- Encryption
- Tamper evident packaging
- Stored in secure areas, for example, locked filing cabinets

Disposal of Portable and Removable Storage

Devices There is risk of disclosure of sensitive information through careless disposal or reuse of equipment. Formal processes should be established to minimize this risk.

- The contents of removable media should be permanently destroyed or rendered unrecoverable in accordance with applicable state, federal or agency record retention requirements when no longer required.
- Storage devices such as hard disk drives and other media (tapes, diskettes, CDs, DVDs, Personal Electronic Devices (PEDs), or other devices that store information) containing sensitive information should be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive information. For disposal of electronic equipment, refer to

the Statewide Policy 107-009-0050 on Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery Policy).

Employee Security Policy

https://www.oregon.gov/das/Policies/107-004-053.pdf

Purpose: The purpose of this policy is to protect information assets and reduce the risk of human error and misuse of enterprise information and equipment.

Policy: Each agency will develop and enforce a policy that:

- Requires pre-employment screen of employees commensurate with the value and risk of the information assets they will have access to;
- Establishes accountability and responsibility to all employees having access to the agency's information assets;
- Establishes processes for timely removal of all permissions for employees having access to information assets and return of agency assets at termination or reassignment; and
- Establishes awareness training for employees.

Compliance

Each agency may, based upon its individual business needs or legal requirements, exceed the security requirements put forth in this document but must, at a minimum, achieve the security objectives defined in this document.

State agencies have six (6) months from effective date of this policy to comply with this policy.

Authority:

This policy is established under the authority of 2005 Oregon Laws Chapter 739, OAR 125-800-005, 125-800-0010 and 125-800-0020.

Applicability:

This policy applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b) and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

Attachments: none

Definitions:

Asset: Anything that has value to the organization.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Security: Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.

Integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.

Risk: The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential or probability that a threat will exploit the vulnerability.

Security Policy: Documentation that describes senior management's directives toward the role that security plays within the organization. It provides a framework within which an organization establishes needed levels of information security to achieve the desired confidentiality, availability and integrity goals. A policy is a statement of information values, protection responsibilities, and organization commitment managing risks.

Integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.

Risk: The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential or probability that a threat will exploit the vulnerability.

Security Policy: Documentation that describes senior management's directives toward the role that security plays within the organization. It provides a framework within which an organization establishes needed levels of information security to achieve the desired confidentiality, availability and integrity goals. A policy is a statement of information values, protection responsibilities, and organization commitment managing risks.

Guidelines:

Agency management should ensure that employees and volunteers:

- Are briefed on compliance with agency policies;
- Sign for the receipt of agency policies:
    - o Acknowledging receipt of the policies; and
    - o Acknowledging their understanding and agreement to comply with agency policies.
- Receive user awareness training;
- Are aware of their roles and responsibilities for the protection of information assets.

Agencies should have documented procedures for the review and classification of appropriate security levels for staff members whose duties have changed due to promotion, demotion, or reassignment.

Voluntary Termination

Agencies should follow normal access control policies and procedures whenever an employee voluntarily leaves state service or accepts a position or job rotation, developmental or work out of classification assignment, within the agency or with another agency. In some cases, agencies may wish

to remove access to information assets at the time an employee informs them of his/her intention to leave or accept a job rotation, developmental or work out of classification assignment.

Involuntary Termination

Access to information systems and assets should be removed prior to or at the same time the employee is notified of an involuntary action. Involuntary termination is disciplinary termination or removal from trial service, layoff, or for temporary actions such as duty station at home, suspension with or without pay or administrative leave pending an investigation.

Information Asset Classification Policy

https://www.oregon.gov/das/Policies/107-004-050.pdf

Purpose: The purpose of this policy is to ensure State of Oregon information assets are identified, properly classified, and protected throughout their lifecycles. Information, like other assets, must be properly managed from its creation to disposal. As with other assets, not all information has the same value or importance to the agency and therefore information requires different levels of protection. Information asset classification and data management are critical to ensure that the state's information assets have a level of protection corresponding to the sensitivity and value of the information asset. This policy collectively applies to all information assets, including but not limited to paper, electronic and film.

Policy: All state agency information will be classified and managed based on its confidentiality, sensitivity, value and availability requirements. Each agency will identify and classify its information assets. Proper levels of protection will be implemented to protect these assets relative to the classifications. This policy is subject to the limitations and conditions of the Oregon Public Records Law.

Information Ownership

All information will have an information owner or owners established within the agency's lines of business. Owners can be individuals or groups of individuals as best meets the business model of the agency. The information owner(s) will be responsible to:

- Create an initial information classification, including assigning classification levels to all data;
- Approve decisions regarding controls, access privileges of users, and ongoing decisions regarding information management;
- Ensure the information will be regularly reviewed for value and updated to manage changes to risks due to new threats, vulnerabilities, or changes in the environment.
- Perform periodic reclassification based upon business impact analysis, changing business priorities and/or new laws, regulations and security standards.
- Follow state archive document retention rules regarding proper disposition of all information assets.

When a person(s) designated as information owner no longer has this responsibility due to departure, transfer or reassignment of duties, the agency will appoint a new information owner(s) in a timely manner to ensure no lapse in accountability and responsibility for information assets.

