Information Security Awareness Basics

by Fred Cohen

Table of Contents

Front matter

Information Security Awareness Basics

ISBN # 1-878109-39-1
Published by Fred Cohen & Associates out of Livermore, CA.

1 Introduction

Information security is used to protect the utility of content that makes our enterprise work.

Without this content and its utility, our enterprise would fail.
With it, we will prosper.

The protection program is designed to control risks to the enterprise and includes specific requirements for *integrity*, *availability*, *confidentiality*, *control over use*, and *accountability* of specific information.

- **Integrity:** Assuring that the content is what it is supposed to be and is suitable to its purpose.
- **Availability:** Assuring that the content is where we need it when we need it and usable for its purpose.
- **Confidentiality:** Assuring that sensitive content is kept private to those who have a specific need to see it.
- **Use control:** Assuring that content and resources are only used in ways and by those that are appropriate and authorized for those uses.
- **Accountability:** Assuring that people and systems are accountable for their actions.

This booklet and the awareness program it goes with are designed to help you, our workers, understand what to do under the circumstances you are most likely to encounter while working for our enterprise so that you can play your role in our information protection program.

This booklet must be read and understood in order to have utility for the enterprise. In order to make certain of this utility, the content is verified through an exam, computer-based questions, group activities, or other similar methods that provide feedback on your understanding and our quality of presentation. Please help us do our job by asking questions when you have them and letting us know of any errors we have made or questions that remain.

2 Emergency contact information

In case of different emergencies, from your company phone, call the following numbers as appropriate to the particulars of the emergency.

What	*Contact number*
Fire	
Police	
Medical emergency	
Help desk	
Computer security	
HR issue	
Legal issue	
Your supervisor	
Main company operator	
Other emergencies	

Please feel free to make a copy of this page and post it above your desk or in another convenient spot so that when you or anyone else in your office area encounters an emergency, they will be able to quickly find the right number to call.

If you have any other emergency information that is important to people in your work area, please add it to your copy of the chart so it will be appropriate to your needs.

Please update new numbers by informing your manager or the help desk of any errors or omissions.

3 Your responsibilities

You are responsible to do certain things related to information protection as part of your job as a worker at this enterprise. Here are some of the most important ones:

- Read this booklet and do what it says to do.
- Stay aware of safety and security-related issues in your work environment.
- Notice the indicators of security problems identified in this booklet and act on them accordingly.
- Follow the legitimate instructions of properly identified security personnel during emergencies.
- Keep yourself and your co-workers safe and healthy by following procedures as they are identified to you.
- Protect the content and operational capabilities of the enterprise working properly, safely, and securely by following the directions on how to properly use them.
- Know what alarms look and sound like and what they mean so you can do the right thing when an alarm is sounded or displayed.
- Wear your badge, keep your security devices safe, and report any lost, stolen, or missing badges or devices in a timely fashion.
- Don't cheat the security system or allow others to cheat it.
- Use the proper procedures and report those who don't.
- Be polite but firm in your security-related dealings.
- Leave your computer in a properly secured state when you are not sitting in front of it so others cannot act like they are you and do bad things under your name.
- Take proper precautions when you travel for your own safety and health as well as the security of our content.
- Only use company assets for company work and follow the acceptable use rules.
- Protect our enterprise and worker privacy by protecting their financial, health, and other confidential information.

4 The help desk and when to call it

The help desk is the number you usually call when there is a computer security-related issue. If you don't know for sure who to call, the help desk is the right place to start.

The help desk is the nerve center of enterprise security and other computer-related event management. When communications fail, when a computer security incident is underway, when computers aren't working right for any reason, or when users need general assistance related to computers, the help desk gets the call.

When your call comes into the help desk, the help desk operator will first triage your call to determine:

- how critical it is,
- how urgent it is, and
- what type of help is needed.

Because a lot of things may be going on at any given time, your call, though critical and urgent to you, might not be as critical and urgent to the enterprise as a whole. So help the help desk do their job by identifying how important the issue is to how many people, how quickly it has to be taken care of before serious harm to the enterprise results, and what sort of help you think you might need. Be patient with them, they are just doing their jobs.

The help desk will give you three important things during your call:

- The name of the operator.
- Your ticket number if one is generated.
- When you should expect to be contacted further.

Write down the ticket number so you can check on your issue later. Write down the name of the help desk operator so you can write a pleasant thank you note later. Put the contact details in your calendar so that when that date and time arrives, you can check for progress if the issues aren't yet settled.

5 Reading your contract

It is your responsibility to read, understand, and keep your legal obligations to the enterprise as a worker and to read and understand the legal obligations of the enterprise to you and others.

Most people don't read their contract, company policies, procedure manuals, or most of the other things they sign and/or agree to as part of their employment. But you should. It is important to you and important to us that we understand each other clearly and that we all fulfill our obligations to each other.

Unless you are a lawyer, we don't expect that you will understand all of the legal subtleties of contract law and the wordings required to say what should be pretty simple. But we do expect that if you don't understand something in a contract, you will ask someone who does, starting with your manager or supervisor.

You also need to make certain that you read and understand any licensing information associated with any software you put on your work computer or take from your work computer. As a rule of thumb, you should not make copies of anything on your computer except for backup purposes, and then only do so by following the rules on how to do backups.

When you download software and accept a contract at work, you are sometimes forming an obligation for all of us, not just yourself. And when you act using the company's resources, you are acting for the enterprise and your co-workers as well as yourself.

Think of everything you do and say at work as part of the contract you have. Sure, we want to be friendly and helpful to others, and we should be, but we also need to be careful not to obligate ourselves or the enterprise to things that we cannot really do later on, and that we don't violate the agreements we have with other enterprises or individuals with regard to their information or their rights.

6 Physical security

The area where you work has to be kept safe from intrusion by people who are not authorized to be there, both for your health and safety, and for the protection of our enterprise assets, including both the physical things like computers, personal data assistants, cell phones, and so forth, and the information that they contain, process, or are able to access. Physical security is necessary to attain these ends.

The first thing to know about physical security is that others do not belong in your workspace unless they work there. If you don't know them or if they don't have proper credentials displayed, you should assume that they do not belong until they show you that they do belong by one of the methods provided by the enterprise.

If someone does not belong in the workspace, use your own judgment as to whether they appear to be a danger to you, others around you, or enterprise equipment or content.

- If you feel like you are in physical danger, try to move to somewhere safer without causing harm to yourself or others and then call security or dial for emergency help as soon as you can.
- If you feel safe for the moment but feel that physical danger may be present or looming, call security from somewhere that won't upset the cause of the hazard.
- Otherwise, if you feel comfortable with it, ask the individual if you can help them find their way, and escort them to the nearest security guard or the front desk and ask the appropriate people at those stations to take care of the issue.

If harm is being done to equipment, or if someone is accessing a computer who should not be doing so, or plugging things into the walls, or anything else similar to this, call your manager or security to handle it. After this incident is over, write up what happened and give copies to your supervisor and to security for their records.