Asset Classification Levels

Each agency shall identify its information assets for the purpose of defining its value, criticality, sensitivity and legal implications. Agency must use the classification schema included in this policy to differentiate between various levels of sensitivity and value. All information assets shall be classified strictly according to their level of sensitivity as follows:

Level 1, "Published" - Low-sensitive information. Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of agency employees, clients and partners. This includes information regularly made available to the public via electronic, verbal or hard copy media.

Examples: Press releases, brochures, pamphlets, public access Web pages, and materials created for public consumption.

Level 2, "Limited" - Sensitive information that may not be protected from public disclosure but if made easily and readily available, may jeopardize the privacy or security of agency employees, clients, partners. Agency shall follow its disclosure policies and procedures before providing this information to external parties.

Examples: Enterprise risk management planning documents, published internal audit reports, names and addresses that are not protected from disclosure.

Level 3, "Restricted" - Sensitive information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners or individuals who otherwise qualify for an exemption. Information in this category may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized agency business must be under contractual obligation of confidentiality with the agency (for example, confidentiality/non-disclosure agreement) prior to receiving it.

Security threats at this level include unauthorized disclosure, alteration or destruction of data as well as any violation of privacy practices, statutes or regulations. Information accessed by unauthorized individuals could result in financial loss or identity theft. Security efforts at this level are rigorously focused on confidentiality, integrity and availability.

Examples: Network diagrams, personally identifiable information, other information exempt from public records disclosure.

Level 4, "Critical" - Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners, or cause major harm to the agency.

Examples: Disclosure that could result in loss of life, disability or serious injury or regulated information with significant penalties for unauthorized disclosure, information that is typically exempt from public disclosure.

Information Asset Protection

Each information asset classification will have a set or range of controls, designed to provide the appropriate level of protection of the information commensurate with the value of the information in that classification.

Compliance

Agencies will properly identify and protect information meeting the definitions, requirements and effective dates outlined in the Oregon Consumer Identity Theft Protection Act (Senate Bill 583, 2007 Legislative Session) as they relate to personal information.

Each agency may, based upon its individual business needs or legal requirements, exceed the security requirements put forth in this policy but must, at a minimum, achieve the security objectives defined in this policy.

To reduce the state's risk exposure for information not covered under Senate Bill 583, agencies will focus initially on classifying and protecting Level 4, "Critical" information. Classification of information shall be accomplished in accordance with the following timeline:

- Agencies shall develop a plan for identifying, classifying and protecting information assets. The plan will be in place no later than June 30, 2009.
- All Level 4, "Critical" information assets will be identified and protected no later than December 31, 2009.
- Agencies shall comply with all other prov1s1ons of this policy, including identification, classification and protection of all information assets, by June 30, 2010.

Authority:

This policy is established under the authority of 2005 Oregon Laws Chapter 739, OAR 125-800-005, 125-800-0010 and 125-800-0020.

ORS 162.305 Tampering with public records

ORS 192.501 Public records conditionally exempt from disclosure

ORS 192.502 Other public records exempt from disclosure

ORS 192.660 Executive sessions permitted on certain matters; procedures; news media representatives' audience; limits

ORS 291.037 Legislative findings on information resources

ORS 219.110 Achieving Oregon benchmarks; monitoring agency progress

Applicability:

This policy applies to all Executive Branch agencies as defined in ORS 17 4.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b)and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

Attachments: none

Definitions:

Asset: Anything that has value to the organization.

Availability: The reliability and accessibility of data and resources to authorized individuals in a timely manner.

Classification: A systematic arrangement of objects into groups or categories according to a set of established criteria.

Confidentiality: A security principle that works to ensure that information is not disclosed to unauthorized subjects.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Owner: A person or group of people with authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security: Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.

Integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.

Sensitive Information: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled.

Sensitivity: A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

Guidelines:

Information Asset Classification Responsibilities

Each agency should establish policies, procedures and practices for managing information assets within the agency's lines of business. These policies, procedures and practices should:

- Establish processes for identifying agency information assets and assign classification levels to all data;
- Establish procedures in support of decision-making regarding controls, access privileges of users, and ongoing information management;

- Ensure the information is regularly reviewed for value and updated to manage changes to risks due to new threats, vulnerabilities or changes in the environment;
- Establish practices for periodic reclassification based on business impact analysis, changing business priorities or new laws, regulations and security standards; and
- Enforce state archive document retention rules regarding proper disposition of all information assets.

Labeling Limited, Restricted or Critical Information

Proper labeling enables all parties to correlate the information with the appropriate information handling guidelines. Information should be properly labeled so that users are aware of classification.

The key to effective labeling is ensuring that a person with access to the information is aware of its classification and what restrictions exist in the release or handling of the information. Each individual piece of information or data does not necessarily have to be physically labeled. For example, one alternative to specifically labeling "Published" information is to have an agency policy that states "Published" information has no label on it while "Limited," "Restricted" and "Critical" are specifically labeled. In this case, agency staff would know that a particular piece of information is at the "Published" level because the information is not labeled.

Information labeling can also occur at a higher or aggregate level than the specific data or document level, depending on how the information is accessed. For example, it may be more effective to label information at the folder level, screen level, application level, report level, or form level, than at the specific document level or data field level. Any labeling strategy that effectively alerts the person accessing the information about its classification level would comply with this policy.

Information Handling

The state's information assets should be handled in a manner to protect the information asset from unauthorized or accidental disclosure, modification or loss. All information assets should be processed and stored in accordance with the information asset classification levels assigned in order to protect the confidentiality, integrity, availability, and level of sensitivity.

An agency that uses information from another agency should observe and maintain appropriate security for the classification assigned by the owner agency.

Information Isolation

Information belonging to different information asset classifications should be logically or physically separated or the aggregate information protected at the highest classification level. Whenever and wherever possible, information assets classified as "Critical" should be stored in a separate, secure area.

Proper Disposal

All electronic, paper and physically recorded information assets should be disposed of in a manner consistent with the information asset classification of the information and comply with established State of Oregon archive laws, rules and regulations. For disposal of electronic equipment, refer to Statewide

Policy 107-009-0050 on Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery Policy).

Cyber and Information Security Policy

https://www.oregon.gov/das/Policies/107-004-052.pdf

PURPOSE

This policy establishes a unified and coherent statewide cyber and information security program to manage risks to state agency operations, information and information systems, and supporting infrastructure and services, while aligning cyber and information security with agencies' missions, goals and business operations.

APPLICABILITY

This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division or office within the Oregon Executive Branch. The following agencies and boards are excluded:

- Secretary of State.
- State Treasurer.
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery.
- State Board of Higher Education or any public university listed in ORS 352.002.

EXHIBITS/INSTRUCTIONS

The Statewide Information Security Plan and the Statewide Information and Cyber Security Standards can be found on the Cyber Security Services' (CSS) website: https://www.oregon.gov/das/OSCIO/Pages/SecurityGuidance.aspx .

Enterprise cyber and information security policies can be found on the Department of Administrative Services' website: https://www.oregon.gov/das/Pages/policies.aspx#IT .

CSS Exception Request Form can be obtained by agencies by emailing eso.info@oregon.gov .

DEFINITIONS

Availability: The principle of ensuring timely and reliable access to and use of information.

Confidentiality: The principle of preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.

Cyber Security: The process of protecting information by preventing, detecting and responding to attacks.

Incident: A single or series of unwanted or unexpected information security events that result in harm or pose a significant threat of harm to information assets, an agency or third party, and which require non-routine preventive or corrective action.

Integrity: The principle of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.

Information System: Computers, hardware, software, storage media, networks, operational procedures and processes used in collecting, processing, storing, sharing or distributing information within, or with any access beyond ordinary public access to, the state's shared computing and network infrastructure.

SPECIAL EXCEPTIONS

State agencies seeking an exception to this policy or cyber and information security program requirements must submit an exception request for approval by the State Chief Information Security Officer (CISO), using the CSS Exception Request Form. The CSS will review all exception requests to assess impact on enterprise risk.

GENERAL INFORMATION

The people of and businesses operating within Oregon have entrusted state government with information that they expect will be protected and secured. Information is a strategic asset that should be managed and secured as a valuable state resource.

(1) General Roles and Responsibilities Protecting information security requires coordinated action by Enterprise Information Services (EIS), state agencies and individual users, all of whom play key roles in protecting state information assets. (a) Enterprise Information Services – Chief Information Security Officer: Within the EIS, the State CISO manages the state's information security program and serves as head of the CSS. The State CISO has overall responsibility for the development, implementation and performance of the cyber and information security program, including:

- Developing and maintaining administrative rules, policies, Statewide Information Security Plan, Statewide Information and Cyber Security Standards and other documentation.
- Managing a risk-based information technology security assessment and remediation program, including establishing enterprise risk and vulnerability management programs, policies and procedures.
- Providing unified enterprise solutions, technology, services and guidance to manage enterprise level risks and assist agencies with implementing their own security programs.
- Identifying enterprise security requirements to limit the risks to state information assets.
- Developing, managing, and executing the enterprise cyber and incident response program.
- Implementing an enterprise information security awareness and training program.

• Providing information to and coordinating information sharing among state agencies regarding cyber security risks, threats, vulnerabilities and security measures.

• Providing information security subject matter expertise to state agencies.

• Maintaining security metrics to track the performance of the program. In coordination with state agencies, CSS will maintain enterprise documents to establish cyber and information security program requirements and guide state agencies in meeting these requirements.

These enterprise documents are comprised of:

• Statewide Information Security Plan: Defines the relevant safeguards for Oregon state agencies and state information systems, networks and applications.

• Policies: Document high-level rules, establish roles and responsibilities and set management expectations for information security practices. Policies complement the requirements outlined in the Statewide Information Security Plan.

• Standards: Identify a set of minimum requirements agencies must meet or approaches agencies must use when implementing the Statewide Information and Cyber Security Standards and information security policies. Agencies may elect to exceed these minimum security standards to achieve their organizational security goals and requirements.

• Best Practices and Guidance: Non-mandatory information that agencies may use to enhance the security of their information systems. CSS will review the Statewide Information Security Plan, policies, and standards annually and update these documents, at minimum, every two years. In addition, the CISO will define annual program priorities and implementation goals and provide this information to state agencies to guide program budgeting, planning and execution. The CISO may also issue binding operational guidance to agencies specifying actions that agencies must implement to safeguard state information and information systems from a known or reasonably suspected information security threat, vulnerability or risk. (b) Agencies, Boards and Commissions: While it is the responsibility of all agency leadership, managers and staff to implement the requirements of this policy, the agency head is ultimately accountable for cyber and information security in their agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise.