7 The guards

Guards are used to protect people and property from harm. They are normally skilled and trained professionals at what they do with special skills associated with interacting with people in situations. They may be armed or not, depending on the specifics of the situation. When dealing with guards, except in the rarest of circumstances, it pays to listen carefully to what they tell you to do and do it as safely and quickly as you reasonably can.

Depending on the specifics of the situation, they may have time to talk to you or answer your questions, or they may not. Use your best judgment based on their behavior and instructions to decide whether to engage them in conversations or discussions.

If there are hazards present, you should tell the guards about these hazards to protect them from coming to unnecessary harm. For example, if a guard enters an area that has fluid on the floor, you should tell the guard what the fluid is on the floor so they don't slip and fall or otherwise get hurt. But again, you need to use your judgment to balance their safety against other risks of the situation.

If you called the guards, you should let them know that you called them and why you did so. If the guards are there because of some dangerous situation, they may want to keep their presence secret, so if you see them, don't give them away until they choose to reveal themselves. If the source of the danger has moved elsewhere, direct the guards to the source of the danger and explain to them what occurred.

If you encounter someone who looks like a guard but doesn't have proper identification or other related things that authenticate that they are a guard, follow their directions and call security to confirm that they are legitimate when you have an opportunity to do so without creating a potential problem.

If you are unsure about a situation, contact your supervisor immediately and ask for their assistance in resolving the issue,

8 Staying healthy and safe

Protecting the people you work with and yourself also helps to protect the enterprise's most valuable information assets, its people. This means that whenever there is something in the physical environment that seems to you to be unhealthy, you should avoid it and contact your supervisor about it. You should also help to protect your fellow workers and the equipment and content of the enterprise by following these guidelines:

- If you are sick, do not come into work. You will likely not work very well and you may get your fellow workers sick as well. Call in sick and let your supervisor know.
- If you encounter someone at work who is sick, try not to contact them physically, stay away from their sneezes and sniffles, and contact your supervisor.
- If you encounter something that you think will make you ill or cause harm to your health, avoid it and contact your supervisor. If your supervisor is not responsive, contact the health and safety officer. If you feel your health may be at risk, it is reasonable and prudent for you to resign over this issue and seek employment elsewhere. Your health is more important than a job.
- When using computers, stress injuries and other similar health risks may arise from excessive typing in one position, lack of physical exercise, working too long without a break, staring at the screen too long, staying in an air conditioned or noisy area without proper protective clothing, or other similar things. Take a break when you need one and make sure your work area is ergonomically suited to your needs so you don't hurt yourself at work.
- Computers may be heavy, have electrical connections, and they sometimes have sharp edges or other similar safety hazards. Only move computers that are supposed to be mobile unless you have been trained to move this sort of thing. Don't create or allow tripping hazards or similar things in your workspace. Don't leave open electrical gadgets on. And bend your knees when you lift.

9 Protecting others

Your responsibility to the enterprise and your co-workers goes beyond keeping yourself safe. You also have a responsibility to others, although it doesn't mean you should put yourself at undue risk in the process. This responsibility means that you should notice what happens in your work environment and, when you see dangers or hazards to others, including the enterprise you work for, you should act to prevent the harm from being done. Here are some examples of the proper way to act:

- If a fellow worker is upset and starting to do harm to the enterprise through their behavior, you should contact your supervisor (or if it's them their supervisor) to let the supervisor know that is going on. It is a good idea to document this in writing.
- If you accidentally stumble on information that you know should not be available to you, like a file cabinet drawer that is left open with obviously sensitive information, or an outdoor shed with boxes of papers and the door open, or a set of boxes labeled employee records, or other similar things, you should report this to your supervisor in an email or a memo or verbally at your earliest convenience.
- If you encounter sensitive information in a computer system or on a Web site, you should report this to the help desk indicating the nature of what you found, that it is a computer security issue, and what you think it might mean to the enterprise if left unfixed.
- If you find that things on the enterprise network look very different or don't seem to be working right and you have not been notified of the changes in advance, you should contact the help desk to report the issue and find out if you missed something or if something else is wrong or broken.

These are only examples. In general, when you see something that just doesn't look right (JDLR), you should report it to your supervisor, security, or the help desk, depending on its nature.

10 Strangers in the workplace

With rare exceptions, people know the people they work with every day and are introduced to new workers by their supervisor. There should be nobody in your work area that you don't know or haven't been introduced to by your management unless they are being escorted by someone you know. If you encounter a stranger in the workplace, even if they have proper attire and a proper badge on, you should do the following:

- Introduce yourself to them in a polite way, indicate that you have never met them before, and ask their name, what their job is, and who they work for.
- If you don't know the person they work for or if their job is not one performed in this area, escort them out of the area and to the proper reception area so they can be properly dealt with.
    - If they refuse, walk to a safe place and call security and report the details.
- If they name someone who legitimately works in your area, help them out by escorting them to that person's location, and
    - If the contact person is present they need to tell you that this is alright and escort the individual from then on or introduce the individual to you so you know that they belong in the workplace.
    - If the contact person is not present, explain that they need to wait at reception for that person to come for them.
- If they claim to be from maintenance or security or some such thing, bring them to your supervisor for proper confirmation and handling.
- File a written report on any such incident not resolved by the legitimate contact person escorting them to your supervisor and security.

Strangers in the workplace are potentially dangerous to you, your co-workers, the enterprise, and themselves. Keep us all safe.

11 Protecting the environment

We all live in one world, and when there are environmental problems they may have serious negative consequences on all of us. For that reason, the protection of the environment is important to our enterprise and all of our workers. Environmental hazards may hurt people as well as harming information in paper, electronic, or other forms. As a result, when you encounter an environmental hazard, or something you think is an environmental hazard, you should respond to it in a timely fashion. Smoke, dust, and other environmental conditions can be very damaging to people and computers. If you are in an environment with a substantial amount of smoke, dust, or other conditions:

- If there is an alarm sounding, take your personal belongings and follow the procedures for that sort of alarm.
- If there is an apparent fire or other hazardous event but no alarm sounding and the event cannot easily be managed by you with available equipment:
    - Take your personal belongings to a safe place,
    - Warn any fellow employees along the way.
    - Pull the first fire alarm you encounter on the way.
    - As soon as you are safe, call emergency services.
- If there is no apparent danger or alarm sounding, and if the situation seems safe to you:
    - Notify your supervisor and other employees in the area with you.
    - Contact ermergency services by telephone.
    - Shut down any equipment you are authorized to shut down.
    - Take your personal belongings and go to the designated emergency collection point.
    - Do not reenter the area until an authorized person tells you the situation has been made safe and the all clear is sounded.

12 Things you hear, see, or smell

People often see, hear, or smell things that are hazardous to them or the equipment they are using. Quick response can save both lives and equipment. When you hear, see, or smell something that is unusual in your work environment, it should concern you. Here's what you should do if it is not an alarm:

- If it is overwhelming or makes you nauseous,
  - Immediately leave the area and go to a well ventilated area or the emergency meeting point.
  - Bring your co-workers with you unless they are unable to come.
  - Contact emergency services or the fire department and report details to them.
  - Do not return to the area until the all clear is sounded.
  - Document what happened when you are in a safe place and report the details to your supervisor.
- If it is not overwhelming and doesn't make you nauseous:
  - Notify your supervisor and co-workers.
  - Try to locate the source.
  - Turn off any equipment that is causing the problem if you are authorized to turn it off, or notify the operator who is authorized to turn it off to do so.
  - Document the incident.
  - Continue working unless the situation changes.

If there is any question that the situation may be associated with a health or safety hazard to you or you co-workers, evacuate the area and call emergency personnel to take care of the issue. Don't try to be a hero or try to show that you can take it. Do the safe thing. Discretion is the better part of valor!

13 Responding to alarms

There are a variety of different sorts of alarms that can occur in the work environment, It is important that you become familiar with

them and what they mean in terms of what they indicate and what you should do when you encounter them. Some of the more common alarm sounds and what they mean include:

- Vehicle sirens usually mean either fire or police are present. Follow instructions they give when they arrive.
- Fire alarms mean that there is a fire. Take personal items and go to the nearest fire exit and collect with other workers at the identified collection point.
- Smoke alarms mean that there is smoke or another similar problem with the air. If it looks safe, turn off computers you are authorized to turn off, collect your personal things, and go to the nearest fire exit. Collect at the identified collection point.
- Sirens indicative of tsunamis, earthquakes, volcanoes, or other natural phenomena should be met with location-specific procedures. Typically, there is a specific path to take for each type of alarm. Proceed immediately. Take only personal belongings.
- Power failures produce alarms in some devices. Do an orderly shutdown of systems you are authorized to shut down and proceed to the meeting location within the facility. Bring flashlights and personal belongings.
- Computer-related alarms associated with virus detection, firewall conditions, and so forth should be reported to the help desk for disposition when they occur, unless other specific instructions are provided.
- Other alarms should have explicit training associated with them If an unknown alarm is heard, notify your supervisor immediately and follow their instructions.

When alone in a facility, alarms are more of a concern. Take suitable precautions and get trained on how to respond to alarms when you are alone before working under these conditions.

14 Badges and tokens

Badges and access tokens are used to identify people and the places they are allowed to be. They are also used to gain access to

facilities and systems. These badges and tokens are to be used in specific ways and protected in order to protect your safety, your personal items, and the enterprise from situations in which the wrong people are in the wrong places at the wrong time. They also help to make sure that everyone is evacuated from a building in an emergency and for other similar safety purposes. Here are the most important rules:

- Badges must be worn on the outside of clothing, in the front part of the individual, between the waste and neck, and with the picture facing outward at all times when within enterprise facilities.
- If a person has a badge that is not appropriate to the area they are in, you should immediately ask if you can help them, and escort them to an appropriate area where they can be introduced to a security guard or to the front desk.
- Anyone without a visible badge should be treated as not authorized to be present, regardless of whether you know them, and regardless of their attire or appearance.
- If you feel physically threatened by them, leave the area as safely as you can, and call security at your first opportunity.
- If you feel comfortable enough doing so, ask if you can help them, and escort them to the guard station, the nearest member of the guard staff, or the entry and exit desk so they can be properly processed to get a badge if they require one.
- Otherwise, contact security immediately, identify the situation, and make sure that they are escorted out by a badged security officer.

Badges and other related security tokens are vital elements of assuring your safety and the well being of the enterprise. Follow these rules religiously even when you know the person.

15 Tailgating

Some people try to enter an area where they are not permitted by following other people into it. This is called tailgating. Tailgating is

not permitted within our enterprise and if you detect someone trying to tailgate behind you into an area or facility, you should do the following:

- If they tried and failed already, you should immediately report it to security by calling the security guards and, from the safety of the facility, identify the individual who did it.
- If they succeeded and you feel threatened, you should note their appearance and location, find an opportunity to separate yourself from them, and immediately call security to report their location and the nature of what they did.
- If they succeeded and you do not feel threatened, you should ask if you can help them, and escort them to security or the entry desk so they can be properly assisted.
- If they are an employee or someone you know, and if you feel comfortable doing so, you should instruct them to exit the area and enter using their own badge. If they indicate they have forgotten it or any other similar excuse, explain that the guard will provide them with a temporary badge and escort them to the guard station.
- If they are a relative of an employee, like a child, or a spouse, they should be escorted to the security desk so security can locate the employee and provide their child or spouse with an appropriate badge to allow them into authorized locations.

Tailgating is strictly prohibited and there are no exceptions. Even the CEO and board members must wear badges at all times and only the guard force may provide admission and escort to individuals who are not badged and are not otherwise authorized to be within an area.

16 Your passwords and theirs

Passwords are the proof that you are who you claim to be or that you are allowed to do something you want to do. Because passwords allow actions and associate them with individuals,

accountability is lost when passwords are misused or improperly cared for, and this means you could be blamed for something you did not do, or someone could harm the enterprise by claiming to be you. The rules for protecting passwords are as follows:

- Do not tell, show, email, or share your password with anyone ever. This includes systems administrators, your supervisor, the help desk, or anyone else. Nobody but you has any reason to know your passwords, ever.
- Do not allow people to look over your shoulder as you use a password, whether it is for a phone message system, an entranceway, an alarm system, or a computer. If they try to do this explain that they are being impolite and ask them to look away. If they refuse, call the help desk and report it as an incident. Provide the name of the person doing this – it will be on their badge.
- If you see someone using anyone else's password, go to a private location and report it to the help desk. This is a violation of company policy, may be illegal, and it is harmful to whoever's password they stole and used.
- If someone tries to get a password from you, you are required to report it to the help desk immediately unless it places you at personal risk, in which case it must be reported as soon as feasible and safe.
- If someone tries to give you their password, refuse to accept it and indicate to them that this is against the rules.
- The passwords you use at work may not be the same as the passwords you use in other places, or over the Internet at distant sites. Never use enterprise passwords except on enterprise systems.
- Make your passwords hard to guess, long, complicated, and unrelated to anything about you or your work.

17 Polite behaviors

Some people portray security as being impolite or gruff. But it should not be. The security behaviors we describe in this booklet

can be done in a very polite way, and they should always be done this way. For example:

- When you escort someone to the front desk or security, you should be helpful, polite, pleasant, and friendly with them, use a pleasant tone of voice, be respectful, and be as nice as you can be.
- When you tell someone that it is impolite of them to look over your shoulder as you type your password, say it nicely, and perhaps even act a little bit embarrassed that they were not properly trained or brought up as well as you were.
- When you call the help desk, they should be polite to you and you should be polite to them. If someone is having a bad day, your being polite and caring can help them feel better and everyone will be better off.
- When you have to go outside because there is a fire or other alarm, help others on their way out, point out the meeting area, and ask them how their family is doing and about other similar things until the emergency passes.
- If someone gets upset because they forgot their badge at home and you are making them go to get a temporary one for the day, be polite and explain that they know the rules just like you do, and that the work will still be here when they return with their badge.
- If someone acts like another worker did something wrong by reporting a security problem or making them display their badge properly, come to the support of the person who followed the rules. They are protecting your safety by making sure that the workplace is safe for all of us.