Each agency head is responsible for:

• Providing clear direction and visible support for the cyber and information security program.

• Accepting cyber and information security risk on behalf of the agency.

• Ensuring the agency's compliance with the Statewide Information Security Plan, state policies, standards and initiatives, and with applicable federal and state laws and regulations.

Each agency must maintain a cyber and information security program to secure the information assets under its control. The basic agency program requirements include:

• Identifying responsibilities for cyber and information security management.

• Maintaining an inventory of agency hardware and software assets and categorizing assets based on their value to the agency and the business processes they support.

• Assessing threats, vulnerabilities and risks to agency information assets.

• Identifying security requirements to effectively limit cyber and information security risks associated with the agency's business goals and objectives.

• Establishing processes for incident identification and reporting.

• Implementing security education, training and awareness for all users of agency information assets.

• Communicating information security policies throughout the agency to users in a form that is relevant, accessible and understandable. Each agency must comply with the Statewide Information Security Plan, state policies and standards. Agencies may either adopt the Statewide Information Security Plan and state policies or create their own plans and policies that comply with these documents. Each agency may, based upon its individual business needs or legal and regulatory requirements, exceed the security requirements established by CSS, but must, at a minimum, achieve the security objectives defined in those documents and may not conflict with those requirements. Agencies are responsible for developing internal procedures and guidance to implement their information security programs. Agencies will review and revise their information security plans, policies, standards and procedures in accordance with the Statewide Information Security Plan and the Statewide Information and Cyber Security Standards, as needed, every two years, at a minimum. Agency information technology and risk environments are constantly evolving. Agencies will implement policies and procedures to regularly monitor and assess their cyber and information security programs.

Agencies shall:

• Ensure that new business needs and risks are reflected in their information security plans and policies.

• Develop plans, in consultation with the EIS and CSS, for information systems and components that cannot be appropriately protected or secured and ensure that such systems are given a high priority for upgrade, replacement or retirement.

(c) Users: Agency, board and commission full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities, collectively referred to as "users," are individuals authorized to access, and have a need to use, state information assets as part of their assigned duties or in fulfillment of assigned roles or functions. All users are governed by and responsible for complying with information security plans, policies, standards, and guidance and are accountable for their actions when using state information assets.

All users are responsible for:

• Being aware of and complying with state and agency plans, policies, procedures, and standards and their responsibilities for protecting the information assets of their agency and the state.

• Using information resources only for intended purposes as defined by the policies, laws and regulations of the state or agency.

• Completing annual enterprise security training and role-specific security training, as well as participating in enterprise and agency security awareness and training initiatives as directed.

(2) Enterprise Security Baseline State information systems are connected with one another and with those of third-party stakeholders and service providers, creating shared risk. In order to establish a common security baseline, Cyber Security Services has defined a minimum set of controls, based on the Center for Internet Security (CIS) Controls, https://www.cisecurity.org/controls/. All agencies must, at minimum, implement the CIS Controls - Basic, as defined in CIS Controls Version 7, by June 2021.

These controls are:

• Inventory and Control of Hardware Assets.

• Inventory and Control of Software Assets.

• Continuous Vulnerability Management.

• Controlled Use of Administrative Privileges.

• Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

• Maintenance, Monitoring and Analysis of Audit Logs. The CSS will provide guidance and assistance to agencies on meeting these controls. These controls establish minimum requirements for all agencies, but are not a comprehensive set of all activities required to protect agency information assets. Agencies remain responsible for taking all necessary steps to secure agency information assets and for implementing statewide standards. Additionally, agencies should seek to implement all 20 CIS Controls as soon as practical. (3) Reviews and Updates the information security risk environment is constantly changing as new technology and services emerge. Consequently, the CSS will review this policy annually and update it, at a minimum, every two years to address evolving risks to state information assets.

Information Security Incident Response Policy

https://www.oregon.gov/das/Policies/107-004-120.pdf

PURPOSE

This policy defines Oregon state government's approach to cyber and information security incident response. Effective incident response helps protect the availability, integrity and confidentiality of state information assets.

APPLICABILITY

This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division or office within the Oregon Executive Branch.

The following agencies and boards are excluded:

- Secretary of State.
- State Treasurer.
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery.
- State Board of Higher Education or any public university listed in ORS 352.002.

FORMS/EXHIBITS/INSTRUCTIONS

The State Information Security Incident Response Plan further details roles and processes for the state's response to cyber and information security incidents.

An Agency Incident Response Plan Template is available to assist agencies in establishing or updating their incident response plan.

These documents and other incident response resources are available at: https://www.oregon.gov/das/OSCIO/Pages/SecurityResponse.aspx

DEFINITIONS

Asset: Anything that has value to an organization.

Availability: Ensuring timely and reliable access to and use of information.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.

Incident Response Plan: Written document that states the approach to addressing and managing incidents.

Incident Response Policy: Written document that defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for responding to and reporting incidents.