Secure and safe behaviors do not have to be mean or oppressive in any way. You are doing yourself and everyone else a favor when you follow the rules and hold others to the same standards.

18 Spam

Spam is the word people use today for unsolicited and unwanted emails. Spam is a big problem because it clogs up email servers

and user systems, takes time and effort to identify and delete, and is sometimes used to carry malicious instructions, software, images, attachments, or unacceptable content. It may also violate other enterprise policies. Since we cannot perfectly stop all spam, we advise our workers to help reduce the amount of spam they get by following these guidelines:

- Don't send spam to others either within the enterprise or elsewhere.
- Don't participate in chain letters at work or send chain letters to anyone at work. If you get a chain letter from anyone at work, don't open any attachments. Report it immediately to the help desk and follow their advice.
- Don't send emails to mailing lists that include everyone at the enterprise or lists with large numbers of people, and don't reply to emails that come from such lists. This tends to create problems for everyone, including you. If you get such an email, and it is not from someone who is supposed to send such things, report it to the help desk.
- Don't use your internal email address or internal mailing list addresses in emails you send outside of the enterprise. This causes spam to come to many more people in the enterprise than they would normally read.
- Don't put internal email addresses on Web sites or other public locations. These locations are farmed by spam companies to get lists of places to send their spam.
- Don't use the remove options on spam you get. Report it to the help desk. When you click on remove, it is often used to verify your address, but when you report to the help desk, they will tell the source to remove all enterprise addresses and refuse further emails.
- When you get spam, click on the email client's spam button to identify it for others in the enterprise and stop the many other copies that will soon arrive.

19 Viruses

Computer viruses are one of the things that comes in email attachments, in programs and other things downloaded from the

Internet, on CD-ROMs, and in various other ways. Completely eliminating computer viruses forever is not feasible, but we can dramatically reduce them by being thoughtful about our work. In particular:

- When you get a virus warning on your computer, unless you have been explicitly instructed by someone in authority at the company to do otherwise:
    - Refuse to use dangerous item (just say no).
    - Contact the help desk and follow their directions.
- If antivirus updates are not automatic on your computer, make sure you do a manual update of your antivirus mechanism at least once per week and more often if you get a notice about a new virus spreading around.
- If you use a computer that is not very susceptible to viruses and you are not required to run antivirus software on it, follow the requirements set for that sort of computer to operate it safely and with greater caution because of the potential for a virus that would not get detected.
- When you get an email from someone you don't know and it has an attachment in it (you can usually tell from your mail client by a paper clip or similar symbol), treat it as if it is a virus and report it to the help desk, or if you prefer, forward it to computer security without opening it, and indicate that it is suspicious email.
- If your computer is acting very slow or seems to be sending or receiving a lot of messages or doing a lot of activity when it normally should not be, try to reboot it. If that doesn't cure the problem, report it to the help desk.

Fighting viruses is a group activity. Your call to the help desk may be one of a thousand they get, and the number of calls received may be the very thing that saves the enterprise from the virus.

20 Spyware and Trojan horses

Spyware is a popular name for a particular kind of Trojan horse software that gets loaded onto your computer and then steals information and sends it to people that try to harm you or all of us

by gaining unauthorized access to content, stealing passwords, or taking other sensitive information. Trojan horses can also corrupt our systems and network, grant access under your name to an attacker, disrupt systems, network, data, or the enterprise as a whole, or cause a wide range of other sorts of harm, including violations of law that could accidentally be blamed on you.

Spyware gets into computers in much the same way as computer viruses, except that it doesn't make copies of itself all on its own like viruses do. Spyware can come in email, in a file you download from the Internet, from visiting malicious Web sites with a browser that is not configured as safely as it might be, by someone breaking into your computer from afar using a weakness in the computer, by someone placing a USB device, CD-ROM, or DVD into your computer, or by getting you to type a command or do other specific actions for them.

This is part of why physical security is important for all of our computers, but it is also another very good reason to only use work computers for work purposes. Very few of the legitimate places we use on the Internet for our work ever have spyware planted on them to break into our computers, and if we find them, we will stop doing business with them. So you can help to reduce spyware and Trojans by following these easy steps:

- Keep your computer properly configured.
- Only go to legitimate business sites.
- Don't accept attachments from strangers.
- Don't let strangers attach devices to your work computer.
- Don't accept unauthorized gift software or CD-ROMs.
- Report strange computer behavior to the help desk.
- Only run company authorized software.
- Only use your work computer for work purposes.

21 Phishing and social engineering

Phishing is a highly publicized name for some recent methods of what is commonly called social engineering. Social engineering is when someone tries to convince you to do something against the

rules or not in your best interest by tricking you into thinking you are doing the right thing.

In these various approaches, a worker will get an email, a phone call, a piece of paper mail, an instant message, a telegram, or any sort of contact that indicates that they should do something, asking for information, or otherwise making a request that could look perfectly legitimate, and even appear to be from a legitimate known sender's email address. When the employee does what they think is right by following directions, filling out a form, or trying to work with the other person, the enterprise gets hurt.

Typical examples include asking for personal information in the context of a fake emergency, asking for user names or passwords, trying to get an account set up for a new executive that has just started or is just about to start, trying to get a remote connection for client, vendor, or business partner access, acting like you are doing computer or machinery maintenance to get access to the building or the network, getting a copy of the company phone book, getting the number or address or email address of another employee, and so forth.

Once the social engineer finds something out they usually leverage it to get more by acting like they are members of the team. They will use the information they get to prove that they are who they claim to be and leverage it even further.

The best way to deal with this is to know what you are and are not allowed to tell to whom and how they are supposed to demonstrate that they are who they claim to be. This is the subject of the privacy, acceptable use, and other similar policies. If you follow the rules and report suspicious behavior to the help desk, you will be doing the right thing.

22 Acceptable use of company computers

Computers at work and computers supplied by the enterprise are for use doing the business of the enterprise. Other uses increase the risks of computer-related problems. Here are the basic rules for what is acceptable use of computers in addition to the rules and processes described in the rest of this booklet:

- Enterprise computers are Federal Interest Computers in the US and are protected by federal laws in most countries we operate within.
- Enterprise computers are FOR AUTHORIZED USE ONLY. Any use or abuse of these systems not explicitly authorized is unauthorized.
- You have no expectation of privacy when you use enterprise computers. We regularly monitor all input, content, and output of our computers and reserve the right to do anything legal with any of the information we gather.
- You are authorized to use enterprise computers for the sole purpose of doing your work for us and that work must be work that we ask you to do as part of your job assignments.
- You may use enterprise computers for communicating with immediate family members or significant others about matters like when you will be home, the hotel you are staying at, contact information, and so forth, but only when this is a departure from your normal day-to-day activities or in a rare and serious family emergency.
- We may respond automatically and/or manually to any and all detected attempts to violate any of the provisions of company policy, violation of law, or other acts we consider suspicious in any way. This response may, at our sole discretion, range over the entire set of legal actions.
- Failure to follow the rules may result in sanctions up to and including termination of work relationships and the initiation of legal proceedings against you.

23 Your privacy and the privacy of others

Our enterprise values the privacy of your personal data and that of others For that reason, personal data is only to be handled by systems and using procedures specifically designed for that purpose. Any placement of your personal data or that of others anywhere not specifically designed for that purpose is not permitted.

We have a policy of being allowed to monitor anything that happens within our environment so long as that monitoring is permitted by law. As a condition of your work for us, we require that you grant us these rights to the maximum extent permitted by law. This includes telephone calls, electronic communications, the use of your cellular telephone within our facilities, anything that contacts or passes into or through our equipment anywhere it may be. and the collection of keystrokes, mouse movements, sounds, pictures, smells, and/or any other Information we can legally collect, anywhere on our site.

While we are allowed to do this, we don't always do it everywhere we can. But at our sole discretion, we may do it anywhere we can and at any time or for any length of time. When we do this, we only do it for legitimate business purposes, the workers who do this are specifically trained in what they are allowed to do and not allowed to do, they are properly supervised, and their actions and decisions are recorded and analyzed to assure that this requirement for safety and security is not abused.

We fully expect that your privacy and security will be balanced by this process and we expect that you will respect the privacy of others as you hope they respect your privacy. Do not disrespect others by violating their privacy, by selling or leaking their information, by looking at information out of interest or curiosity, or by retaining information after its purpose no longer exists. Private information about individuals is for business use only and only for the legitimate purposes it was collected and stored for.

24 Protected health information

Among the private information that is sensitive and protected by laws all over the world, is protected health information. Special requirements apply to this information and anyone who is allowed access to it. Everyone shares in the responsibilities identified here:

- You may not access information about individuals and any medical condition, testing, treatment, prescriptions, medical billing information, names of their doctors, or anything else that might in any way reveal information about their medical or health related condition unless that information is necessary in order to perform your job.
- Examples where this information may be required include but are not limited to;
    - in a medical emergency to save the person's life;
    - in decisions about work where there are medical requirements associated with the job or location;
- In cases where this information must be used or provided, it may only be used or provided to those who need to know it and the process must reveal as little as possible about the individual while still meeting the health, safety, and work requirements.
- All protected health information must be labeled as such and protected suitable to the requirements of legal, regulatory, and business requirements.
- Access is restricted to only those who have a legitimate job requirement for access, that access is logged in detail, and those individuals are held responsible for their actions in periodic reviews.
- Individuals with access to health information must have proper background checks before being granted access.
- If you encounter this information in any other context, contact security immediately to identify the situation, remain there to protect the information until relief arrives, and inform your supervisor in writing of what took place.
- Health information is released ONLY after it is legally mandated or pursuant to a request by the individual.

25 Protected financial information

Financial information such as retirement funds, pay rates, health care program fees, deductible levels, banking information, account information, government financial forms, tax information, taxpayer identification information, and all other individual or corporate financial information is also highly sensitive and protected under the laws of most countries and the policy of our enterprise. Special requirements apply to this information and anyone who is allowed access to it. Everyone shares in some responsibilities and they are identified here:

- You may not access financial information about any other individual unless you need it to do your job.
- In cases where this information must be used or provided, it may only be used or provided to those who need to know it to perform the necessary function.
- All protected financial information must be labeled as such and specially protected to meet legal, regulatory, and business requirements for its protection.
- Access is restricted to only those who have a legitimate job requirement for access, that access is logged in detail, and those individuals are held responsible for their actions in periodic reviews.
- If you encounter this information in any other context, contact security immediately to identify the situation, remain there to protect the information until relief arrives, and inform your supervisor in writing of what took place.
- You may not share your salary or other compensation information with other workers or try to get them to reveal their information to you.
- After this information is no longer required by law or regulation, it must be destroyed using proper disposal methods.
- This information may only be released to authorities upon presentation of proper legal mandate and the enterprise will seek all legal remedies to protect against its release.

26 Company confidential information

Our enterprise also has other information that is confidential. For example, business plans, pricing information, bids for contracts prior to completion and public release, marketing information prior to its release, personal contact information on clients, customers, vendors, and media, spreadsheets used to make business decisions, and other similar information that is protected to help assure success and maintain an edge in the competitive environment. This information must be protected in order to assure that the enterprise stays operating and you still have your job tomorrow. The rules for this sort of information include:

- You may only access company confidential information that you need to do your job.
- Company confidential information must be labeled as such and be kept in a place that is authorized to store it.
- If you encounter this information in any other place, contact security immediately to identify the situation. Inform your supervisor in writing of what took place.
- You may not share this sort of information with anyone outside of the enterprise or with other workers who don't need it to do their jobs.
- You must use reasonable and prudent measures to assure that this information is properly labeled and protected, including following all the rules associated with the specific information and its use.
- For mergers and acquisitions information or financial reporting information, only very limited sets of people are authorized to access the information.
    - It must be properly labeled and segregated so that only those team members with authorized access can gain access.
    - If you see information with special labels, report it to security immediately, remain with it until relieved, and report it to your supervisor in writing.

27 3rd party confidential information

Some of the information we keep at our enterprise belongs to other enterprises or individuals. Because we don't own this information, it has to be specially protected according to the terms of the contracts we have with these 3rd parties. This includes copyrights, 3rd party sensitive content, licensed content, and all manner of other things.

Since each 3rd party may have different contractual relationships with us and release of this information may be damaging to us financially or in terms of reputation, this information is also specially protected. The rules for 3rd party information are:

- Only people authorized to access the specific 3rd party information may access it.
    - If you don't know you are authorized you aren't.
- Access to 3rd party information comes with details on how you are allowed to use it, restrictions on its use, and so forth. You need to follow all of the specific requirements for each 3rd party information type you use.
- 3rd party information that has control requirements must be labeled as such.
    - If you don't see a label, it is not controlled.
- If you do see a label and you are not authorized to use the information, don't use it.
    - Report its presence to security so they can secure it properly.
    - Write a memo to your supervisor identifying what happened and what you did.
- If you come across something you think is 3rd party information that is not labeled as such, report it to your supervisor.
- If you aren't sure, err on the side of caution.

28 Trade secrets

Trade secrets are specially protected confidential information that must be kept secret to retain a business advantage over competitors. Trade secrets must be:

- Things that nobody else knows.
- Rare and specific to a specific advantage.
- Labeled as trade secret.
- Protected so that access is in fact limited.
- Tracked so that every copy is known.
- Accounted for so that every person granted access is identified and the period of their possession is listed.