Incident Response Procedures: Written document(s) detailing the steps taken when responding to incidents.

Information: Any communication or representation of knowledge in any medium or form. Examples include but are not limited to:

- Documents, reports, statistics, files, and records, compiled or stored in digital or physical form.
- Emails or messaging system conversations and their attachments.
- Audio and video files.

- Images, graphics, pictures and photographs.
- Programs, software and macros.
- Spoken conversations.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.

Integrity: Guarding against improper information modification or destruction, which ensures information nonrepudiation and authenticity.

Risk: A measure of the extent to which an organization is threatened by a potential circumstance or event, which takes into account the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

Security Event: An observable, measurable occurrence involving an information asset that is relevant to security operations.

Security Incident: A single or series of unwanted or unexpected security events (refer to definition of "security event") that results in harm, or poses a significant threat of harm, to information assets, an agency, or third party and requires non-routine preventive or corrective action.

GENERAL INFORMATION

(1) General Roles and Responsibilities

Responsibility for incident response is shared among Enterprise Information Services (EIS), Cyber Security Services (CSS) and agencies to ensure that state response efforts are adequate, uniform, and coordinated, regardless of incident size or complexity.

(a) Enterprise Information Services – Cyber Security Services:

CSS manages the state's response to incidents including those involving an actual or suspected breach under the Oregon Consumer Information Protection Act (ORS 646A.600 et seq.). Depending upon the incident scope and impact, and agency capabilities, CSS may either directly manage the incident or coordinate with the affected agency on the incident response. The CSS's role may change during the incident.

CSS Security Operations Center (SOC) will collect, classify, and catalog all reported information security incidents and assess incident scope and impact. CSS SOC will respond to information security incidents that potentially impact multiple agencies or which pose a significant risk to the state. CSS SOC manages inter-agency incident response resources and communications for incidents that impact multiple agencies. In addition, CSS maintains expertise and capabilities to assist state agencies with incident response.

CSS will establish enterprise policy, standards, and guidelines for statewide and agency-level cyber and information incident response. CSS will develop and maintain the State Information Security Incident Response Plan to define processes for incident response preparation; detection and analysis; containment, eradication and recovery; and post-incident analysis. CSS may also develop supporting

procedures and processes. CSS also leads enterprise training, exercises, and other activities to test, evaluate, and improve the incident response program.

The State Chief Information Security Officer develops partnerships and engages with the Oregon Cybersecurity Advisory Council, regional and local governments, other state governments, the federal government, law enforcement organizations, and private sector entities to prepare for, respond to and recover from incidents.

(b) Agencies:

Agencies are responsible for reporting incidents to CSS SOC, per "Reporting Information Security Incidents" below, and for taking steps necessary to respond to an incident, in coordination with or at the direction of the CSS SOC.

Each agency must maintain the capability to respond to information security incidents involving information in any form. Agencies may establish this capability by using internal or a combination of internal and external resources, but at a minimum agencies must maintain:

- An incident response plan.
- Processes and procedures for implementing this incident response plan.
- A point of contact to interface with CSS SOC.

State agencies may, based on their individual business needs or legal or regulatory requirements, exceed the requirements outlined in this policy but must meet these minimum requirements.

Agencies must maintain an internal incident response plan that details agency processes and responsibilities, including how the agency will support CSS-led incident response efforts. The agency plan must align with the State Information Security Incident Response Plan. Agency incident response plans must identify:

- Incident response roles and responsibilities.
- Resources and procedures for incident management across the following activities:
    - Preparation.
    - Detection and Analysis.
    - Containment, Eradication and Recovery.
    - Post-Incident Activity.
    - Communications with internal and external stakeholders.
    - Notification of CSS SOC upon incident determination.
- Procedures for managing incidents involving regulated information, including documenting notification requirements and processes.
- Awareness training regarding information security incident responsibilities, incident identification and reporting.
- Training for designated responders specific to their role within an incident.

- Processes for testing and updating the plan.

Agencies must review incident response plans annually and update plans to address system and organizational changes; lessons learned during plan implementation, testing or execution; and changes in enterprise policy, standards and guidance.

Agencies must provide incident response plans to CSS SOC for review.

(2) Reporting Information Security Incidents

Each agency must report information security incidents to CSS SOC no later than 24 hours after discovery via the CSS SOC Hotline, 503-378-5930. In some cases, it may not be feasible to have complete and validated information prior to reporting. Agencies should provide all available information at the time of notification and report updated information as it becomes available.

If unsure whether a situation is an incident, agencies should consult with CSS SOC to determine if an incident has occurred. Agencies should err on the side of caution and report all suspected incidents to CSS SOC.

State agencies are also required to report incidents to the Legislative Fiscal Office (per ORS 276A.306), and to make any other notifications required by law or regulation.

Reportable incidents must meet all four of the following criteria (for examples, refer to “Guidelines” below):

- Involves information security.
- Is unwanted or unexpected.
- Shows harm, intent to harm or significant threat of harm.
- Requires a non-routine response.

All users who are provided authorized access to agency information or systems are responsible for promptly reporting suspected or actual security incidents to their agency points of contact.