Unless you have access to trade secrets and have been trained in their use, you should never encounter it. If you see something labeled Trade Secret and you don't have authorized access to it:

- Don't look at the contents.
- Cover it with something so nobody else can see it.
- Immediately call security and identify it to them.
- Remain there until security comes to secure it.
- Report what you did to your supervisor in writing.

Trade secrets lose their legal protection if they get out. If you know a trade secret:

- Don't tell anyone else about it unless they are authorized to know it.
- Unless you know they are authorized by the trade secret authorization process you must assume that they are not authorized.
- If anyone asks you about a trade secret and they are not authorized, do not tell them. Report them to security.

29 Classified content

Classified information is specially protected government information that has government-specified protection requirements. If you have access to classified Information, you will be briefed on special control requirements associated with that content and the systems that access it.

If you see anything marked as CLASSIFIED, SECRET, TOP SECRET, or with a similar marking, and if you are not authorized to access it:

- Immediately place something over top of it:
  - Do not read it.
  - Do not let others read it.
- If you are near a phone:
  - Contact security to come and get it.
  - Wait for a security guard to come and secure it.
- If you are not near a phone and there is a lot of it:
  - Secure the area.
  - Go immediately to a location with a phone.
  - Contact security to come get the content.
  - Return to the location and wait for the guard to get it.
- Otherwise, take the material to the nearest security guard.

30 Patents

Patents are published processes, combinations of matter, or means and methods that enable someone who is normally skilled in the art of the day in the technical field of the patent to do something useful that they could not have done if the patent had not been disclosed. Patents grant the enterprise the right to charge other people for use of the patented art.

- There is no need to protect the patent itself after the invention is disclosed as part of the patent process.
- Prior to patent, the art should be kept strictly confidential.
- Most notes on what is done in terms of inventions while at work may become the subject of patents at a later time, so it should be protected until determined not to be of import.
- If you are using patented art in your work and the patent belongs to someone outside of the enterprise, you need to make sure you have a license to use it. This can be understood through contact with the legal department.
- Do not use patented work of others unless it is licensed to the enterprise.

31 Copyrights

Copyrights restrict the right to make copies and require that a fee be paid to the copyright owner or licensee for each copy made.

There are two types of copyrights that are important to the information protection process; ours and theirs. Our copyrighted material is valuable because we may be able to charge people to make copies of it. Theirs is important because we need to make sure we pay for every copy we have or make. Here are the basic rules:

- Don't make copies of copyrighted material unless the copyright is owned by the enterprise or a fee has been paid in advance for every copy you make.
- Don't store unauthorized or non-licensed copies on your computer, your disks, tapes, paper, or on any other media you use or are in charge of at the enterprise.
- These rules apply to:
    - Music
    - Videos
    - Pictures
    - Books
    - Booklets
    - This booklet!
    - Any information put into any tangible form
    - Computer programs
    - Computer games
    - Operating systems, libraries, and downloads
    - Copies of information from Web sites
- Exceptions include:
    - One fair use copy made of a small portion of an overall work for reference purposes
    - Government documents which are not copyrighted
    - Works for which you have the author's permission
    - Backups of software authorized to be on your enterprise computers.

32 What you send in emails

You are responsible for what gets sent in emails. There are certain things you may not send in emails and other things you should not send in emails. You must not send:

- Sensitive, proprietary, confidential, 3rd party, financial, health, trade secrets, classified, or copyrighted materials or other similar content in emails unless they are encrypted with an enterprise approved encryption system for that type of content and sent only to properly authorized recipients.
- Information that could do harm to others if delivered or intercepted in transit.
- Contraband content that is illegal in any jurisdiction the email might pass through.
- Encrypted email to or passing through China or France.
- Spam or other unauthorized bulk email.
- Email not for enterprise purposes, except as explicitly authorized by enterprise policy.

You should not send:

- Things that make you or the enterprise look bad or that might be misinterpreted.
- Any emails when you are angry or upset.
- Emails without spelling checked and corrected.
- Emails that could reveal information about you that you wouldn't want published in the front page of the newspaper.
- High volumes of email or large email attachments.
- Email with jokes or other similar information that might be misinterpreted in the wrong context.
- Information that is negative about the enterprise.

Email is not private and once you push the send button, the email is gone – so remember:

THINK BEFORE YOU PRESS SEND

33 What you say on the phone

We use the telephone for many critical communications and for that reason, we need to make sure we get the full value out of this media while understanding the risks in its use.

- Listening in on or recording telephone conversations is illegal in many places, but there are some cases in which this can happen.
- You should not listen in on other peoples' phone calls or record them.
- If the enterprise or law enforcement wishes to listen to or record conversations, it may, under certain circumstances, and you should assume that your calls may be recorded.
- You have no expectation of privacy when you use the telephone at work, including your personal cellular telephone.
- When you use telephone systems, conference calling services, voice over Internet Protocol (VoIP) services, or computer-based conference systems, calls may be recorded, in some cases without notice.
- Telephones should not be used to exchange highly sensitive data, like trade secrets, that require special protection.
- Do not trust that the person on the other side of a phone call is who they claim to be unless you have some authentication that they are who they claim to be. Many people use telephone calls to act like they are someone else in order to get workers to do the wrong thing or to get sensitive data.
- On phones with caller identity functions, when you can determine that the caller is calling from the number they normally call from, and when you know the caller by voice from previous in-person conversations with them, you can be pretty sure they are who you think they are.

The telephone is a critical business tool, but you should be aware that it can be abused and be careful what you use it for.

34 Using the Internet

The Internet, a reflection of the rest of the world, has its good neighborhoods and its bad neighborhoods. Stay in the safer neighborhoods and you and the enterprise will be safer. Here are some key tips to staying safe on the Internet:

- Only use our computers and networks for our legitimate business purposes.
- Don't use search engines to look up sensitive topics because the search engine owners may sell the details of what you were looking for.
- Don't send sensitive information over the Internet unless it is encrypted with an enterprise approved encryption method and system.
- Assume that the information you find over the Internet is wrong unless it comes from a source you know to be of high integrity and knowledge in the area of interest.
- The Internet is full or rumors, deceptions, frauds, spies, and lies. Only trust it for business exchanges with sources you have good reason to believe are legitimate.
- Don't provide personal information, debit cards, phone numbers, addresses, email addresses, or other similar information to Internet sites except for legitimate business purposes and with approved trading partners.
- Don't load computer programs from the Internet to run on your work computer unless instructed to do so by an authorized enterprise representative. This should rarely happen.
- You may not do stock trading or other personal business transactions using enterprise computers.

The Internet has a lot of interesting things, fun things to do, interesting places to visit, and enjoyable games, toys, and people that are not related to work. We certainly hope you enjoy them, but you may only do so from home on your own time, not at work or using enterprise computer systems or networks.