Upon identification of an incident, the agency must immediately initiate its incident response plan and designate a point of contact to communicate information security incidents to CSS. The agency point of contact will work with CSS to establish the method of reporting. CSS will communicate with the agency point of contact to coordinate, investigate and respond to the incident, as needed. The agency must support CSS in its responses, including but not limited to, providing the necessary resources, providing all requested information and taking actions as directed by CSS.

(3) Incident Categorization

CSS will categorize incidents as described in the State Information Security Incident Response Plan. CSS has ultimate authority to determine an incident has occurred and to categorize incidents, and may reclassify and escalate incidents as conditions change. CSS may require agencies to take action based upon the incident categorization.

GUIDELINES

An incident involves a single or series of unwanted or unexpected information security events that results in harm, or poses a significant threat of harm, to information assets, an agency, or third party and requires non routine preventive or corrective action. Incidents may take various forms – for example, some incidents involve a breach of personal information – and can stem from various causes. The lists below provide examples of reportable information security incidents, along with examples of events that agencies do not need to report to CSS SOC. These lists are meant to guide agencies, but are not comprehensive.

- Reportable incidents include, but are not limited to, the following:

    a. Any incident relevant to regulated data, including the Oregon Consumer Identity Protection Act; breaches of personal information are a type of incident.

    b. Malware that has become widespread.

    c. Successful phishing attempt.

    d. Denial of service attacks.

    e. Lost or stolen documents or information assets (e.g., laptop, thumb drive, etc.) containing sensitive or potentially sensitive information.

    f. Conversation containing Level 3 or Level 4 information overhead by an unauthorized person who discloses the information to the public.

    g. Website defaced.

    h. Unauthorized access to information.

    i. Any kind of sabotage that affects information or information systems.

- Non-reportable events that do not qualify as incidents include the following:

    a. Criminal violations with no information security component, such as car theft.

    b. Increased website activity that leads to the site becoming unavailable (activity is not unwanted or unexpected – e.g. due to popularity).

    c. Documents lost, where there is no harm, no intent to harm, or no significant risk of harm (e.g., briefcase containing publicly disclosable documents).

    d. Computer virus detected on a workstation that is successfully contained by anti-virus software (i.e., no non-routine action is required).

Privileged Access to Information Systems Policy

https://www.oregon.gov/das/Policies/107-004-140.pdf

Policy/Purpose:

This policy establishes the process and expectations for granting and using privileged access to the information systems of the State Data Center (SDC). Privileged access enables users to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff who perform computing account-administration, or other staff whose job duties require special privileges over a computing system or network.

Authority:

Statewide Policy #107-004-110: Acceptable Use of State Information Assets ORS 182.122: Information Systems Security in Executive Department

Applicability:

This policy applies to all SDC users and contractors, and staff and contractors of customer-agencies who require, request, and acquire privileged access to the SDC's information systems.

Attachments:

Attachment A: Privileged Access Request

Attachment B: Privileged Access Agreement

Definitions:

Authorized Requestor – A person delegated by an agency who is authorized to approve and submit user requests for privileged access.

Compelling Circumstances – Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or state policy, or significant liability to the SDC or its customers.

Electronic Communications – Any transfer of signals, writings, images, sounds, data or intelligence that is created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or more electronic communication systems. Under this policy, an electronic file that has not been transmitted is not an electronic communication. (This definition is modeled after the Electronic Communications Privacy Act (US Code Title 18 § 2510).

Electronic Communications Records – The contents of electronic communications created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or more electronic communications systems or services. This definition applies to original records, copies, or modifications of original records, and includes attachments to electronic communications records and transactional information associated with such records.

Electronic Communications Systems or Services – Any system used to message, collaborate, publish, broadcast, or distribute, which depends on electronic communications resources to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network-systems between or among users or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

User, End-User – People who use IT services on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT services directly.

Holder of an Electronic Communications Record – A user of electronic communications who, at a given point in time, receives or possesses a particular electronic communications record. This definition applies whether or not the user is the original creator of the record. Also see "Possession of Electronic Communications Record," below.

Information Systems – Computers, hardware, software, storage media, networks, and the operational procedures and processes used to collect, process, store, share or distribute information — beyond ordinary public access — within the state's shared computing and network infrastructure.

Possession of Electronic Communications Record – A person possesses an electronic communications record when he or she has effective control over the location of its storage or access to its content. Example: Under this policy, an electronic communications record that resides on an electronic communications server awaiting download to an addressee is in the possession of that addressee. This definition does not apply to system administrators and other operators of SDC electronic communications services with regard to electronic communications not specifically created by or addressed to them.

Privileged Access – Access to an information system that enables the user to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access implies greater access than the average end-user.

Transactional Information – Information, including electronically gathered information, needed to complete or identify an electronic communication. Examples include but are not limited to electronic mail headers, summaries, addresses and addressees.

Guidelines:

Overview

The SDC grants privileged access to SDC information systems based on the job requirements of requestors, according to the following scenarios:

a) A user requires access over an extended period of time from a known location or locations. The SDC grants administrative credentials to the user via this policy. In addition, appropriate firewall rules will be set up to allow access for the necessary tools, e.g. SSH, RDP, to permit the user to access the systems, devices, and data outlined in the user's Privileged Access Agreement.

b) A user requires access over an extended period of time from possibly varying locations. The SDC grants administrative credentials to the user via this policy. In addition, the SDC will create a VPN account for the user that includes filters to allow access for the necessary tools, e.g. SSH, RDP, to permit the user to access the systems and devices outlined in the user's Privileged Access Agreement.

c) A customer requires ad-hoc access, such as for technical support or for initial application configuration. An SDC technician creates a conference session to allow one or more remote users to share a session. The technician connects to the device that needs to be shared, using his or her credentials, and shares the window with the remote party. The technician stays present to monitor the

changes being made and closes the session after the work is completed. Optionally, the technician may record the session to create a record of the changes made.

II. Expectations and Requirements

a) Users with privileged access must respect the rights of system users, respect the integrity of systems and related physical resources, and comply with relevant laws and regulations.

b) Users with privileged access have an obligation to keep themselves informed regarding any procedures, business practices, policies and operational guidelines pertaining to the activities of their local department. In particular, the principles of privacy of information hold important implications for system administration at the SDC.

c) Privileged access applies to a particular period of time and includes only specific tasks. Time periods are based on the required tasks; the time period may be brief, such as one-time access, intermittent access, or longer.

d) Privileged access will end at the close of the time period granted by the SDC.

e) It is the customer agency's responsibility to immediately inform the SDC every time an employee leaves, changes duties or no longer needs privileged access to perform their current job duties.

f) The SDC will perform a review twice a year or at least 180 days to verify that accounts are still active. The SDC shall provide a list of inactive and expired accounts to customer agencies. It is the customer agency's responsibility to review the list of exceptions and to notify the SDC within 30 days, when list of exceptions received, of any modifications or else the SDC will revoke access.

g) People approved for privileged access will have two user IDs: one for normal day-to-day activities and one to perform administrator duties.

h) Users with privileged access may only use their access to perform the tasks and functions outlined in the user's Privileged Access Agreement. Any other use including viewing, modifying, copying, disclosing or destroying a system or other user's data, is unauthorized.

i) Users must receive approval from the SDC Change Control Board before making changes to production systems. This does not apply to changes in test or development systems.

j) An agency must communicate directly with its privileged access users if the agency has special requirements, including documentation, related to confidentiality and secrecy.

k) Electronic communications users are not responsible for electronic communications records in their possession when they have no knowledge of the existence or contents of such records.

l) The SDC grants privileged access to users exclusively for the performance of their day-to-day job duties.

m) A Privileged Access Agreement for System Administrators (i.e., the privileged access individual user agreement) shall be signed and submitted to the SDC before the SDC shall grant privileged access to the requesting user.

n) An agency CIO and/or Authorized Requestors shall approve and submit a request for privileged access.

See document for Attachments

Transporting Information Assets

https://www.oregon.gov/das/Policies/107-004-100.pdf

Purpose:

The purpose of this policy is to ensure the security of state information assets when in transit. Information assets can be vulnerable to unauthorized access, misuse or corruption during physical transport. Minimum safeguards must be implemented to protect sensitive information from accidental or intentional unauthorized access, modification, destruction, disclosure, misplacement or permanent loss throughout the delivery/transport cycle.

Policy:

Each agency must use appropriate security controls for transportation of sensitive information assets (physical media -e.g. tape, disk, paper) during transit and beyond the physical boundaries of a facility from loss, destruction or unauthorized access. Each agency that sends, receives or transports confidential or sensitive information to or from another facility or agency/entity is responsible to assure that the information is protected appropriately during transit. The determination of the sensitivity level of an asset is governed by the statewide policy 107-004-050 Information Asset Classification in which it is the responsibility of the information owner to identify sensitive information and ensure appropriate protection.

Authority:

This policy is established under the authority of 2005 Oregon Laws Chapter 739, OAR 125-800-005, 125-800-0010 and 125-800-0020.

Applicability:

This policy applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b)and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

Attachments: none

Definitions:

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Owner: Person with authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Sensitive Information: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled.

Guidelines:

Agencies should evaluate transport options based on the level of sensitivity of the information being transported, the level of risk involved in the transport, and the possible impact of loss or damage to the asset to determine the appropriate means of transportation for different assets. The guidelines provided should be evaluated and applied to the transport of sensitive information where appropriate.

The Department of Administrative Services Enterprise Security Office can provide guidance and consultation to state agencies on best practices to be employed for providing secure transportation of sensitive information.

Considerations for protecting sensitive information assets being transported between sites include:

a. Carrier considerations

1. Use reliable transport or carriers.

2. Agency management should review carrier transport procedures, identify, and approve carriers appropriate for asset transport based on the risk, volume, and sensitivity of the asset being transported, e.g. the US Postal Service may be appropriate for delivery of documents such as checks but not be appropriate for transporting data backup media with large volumes of sensitive information.

3. Develop procedures to check the identification of carriers where appropriate.

4. Incorporate security and liability language into contracts with vendors transporting sensitive state information, including transit to destruction facilities.

5. Sensitive information transported in vehicles by employees should be logged, inventoried, and kept locked and out- of-sight when the employee is not in the vehicle.

b. Packaging considerations

1. Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturer specifications (e.g. for software), for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields.