35 What you FAX and where you FAX it

Facsimile (FAX) machines immediately send documents to remote locations. This is a tremendous business advantage because it saves a lot of time and money over alternatives. But there are some common errors made with FAX machines that can also be big problems for the enterprise. Here are some guidelines:

- Check the number before you FAX! Many cases have been reported in the news of a company sending a FAX that went to the wrong place, like a newspaper or a competitor, instead of the correct recipient.
- FAX machines have the same issues as telephone calls, because they use the same underlying systems. The same rules apply.
- Never FAX highly sensitive information except to internal enterprise FAX machines specifically authorized for that specific information when there is an authorized person at the other end waiting at the FAX machine for the information to arrive.

36 Testing security

The information security people at our enterprise have specific responsibility for testing information security, and they are the ONLY people who are authorized to do so.

- DO NOT test security unless you are explicitly authorized to do so. It can be dangerous to you and the enterprise.
- It is often illegal to test security, it is certainly against the rules, and it is grounds for immediate termination of your work for the enterprise.
- If you accidentally encounter what you think to be a security problem, notify the help desk or the security office, but do not explore it further or try to prove it one way or the other.

37 Use of enterprise financial instruments

There are specific rules associated with the use of financial instruments (credit cards, purchase orders, contracts, electronic funds transfers, and other enterprise financial mechanisms and processes). The information security aspects of those rules are covered briefly here. If you are authorized to act in a financial way for the enterprise, you will receive additional briefings on the details of your uses, however these general rules apply:

- You may only use enterprise financial instruments to transact authorized enterprise business.
- You are personally responsible for unauthorized use of enterprise financial instruments you are authorized to use.
- Do not use enterprise financial instruments to violate any enterprise policy, procedure, or process. Just because you have access to make decisions about the use of enterprise monies does not mean you are allowed to break the rules.
- The use of enterprise financial instruments subjects you to a wide variety of laws and regulations, some of which carry fines or criminal jail sentences if violated. We provide training in the aspects of these laws and regulations we think are most relevant to you and your job, however, ignorance of the law is no excuse.
- If you lose or improperly or accidentally reveal information or instruments such as credit or debit card numbers, credit or debit cards, unprinted or unwritten checks or check stock, stock certificates, bank notes, bank account numbers, or other similar financial instruments or related information, immediately contact the help desk so that they can help prevent any losses that may result and help walk you through the procedures to try to limit any losses.
- Intentional improper use of any enterprise financial instrument or system will almost certainly result in immediate termination and both civil and criminal prosecution under all applicable laws. Don't do it!

38 Least privilege

Our system of controls is designed to try to give workers as little access as we can while still allowing them to do their jobs efficiently. This is called the principle of least privilege. But unfortunately, our desire to use least privilege is not always met by the technology or mechanisms we are able to cost effectively put in place. For that reason we also have rules about privileges and duties:

- Just because you seem to have a privilege does not mean you are allowed to use it. If you appear to have a privilege that you think you should not have:
    - Report it to the help desk
    - Don't use it or test it, just leave it alone
    - Don't tell others about it
    - Don't expect it to be fixed right away
- If you don't have a privilege you think you need to get your job done:
    - Request it from your supervisor
    - Don't try to get around the protections just because you can find a way to do it
    - Ask permission to do it rather than forgiveness for having improperly done it
- In an emergency situation, or what you believe to be an emergency situation, do not try to bypass protections. Report the emergency to the help desk so that an authorized person can act on the emergency in a safe manner.

Many people view these sorts of privileges as granting status or as points of pride, but those who have more and more privileges often find that they also have more and more responsibilities that go with those privileges and that they ultimately become burdens. Keep in mind that the reason you have these privileges is so you can do work for the enterprise, and more privileges usually means more work, but not necessarily more pay.

39 Separation of duties

When there are important issues at stake for the enterprise, the costs and consequences of mistakes or malicious acts can be very high. In these cases, the duties associated with carrying out critical business functions are separated among more than one person and/or system so that any single individual cannot do more than a certain amount of harm. This is called separation of duties. Examples you are likely to encounter include:

- Workers identify the hours they have worked

    - Supervisors approve of those hours
- Purchase orders are written by the purchasing process
    - But they are only honored by accounts payable
- Auditors can come and review systems and accounts
    - But auditors can't make any changes to them

When you find a situation where there are separations of duties, it may appear at first that the system is terribly inefficient. It takes 3 people to screw in a light bulb; one to request it, one to approve it, and one to actually screw it in. This is just part of the price we pay for making sure that we don't waste light bulbs. Here are some important rules with regard to separation of duties:

- Don't try to bypass the separation of duties requirements. If you get caught you may be subject to criminal and/or civil prosecution and you will likely be terminated from further work.
- Don't forge someone else's signature, like signing your the name of your boss to a document because your boss is out of town. Go to their boss, and on up the food chain till you get to an authorized authorizer. If it isn't important enough to bother whoever is available, let it wait until the normal approver is available.
- There is rarely if ever a situation so urgent that it is worth disturbing the normal operation of the enterprise to get some piece of paperwork done. When it is, make sure your supervisor is the one doing it and not you.

40 Frauds against you and the company

Criminals sometimes use enterprise information and/or systems to perpetrate frauds. There are many different methods of carrying out frauds, ranging from tricking workers into making purchases of supplies that they don't need to tricking financial systems into losing track of critical financial data. They may even take your personal information from the company and use it to defraud you. While we cannot tell you all of the possible ways they may do bad things, we have some basic advice for how to avoid them and what to do about them:

- **JDLR - It Just Doesn't Look Right:** Sometimes things just don't look or seem right to you. When this happens, it is time to report what is happening to your supervisor.
- **It's unusual or out of the ordinary:** When extraordinary things are requested of you that seem to fly in the face of normal work rules or procedures, you should always follow procedures laid out by the enterprise rather than getting too creative. Be considerate, polite, and helpful, but follow the rules.
- **You are asked to violate a rule:** Sometimes you may be simply asked to not follow some rule as a personal favor or out of kindness and consideration for the unusual circumstance. Don't do it, take notes on what was asked and by whom, and report it to your supervisor.
- **Your supervisor asks you to violate the rules:** If it is requested by your supervisor, document it carefully and explain that it is against the rules. If told to override the rules by your supervisor and if the action is not illegal, immoral, or unethical, and if you are comfortable doing it, document the supervisor override in writing, send a copy to your supervisor and their supervisor, and do what your supervisor told you to do.
- **You don't feel comfortable about it:** If you don't feel comfortable about it, don't do it. Document the request, identify the circumstances, and report it to your supervisor and their supervisor.