2. Employ the use of tamper-evident packaging (which reveals any attempt to gain access).

3. Clearly delineate on a form inside the package the number, type, and destination of media.

4. Use secure and clear address labeling.

c. Storage considerations

1. Store packages with sensitive information in a secure location prior to pick up.

2. Store packages with sensitive information in a secure location/compartment in the delivery vehicle.

3. Sensitive packages should be stored in a secure location by receiving entity.

d. Transfer of custody considerations

1. Where feasible and appropriate, the person releasing and the person receiving the package should sign a log to maintain a chain of custody at each point of transfer. In some cases, e.g. the retrieval of assets from a lock box, it may be appropriate that the receiving person should log the pickup of the asset.

2. The log should include date and time picked up, number of packages, destination, etc.

3. The delivery driver should validate the information on the log and sign it.

4. Establish procedures for logging distribution of packages within an organization (e.g. State Data Center, Publishing and Distribution, etc.).

e. Controls, means of managing risk including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management or legal nature, should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification, including:

1. Use of locked containers.

2. Where appropriate and feasible, employ data encryption.

3. Delivery by hand.

4. In exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

5. Deposit in a secure lockbox for after-hours delivery with a shipping receipt.

6. Procedures, as appropriate, for transfer and receipt of information including, as required, notification and acknowledgment of receipt.

Link to Additional Security resources for state agencies

https://www.oregon.gov/das/OSCIO/Pages/Securityresources-ag.aspx

Statewide Information and Cyber Security Standards

https://www.oregon.gov/das/OSCIO/Documents/2019StatewideInformationAndCyberSecurityStandardsV1.0.pdf

Slide 101

ASSESSMENT

Assessment

1. Which of the following actions could make our sensitive information vulnerable to cybercrime?
   a. Connecting to secure wireless connections
   b. Opening e-mail attachments from unknown source
   c. Refraining from posting information about our organization on your personal social networking sites
   d. Keeping security software up-to-date

2. Which of the following actions could result in loss or theft of personal information?
   a. Carrying your laptop on your person at all times when traveling
   b. Keeping track of your USB drive at all times
   c. Loaning an unauthorized person, such as a messenger or visitor, your security badge to our building
   d. Discussing sensitive information only in a private setting so passersby cannot overhear the conversation

3. Which could be a warning sign of social engineering?
   a. Ambiguous messages requiring clarification
   b. Any communication from individuals outside our organization
   c. Unsolicited message appealing to your fear, sympathy, or trust
   d. Customers, clients, or business partners with foreign accents

4. Which of the following forms of communication can experience social engineering?
   a. Any form of communication
   b. Telephone
   c. Electronic Messages
   d. In person

5. Verify the source of any electronic communication that contains a hyperlink. This includes communication via:
   a. E-mail.
   b. Instant messenger.
   c. Texting and social networking.
   d. All of the above.

6. Once you have posted information to the Internet, you can always retrieve or delete it.
   a. True
   b. False

7. Look out for which security threat specifically when using a cloud-based service?
   a. Expired passwords
   b. Out of date security software.
   c. Using only the cloud-based storage to save your files.

d. Phishing attempts from people impersonating a third party.

8. Which should be a security consideration before sending sensitive information using a cloud-based service?
   a. Has the information been fact-checked?
   b. Is the information subject to compliance requirements?
   c. Do you have prior experience working with the recipient?
   d. Is the recipient in a different time-zone?

9. If you fall victim to hacking, the only step you need to take to regain access to your account—and prevent another attack—is to alert the IT department.
   a. True
   b. False

10. Which of the following steps should you take to prevent hackers from gaining access to your accounts?
    a. Use a reputable antivirus software and keep it up-to-date.
    b. Use a secure password and change it frequently.
    c. Use different passwords for each of your accounts.
    d. All of the above.

11. Which of these activities is recommended when working at home?
    a. Using a cross-cut shredder to dispose of documents.
    b. Inserting personal peripheral devices into your work computer.
    c. Allowing family members to use your work devices.
    d. Connecting "smart" devices to your home network.

12. Using a VPN to connect to our organization's network is recommended when working from home.
    a. True
    b. False

13. You should use your professional username and password as credentials for a personal account.
    a. True
    b. False

14. Which is the best definition of "data minimization"?
    a. Collecting, accessing, and retaining the least amount of information necessary.
    b. Compressing data so that it fits more efficiently into network storage.
    c. Editing out unnecessary elements of our policies.
    d. Possessing too little information to get the job done.

15. Which best describes the concept of "data minimization?"
    a. Big data requires big risks.
    b. Small quantities of data, large levels of efficiency.
    c. The less data we handle, the less risk we create.
    d. Minimized data, maximized profit.

16. Under what circumstances is it most ideal for you to change your password?
    a. Your coworker gives you a suggestion for a very strong password.
    b. If your password, or your computer system, has been compromised.
    c. It's been at least 90 days since the time you last changed your password.
    d. You've heard about a data breach affecting one of our competitors.

17. You should share your password only with a member of our IT department, and even then, only when they are in your presence.
    a. True
    b. False

18. Which of the following is a good practice for device passwords?
    a. Use a different password for each device.
    b. Store passwords as contacts in a smartphone's address book.
    c. Use cached information to recall passwords.
    d. Keep your password written near your devices.

19. It is unacceptable to let a client or vendor use your device, even if you are watching them.
    a. True
    b. False