41 Contraband

Certain information is not permitted in the workplace. This may be for legal reasons, because of local regulations, because of the potential for law suits, because it is inappropriate in a business context, because or relationships with vendors or clients, because of possible negative publicity, or because the management simply decided that it was not something they wanted in the enterprise. The following are examples of contraband:

- Pornography, depictions of scantily clad people, animals having sex, dead bodies, violent acts, crimes being committed, bodily functions, and other graphic depictions of things that may be offensive to others are prohibited.
- Loud and disruptive music that effects work, scratching sounds, or sounds that bother other workers are not permitted unless they are necessary in order to accomplish the work underway.
- Subsonic or ultrasonic sounds, shaking, and similar disturbing sonic mechanisms are also not permitted.
- Unauthorized or unpaid for copies of music, videos, CDs, DVDs, tapes, talks, slides, or other similar intellectual property or mechanisms that store or provide them are not permitted.

The rules on contraband are pretty simple:

- Don't bring it into, produce it in, keep it in, or leave it in the workplace or enterprise facilities.
- If you find it, identify it to management immediately and ask to have it removed.
- If you believe it is illegal, also contact security and identify the legal issue so they can come and deal with it.
- Document what you saw and did and provide the documentation to your supervisor.

You are not being impolite when you tell others not to do things that disturb you. They are impolite to not be considerate of your needs.

42 Portable electronic devices

Many workers have enterprise-provided personal data assistants, cell phones, pagers, blackberries, iPods, laptops, or other similar devices. These hand held computers often have capabilities similar to other computers in the workplace and need to be treated in most ways like other computers, however, because they are so mobile and so easily lost, there are some special precautions to take:

- The device must not be used to store confidential company information unless that specific information is authorized for your mobile use. Examples of special authorizations include:
    - Customer lists for sales staff, which is restricted to the data needed by the specific sales person.
    - Contact information for people on the road to be able to get in touch with co-workers. This should not include a complete company directory.
- The device may be used as a pathway into the enterprise, so it must be kept with you or under your control at all times, with a few exceptions:
    - At airports or other mandatory security searches, it may be placed in your purse, brief case, or security bin to go through the screening process.
    - At hotels you may leave it in your locked hotel room with your other equipment when you go out to do other things, but it must be turned off.
    - At home it can be placed with your other valuables such as your watch, work-related papers, and so forth.
    - It can be kept locking in your car trunk but you may not leave it in your car or in a meeting room or in other places when you leave those locations.
- The device and its content is valuable and if lost, left, or stolen it must be immediately reported to computer security or the help desk. This will, among other things, allow it to be disabled from exploitation by others and tracked for recovery purposes.

43 On the road and at home

When you are on the road or at home, if you are using enterprise computers or information or working remotely, there are specific rules you need to follow to assure that protection remains effective.

- You need to maintain an appropriate level of physical security and control over enterprise information and

devices to make up for the lack of other physical security controls normally in place in the work place.

- You need to follow all work rules in the same way you would have to if you were at work. Just because you are on the road or at home, doesn't mean you can risk your health or safety or put the enterprise at risk.
- You need to be careful not to lose devices by maintaining control over them, following the same requirements as those required for mobile devices.
- You need to obey all of the local laws and ordinances, including traffic laws. This includes your travel to and from work.
- You need to protect information assets of the enterprise from accidental misuse by your children, spouse, significant other, visitors, and guests. This means that they may not use enterprise accounts, devices, papers, or systems for any reason.
- When the normal procedure indicates that you are supposed to call security or the help desk, document an incident, or contact management, these requirements are unchanged by your location.
- When requirements indicate you should leave an area, take portable computers and similar devices with you when you evacuate an area while on the road or at home, unless doing so endangers you, in which case you should balance your actions in favor of your own safety. Protect what you can of enterprise assets without putting yourself at increased risk for harm.

44 Other rules, policies, and requirements

This awareness booklet is not the complete set of rules, requirements, and issues that you will need to know about during your work, but it is a helpful reference to the most common issues that come up.

After you are briefed and trained on issues in all or part of this booklet, you need to pass a test to make sure that you recognize and understand these requirements and know how to do your job

properly. The exam included in this booklet is a sample that you can practice on. All of the answers are found within this booklet, but you might have to dig a bit or think about it.

- Keep this book at your desk or with other work materials so you can reference it if you have any questions or if you encounter anything that you are unsure about.

- If you lose this booklet, contact the help desk or your supervisor for another copy. If you have any questions about anything in this booklet, contact your supervisor or the help desk, or ask the person who did the training associated with the information in this booklet.

- You should also make sure that you are aware of other enterprise policies, standards, procedures, requirements, or other things associated with your work so that you can follow all of the applicable rules and requirements of your work and work safely and securely in your own and the enterprise's best interest.

If you have any questions about this booklet not related to the enterprise you work at, if you want to purchase additional copies of the generic version, or if you want to build a custom version of this booklet for your enterprise or group within the enterprise, please don't hesitate to contact the publisher directly.

45 Sample exam

1: You are on the phone with one of your best clients and they ask if you can help them out by expediting them getting a copy of a document that they are not supposed to have. You should:


Give them a courtesy copy to help get the next order.


Tell them that it is inappropriate for them to ask for this.


Tell them that you don't have authorization to do this and get them in touch with someone who does.

- Tell them that you will ask permission internally and politely tell them that the answer was no when the time comes.

2: A dangerous looking stranger enters the workplace with a long trench coat on and not wearing a badge. You should:

- Physically stop them from proceeding and throw them out
- Politely encounter them and ask if you can help them
- Get to a safe place and call security
- Ignore the stranger and continue working

3: Someone who you think you recognize enters your work area, but you don't see a badge on them. You politely approach them and ask if you can help them in any way. They say that they are fine and don't need any help and continue walking down the hallway looking like they know where they are going. You should:

- Politely explain to them that because they don't have a badge on, you are required to escort them to security or the front desk so they can get properly badged.
- Let them go, call security, and ask them to come and deal with the individual.
- Let them be, they obviously belong here and you are only interfering with their work and yours.
- Escort them everywhere they go and ask someone else to call security.

4: You get a call from someone who indicates that they are the secretary for a board member and that they were referred to you by the secretary of the CEO as the right person to contact for an electronic copy of the company phone book required for a study being done by the Board. You are indeed the right person to do this. They provide the name of the board member they work for when you ask for it, and this person is indeed on the board of directors. You contact the CEO's secretary and confirm that they told this person that you were the proper contact for this information. They tell you to email the electronic phone book to their email address, which is an external email address. You should:

- Email them the phone book.

- Explain that the phone book may not be emailed outside of the enterprise ands that you will have a CD-ROM with this information mailed to the board member's home address.
- Explain that in order to get this information you need to get permission from the security department and get their contact details so security can call them back.
- Tell them that you don't think they work for this board member and that you are going to report this call to security.

5: You are on the road and after a plane ride, cab ride, and hotel check-in, you get to your room and discover that you cannot find your PDA. You should:

- Immediately call the help desk to notify them of the lost PDA so they can cut off further access and then look further for it.
- Call the cab company and airline, and wait until you get responses from them before notifying the help desk.
- Wait till you get back to work and buy a new PDA to replace the lost one.
- It has your name and address on it, so whoever finds it will likely call you to get it back to you. Just wait for them to do it and don't panic.

6: