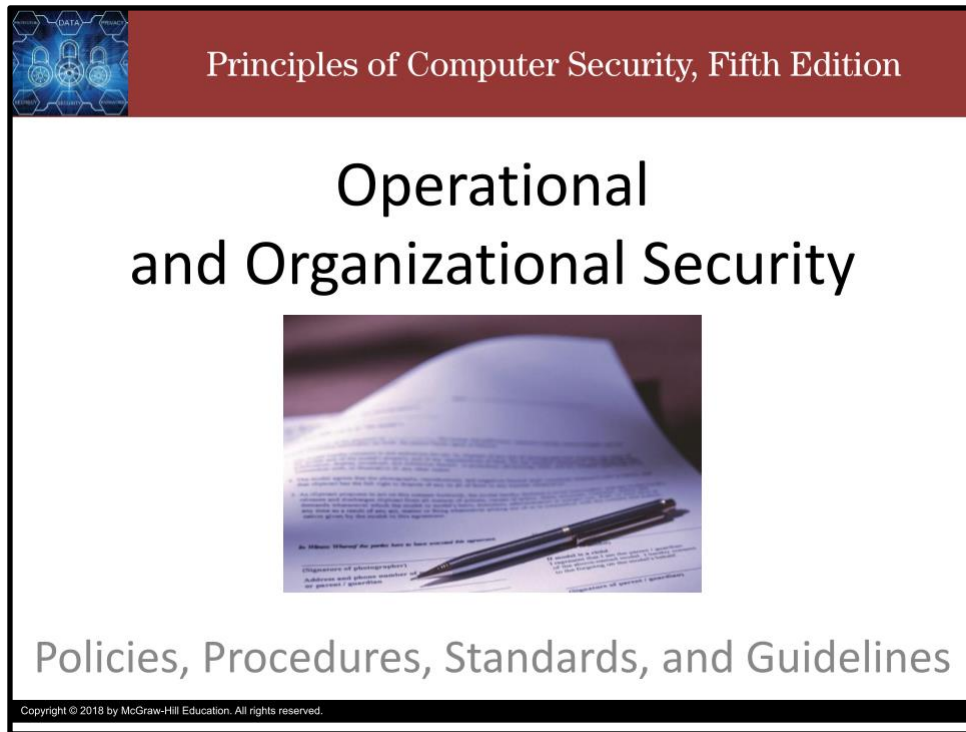



# Operational and Organizational Security: Policies, Procedures, Standards, and Guidelines

Slide 1



The image shows the front cover of the book 'Principles of Computer Security, Fifth Edition'. The cover has a dark red header with the title 'Principles of Computer Security, Fifth Edition' in white. Below the header, the main title 'Operational and Organizational Security' is centered in a large, black, sans-serif font. Underneath the main title is a photograph of an open document with a pen resting on it. At the bottom of the cover, the subtitle 'Policies, Procedures, Standards, and Guidelines' is written in a smaller, grey font. In the top left corner, there is a small graphic with the word 'DATA' and some icons. At the very bottom, there is a small copyright notice: 'Copyright © 2018 by McGraw-Hill Education. All rights reserved.'

Howdy! In this video, we discuss policies, procedures, standards, and guidelines for security.



Principles of Computer Security, Fifth Edition

## Policies, Procedures, Standards, and Guidelines

- **Policies** – high-level, broad statements of what the organization wants to accomplish
- **Procedures** – step-by-step instructions on how to implement policies in the organization
- **Standards** – mandatory elements regarding the implementation of a policy
- **Guidelines** – recommendations relating to a policy

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An important part of any organization's approach to implementing security are the policies, procedures, standards, and guidelines that are established to detail what users and administrators should be doing to maintain the security of the systems and network. Collectively, these documents provide the guidance needed to determine how security will be implemented in the organization.

Policies are high-level, broad statements of what the organization wants to accomplish.

Policies are made by management when laying out the organization's position on some issue.

Procedures are step-by-step instructions on how to implement policies in the organization.

Procedures describe exactly how employees are expected to act in a given situation or how to accomplish a specific task.


Standards are mandatory elements regarding the implementation of a policy.

Standards are accepted specifications providing specific details on how a policy is to be enforced.

Guidelines are recommendations relating to a policy.

The key word here is "recommendations".

Guidelines are not mandatory.



Principles of Computer Security, Fifth Edition

## Standard Operating Procedures (SOPs)

- Procedures – step-by-step instructions on how to implement policies
- Standards – mandatory elements regarding the implementation of a policy
- SOPs – **Standard (Operating) Procedures**
  - **Mandatory step-by-step instructions** set by the organization so that **in the performance of their duties**, employees will **meet the stated security objectives of the organization**.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Procedures are step-by-step instructions on how to implement policies.


Standards are mandatory elements regarding the implementation of a policy.

Some standards come from outside the organization, such as financial regulations.

Others are set by the organization itself to meet its own security goals.

This is what a Standard Operating Procedure is.

It provides clear instructions for what employees should do and the degree to which they should do them.



Principles of Computer Security, Fifth Edition

### Four steps of the policy lifecycle

1. Plan for security in your organization.
  - Develop the policies, procedures, and guidelines
2. Implement the plans.
  - Includes an instruction period
3. Monitor the implementation.
  - Ensure effectiveness
4. Evaluate the effectiveness.
  - *Vulnerability assessment and penetration test*

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Just as the network itself constantly changes, the policies, procedures, standards, and guidelines should be included in living documents that are periodically evaluated and changed as necessary. The constant monitoring of the network and the periodic review of the relevant documents are part of the process that is the operational model. When applied to policies, this process results in what is known as the policy lifecycle.

The first step is to plan for security in your organization.

The prerequisite for this step is to understand the security requirements.

The product of this step are a set of policies, procedures, and guidelines.

The next step is to implement the plans (the policies, procedures, and guidelines).

This necessarily includes an instruction period where everyone must learn the plan.

The third step is to monitor the implementation in order to ensure effectiveness.

The fourth step is to evaluate the effectiveness.

There are many tools for doing this evaluation.

Two common tools are vulnerability assessments and penetration testing.

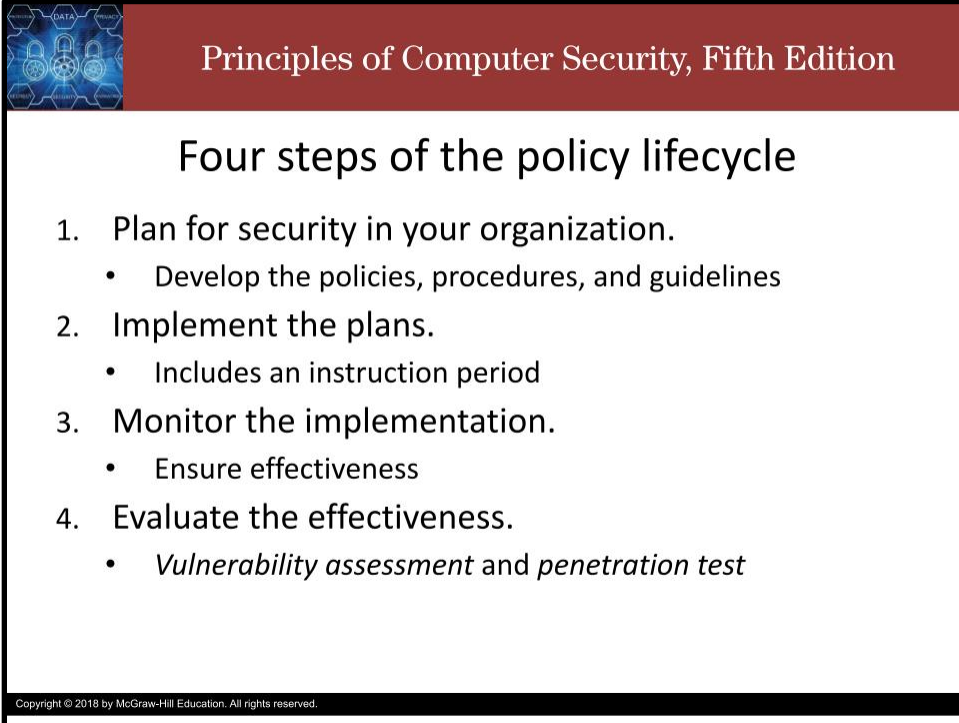
A vulnerability assessment is an attempt to identify and prioritize the list of vulnerabilities within a system or network.

A penetration test is a method to check the security of a system by simulating an attack by a malicious individual to ensure the security is adequate.

Many different methods of evaluation should be combined to get a complete picture of the organization's security posture.

After reviewing the evaluation, the lifecycle repeats from step 1, making adjustments to the plan to continually maintain and improve the security posture.

## Slide 5



Principles of Computer Security, Fifth Edition

### Four steps of the policy lifecycle

1. Plan for security in your organization.
  - Develop the policies, procedures, and guidelines
2. Implement the plans.
  - Includes an instruction period
3. Monitor the implementation.
  - Ensure effectiveness
4. Evaluate the effectiveness.
  - *Vulnerability assessment and penetration test*


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A security policy is a high-level statement produced by senior management

It outlines both what security means to the organization and the organization's goals for security.

The main security policy can be broken down into additional policies covering specific topics.

The security policy should include other policies, including change management, data policies, and human resources policies.



Principles of Computer Security, Fifth Edition

## Change Management Policy

- *Change management* ensures proper procedures followed when modifications to the IT infrastructure are made.
  - Modifications prompted by a number of different events
- “Management” □ process controlled in some systematic way.
- Change management process includes various stages:
  - Request change, review and approve process, examine consequences, implement change, document process

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Change management ensures proper procedures are followed when modifications to the IT infrastructure are made.

Modifications can be prompted by a number of different events, including new laws or regulations, updated versions of software or hardware, implementation of new software or hardware, or improvements to the infrastructure.

The word “management” in the name implies that process controlled in some systematic way.

A change management process should include various stages, including a method to request a change to the infrastructure, a review and approval process for the request, an examination of the consequences of the change, resolution (or mitigation) of any detrimental effects the change might incur, implementation of the change, and documentation of the process as it related to the change.

## Slide 7



Principles of Computer Security, Fifth Edition

### Data Policies

- Data Ownership – Who owns the data?
- Unauthorized Data Sharing – What can be shared?
- Data Backups – What? How often? Where? etc.
- Classification of Information – Levels? Handling?
- Data Labeling, Handling, and Disposal
- Need to Know – Least privilege
- Disposal and Destruction Policy

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Data can be shared for the purpose of processing or storage.

Control over data is a significant issue in third-party relationships.

There are many questions that need to be addressed.

A good way to address them is through policy.

Data requires an owner.

Data ownership is a business function and data ownership roles for all data elements need to be defined in the business.

Requirements for security, privacy, retention, and other business functions must be established.

Not all data requires the same handling restrictions, but all data requires that this kind of information be defined.

Defining it is the responsibility of the data owner.

Unauthorized data sharing can be a significant issue, and in today's world, data has value and is frequently used for secondary purposes.

Ensuring that all parties in the relationship understand the data-sharing requirements is an important prerequisite.

Ensuring that all parties understand the security requirements of shared data is also important.

Data ownership requirements include backup responsibilities.

Data backup requirements involve determining level of backup, restore objectives, and level of protection requirements.

They can be defined by the data owner and then executed by operational IT personnel

Determining the backup responsibilities and developing the necessary operational procedures to ensure that adequate backups occur are important security elements.

Classification of information is needed due of differences in importance or sensitivity of data

Factors affecting information classification include the value to the organization, age, and laws or regulations governing protection.

The most widely known classification system is the Confidential, Secret, and Top Secret categories used by the U.S. government and military.

Businesses might use classifications like Publicly Releasable, Proprietary, Company Confidential, and For Internal Use Only

Data labeling enables an understanding of level of protection required.

For data inside an information-processing system, protections should be designed into the system

Data outside the system require other means of protection.

Training ensures that labeling occurs and is used and followed.

This is important for users whose roles are impacted by the material, and particularly so for proper data handling and disposal

Need to know goes hand-in-hand with least privilege.

The guiding factor is that each individual is supplied the absolute minimum amount of information and privileges needed to perform their work.

That is, access requires a justified need to know.

A data policy should spell out these two principles.

It should also specify who in the organization can grant access to information and who can assign privileges to employees.

Many potential intruders have learned the value of dumpster diving. An organization must be concerned about not only paper trash and discarded objects, but also the information stored on discarded objects such as computers. Several government organizations have been embarrassed when old computers sold to salvagers proved to contain sensitive documents on their hard drives. It is critical for every organization to have a strong disposal and destruction policy and related procedures.

For example:

Important papers should be shredded.

Delete all files and overwrite data on magnetic storage media before discarding.

Possibly destroy data magnetically using a strong magnetic field to degauss the media.

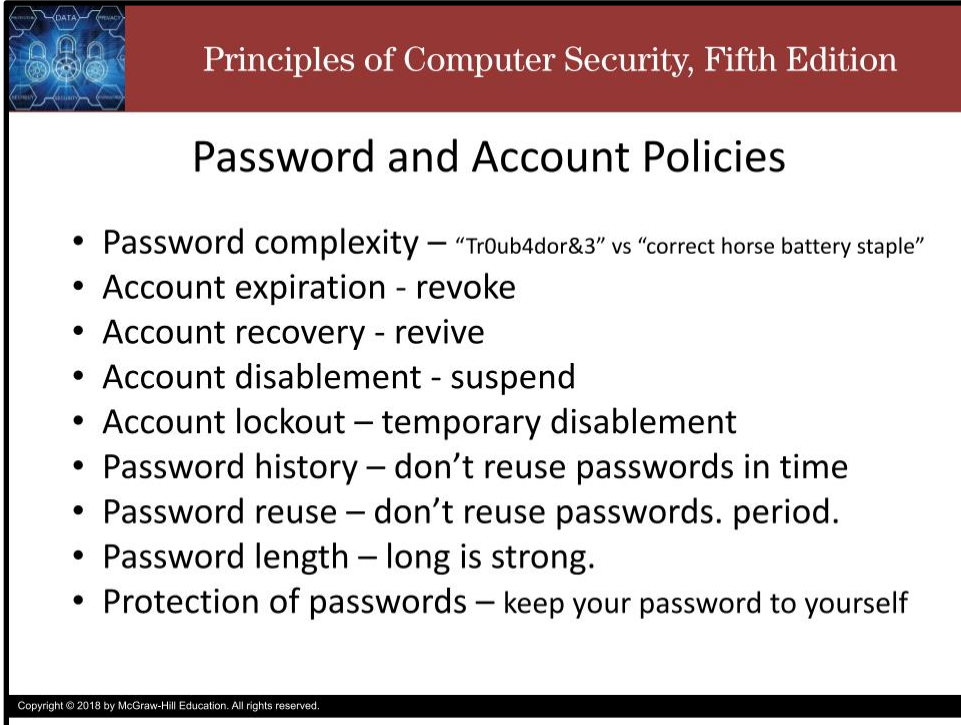
Or even file off magnetic material from the surface of a hard drive platter.

Destroy CDs and DVDs and other removable media by shredding.



The best practice is to match the action to the risk level.

## Slide 8



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header is a white area with the title "Password and Account Policies" in black. A list of nine bullet points follows, detailing various password and account management policies. At the bottom left of the slide, there is a small graphic of a network with nodes and lines, and a copyright notice.

Principles of Computer Security, Fifth Edition

### Password and Account Policies

- Password complexity – “Tr0ub4dor&3” vs “correct horse battery staple”
- Account expiration - revoke
- Account recovery - revive
- Account disablement - suspend
- Account lockout – temporary disablement
- Password history – don’t reuse passwords in time
- Password reuse – don’t reuse passwords. period.
- Password length – long is strong.
- Protection of passwords – keep your password to yourself

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Depending on who you ask, the average user between 20 and 200 passwords. It is likely that most people actually have only a handful of passwords which they reuse, or they have a system for modifying a base password to create a different but related password for most accounts.

Improper use or control of passwords is a leading cause of getting poned.

A password policy sets the expectations for password use and storage.

Password complexity should include a minimum length and guidelines to use both upper and lower case letters, numbers, and symbols. The length is the most important factor in security.

Account expiration should occur when a user is no longer authorized on a given system

Account recovery can be serious, especially if an administrator password is lost.

There needs to be a recovery plan to handle such a tragedy.

Account disablement is preferable to removal because removal might result in permission and ownership problems.

Account lockout is a temporary disablement (for example, when a user tries to log on too many times, too quickly)

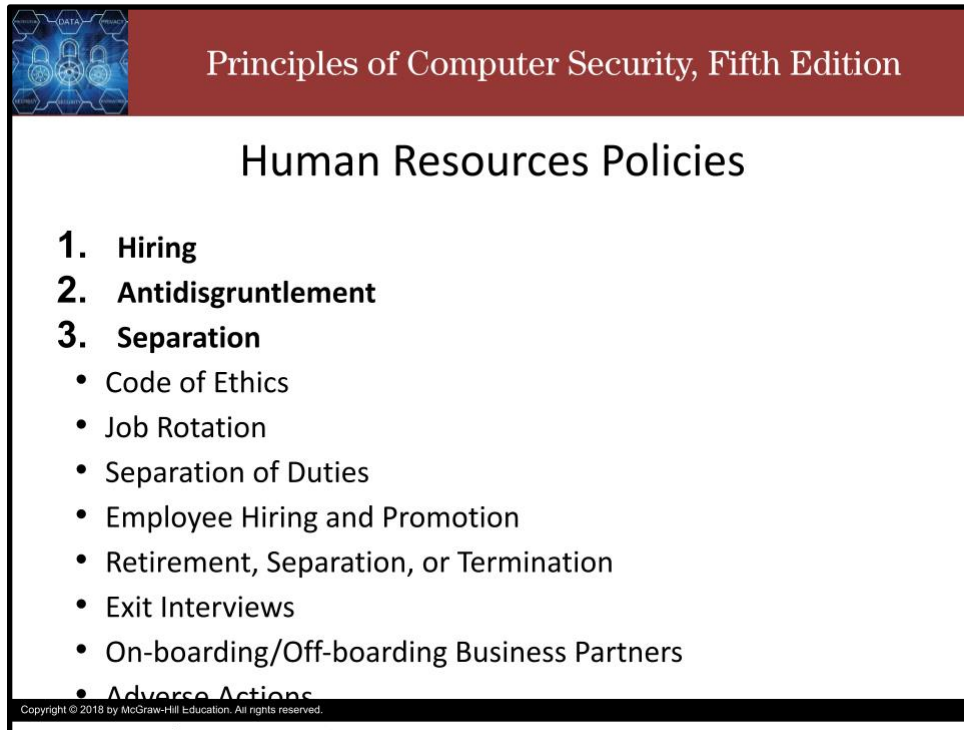
A password history is useful to prevent users from reusing prior passwords

Password reuse is not a good idea, just in general.

Password length should be at least 10 characters, with 12 preferable. The longer the password, the stronger the password.

A password protection policy should prohibit users from writing down or sharing passwords.

## Slide 9



Principles of Computer Security, Fifth Edition

### Human Resources Policies

- 1. Hiring**
- 2. Antidisgruntlement**
- 3. Separation**
  - Code of Ethics
  - Job Rotation
  - Separation of Duties
  - Employee Hiring and Promotion
  - Retirement, Separation, or Termination
  - Exit Interviews
  - On-boarding/Off-boarding Business Partners
  - Adverse Actions

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Humans are the weakest link in the security chain. As such, it is critically important to have policies that relate to the human resources of the organization. There are three kinds of policies that are needed: Policies for hiring people.

Policies to keep employees from being “disgruntled”.

And Policies to address employees leaving the organization.

There are many more specific policies that fit into these categories. Security must be considered in all of them.

Just to mention a few: A code of ethics describes expected behavior at highest level. It sets tone for how employees act and conduct business. Codes of ethics can require that employees are honest and perform all activities in a professional manner. They can address principles of privacy and confidentiality and state how employees treat client and organizational data, and how to handle conflicts of interests. Job rotation can help to improve the resiliency of the organization. The employee hiring and promotion policy can require that a commitment to maintaining security is a condition of employment. Policies covering the retirement, separation, or termination of an employee can lay out what to do to ensure information security throughout the separation process, be it amiable or not so much. Mandatory

vacation sounds wonderful. Would you believe that it actually serves as a practical and useful security protection mechanism?

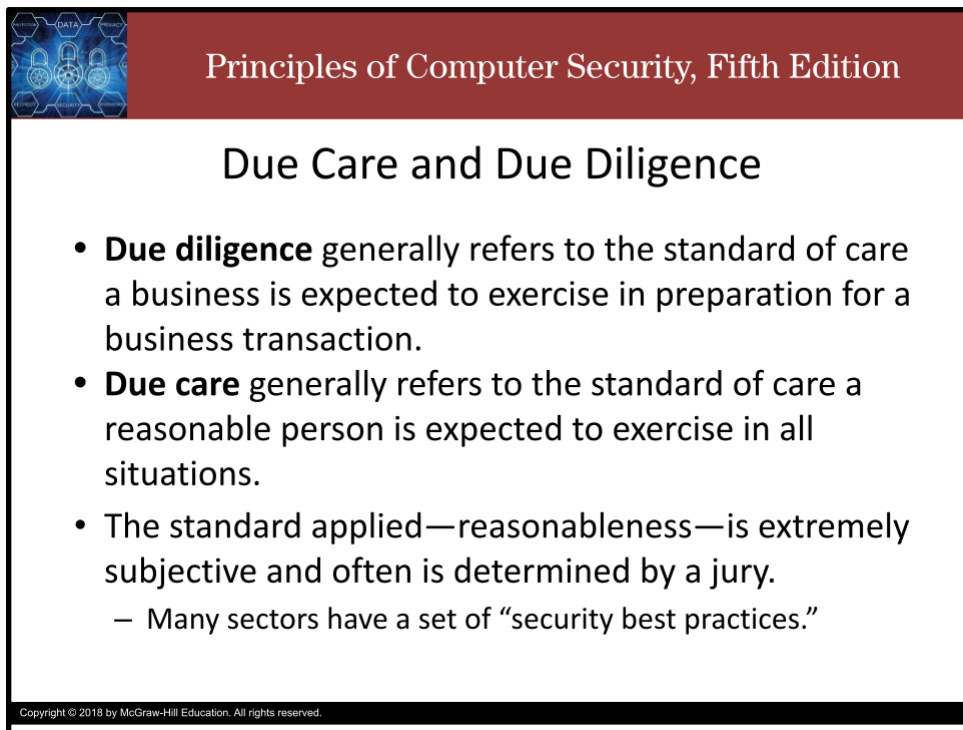
An employee who never takes time off might be involved in nefarious activity.

Requiring mandatory vacations can interrupt harmful activities, like data exfiltration and various forms of corruption. An acceptable use policy outlines what the organization considers to be the appropriate use of company resources, such as computer systems, e-mail, Internet access, and networks and how that expectation is enforced, such as through auditing or monitoring.

A “Bring your own device (BYOD)” policy’s primary purpose is to lower the risk associated with connecting a wide array of personal devices to a company’s network. The policy can require that devices be maintained in a current, up-to-date software posture, and with certain security features.

A privacy policy explains the organizations’ guiding principles and commitments to guarding personal data to which the organization has access.

## Slide 10



The slide features a dark red header with a small graphic of padlocks and the text "Principles of Computer Security, Fifth Edition". The main content is on a white background with a black border, containing a title and a bulleted list. A small copyright notice is at the bottom left.

Principles of Computer Security, Fifth Edition

### Due Care and Due Diligence

- **Due diligence** generally refers to the standard of care a business is expected to exercise in preparation for a business transaction.
- **Due care** generally refers to the standard of care a reasonable person is expected to exercise in all situations.
- The standard applied—reasonableness—is extremely subjective and often is determined by a jury.
  - Many sectors have a set of “security best practices.”

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

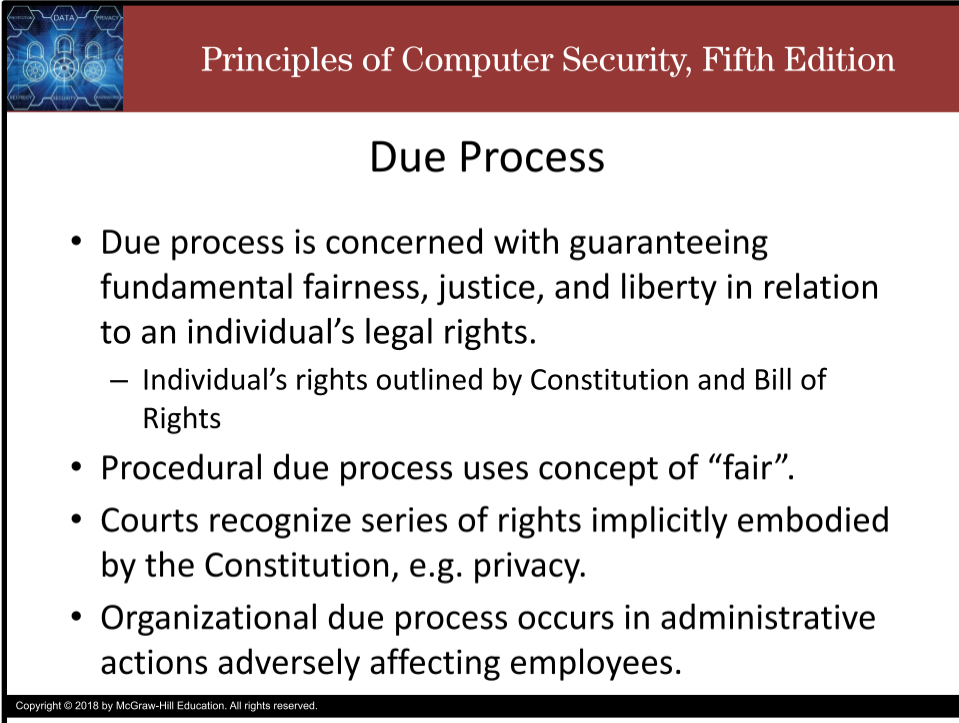
Due diligence is the application of a specific standard of care. Due care is the degree of care that an ordinary person would exercise.

An organization must take reasonable precautions before entering a business transaction or it might be found to have acted irresponsibly. In terms of security, organizations are expected to take reasonable precautions to protect the information that they maintain on individuals. Should a person suffer a loss

as a result of negligence on the part of an organization in terms of its security, that person typically can bring a legal suit against the organization.

The organization will need to show that it had taken reasonable precautions to protect the information, and that, despite these precautions, an unforeseen security event occurred that caused the injury to the other party. Since this is so subjective, it is hard to describe what would be considered reasonable, but many sectors have a set of “security best practices” for their industry, which provides a basis for organizations in that sector to start from. If the organization decides not to follow any of the best practices accepted by the industry, it needs to be prepared to justify its reasons in court should an incident occur. If the sector the organization is in has regulatory requirements, justifying why the mandated security practices were not followed will be much more difficult (if not impossible).

## Slide 11



Principles of Computer Security, Fifth Edition

### Due Process

- Due process is concerned with guaranteeing fundamental fairness, justice, and liberty in relation to an individual’s legal rights.
  - Individual’s rights outlined by Constitution and Bill of Rights
- Procedural due process uses concept of “fair”.
- Courts recognize series of rights implicitly embodied by the Constitution, e.g. privacy.
- Organizational due process occurs in administrative actions adversely affecting employees.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

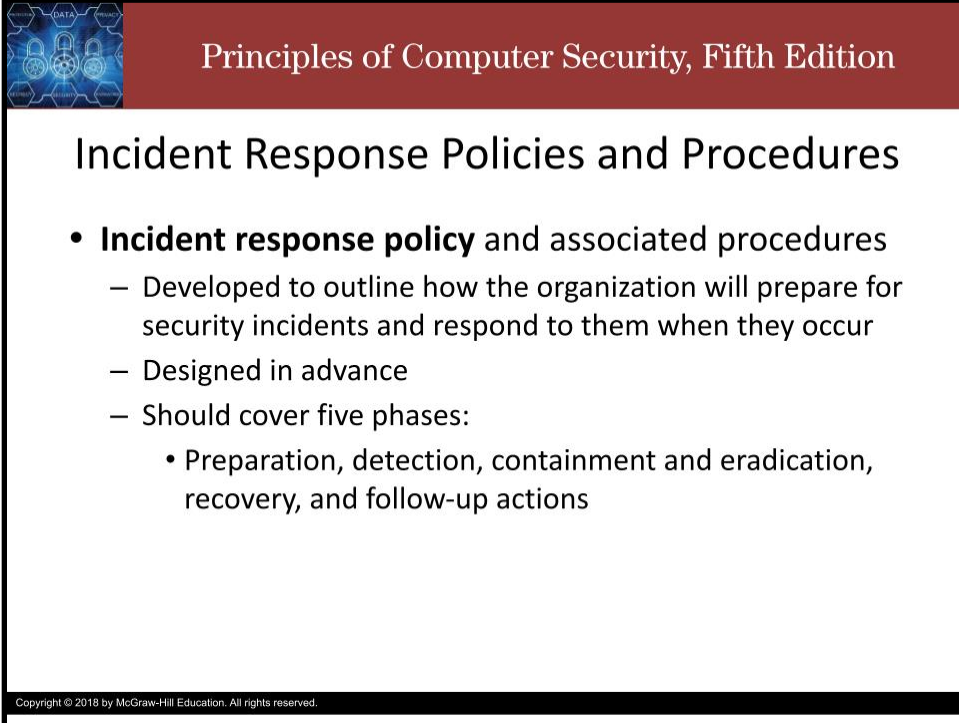
Due process is concerned with guaranteeing fundamental fairness, justice, and liberty in relation to an individual’s legal rights. In the US, due process is concerned with the guarantee of an individual’s rights as outlined by Constitution and Bill of Rights.

Also of interest is the recognition by courts of a series of rights that are not explicitly specified by the Constitution but that the courts have decided are implicit in the concepts embodied by the Constitution. An example of this is an individual’s right to privacy.

From an organization’s point of view, due process may come into play during an administrative action that adversely affects an employee. Before an employee is terminated, for example, were all of the employee’s rights protected? An actual example pertains to the rights of privacy regarding employees’ e-mail messages. As the number of cases involving employers examining employee e-mails grows, case law continues to be established and the courts eventually will settle on what rights an employee can

expect. The best thing an employer can do if faced with this sort of situation is to work closely with HR staff to ensure that appropriate policies are followed and that those policies are in keeping with current laws and regulations.

## Slide 12



**Principles of Computer Security, Fifth Edition**

### Incident Response Policies and Procedures

- **Incident response policy** and associated procedures
  - Developed to outline how the organization will prepare for security incidents and respond to them when they occur
  - Designed in advance
  - Should cover five phases:
    - Preparation, detection, containment and eradication, recovery, and follow-up actions


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

No matter how careful an organization is, eventually a security incident of some sort will occur. When it happens, how effectively the organization responds to it will depend greatly on how prepared it is to handle incidents.

Incident response policy and associated procedures are developed to outline how the organization will prepare for security incidents and respond to them when they occur

They are designed in advance and should cover five phases: Preparation, detection, containment and eradication, recovery, and follow-up actions.

Incident response is covered more thoroughly in another module.



## Principles of Computer Security, Fifth Edition

### Attribution

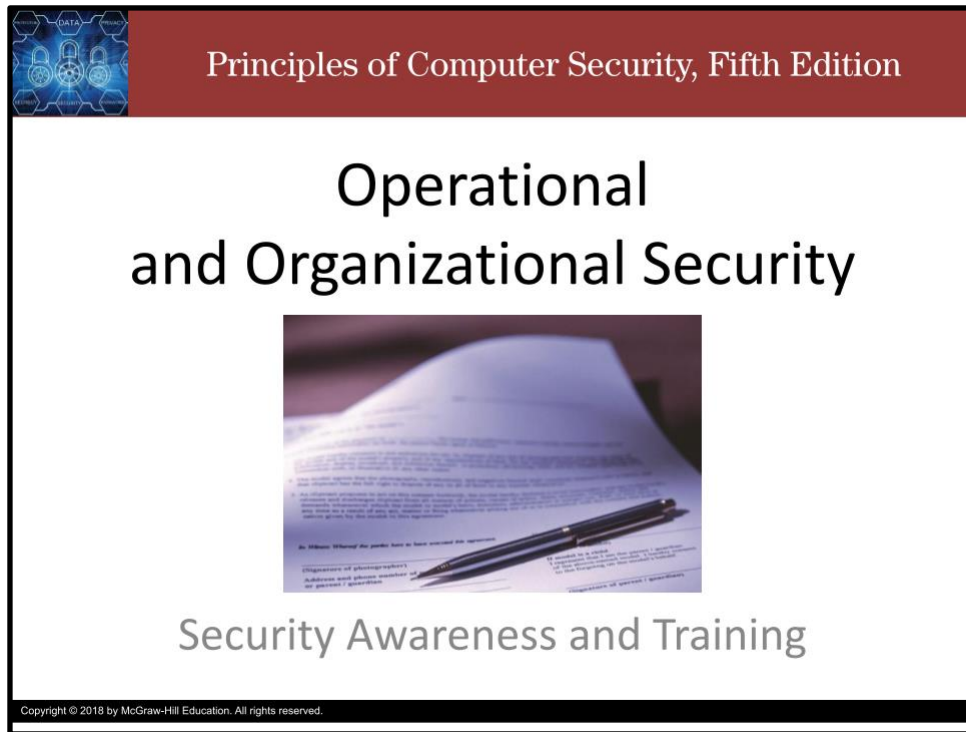
- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.


# Operational and Organizational Security: Security Awareness and Training

Slide 1



The image shows the front cover of the book 'Principles of Computer Security, Fifth Edition'. The top section is a dark red banner with the title 'Principles of Computer Security, Fifth Edition' in white serif font. Below this, the main title 'Operational and Organizational Security' is centered in a large, black, sans-serif font. Underneath the main title is a photograph of an open document with a pen resting on it. At the bottom of the cover, the subtitle 'Security Awareness and Training' is written in a smaller, grey, sans-serif font. A small logo with the word 'DATA' is visible in the top left corner of the cover. At the very bottom, there is a small copyright notice: 'Copyright © 2018 by McGraw-Hill Education. All rights reserved.'

Howdy! In this video, we discuss security awareness and training.



Principles of Computer Security, Fifth Edition

## Security Awareness and Training

- Programs enhance an organization's security posture.
  - Teach personnel how to follow the correct set of actions to perform their duties in a secure manner
  - Make personnel aware of the indicators and effects of social engineering attacks
- Properly trained employees perform duties in a more effective manner.
- Security awareness programs and campaigns
  - Fairly easy to implement and not very costly
  - Annoying but effective

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Security Awareness and Training programs enhance an organization's security posture in two direct ways:

First, they teach personnel how to follow the correct set of actions to perform their duties in a secure manner.


Second, they make personnel aware of the indicators and effects of social engineering attacks.

Properly trained employees are able to perform their duties in a more effective manner, including their duties associated with information security. The extent of information security training will vary depending on the organization's environment and the level of threat, but initial employee security training at the time of being hired is important, as is periodic refresher training. A strong security education and awareness training program can go a long way toward reducing the chance that a social engineering attack will be successful.

Security awareness programs and campaigns can include seminars, videos, posters, newsletters, and similar materials, and are fairly easy to implement and not very costly.

They can be a bit annoying, but they are effective.





Principles of Computer Security, Fifth Edition

## Security Policy Training and Procedures

- Personnel need training with respect to the tasks and expectations to perform complex tasks.
  - Applies to security policy and operational security details
- Use refresher training for periodic reinforcement.
- Collection of policies should paint a picture describing the desired security culture of the organization.
  - Security policy – high-level directive
  - Second-level policies – password, access, information handling, and acceptable use policies

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


If employees are going to be expected to comply with the organization's security policy, they must be properly trained in its purpose, meaning, and objectives.

Training with respect to the information security policy, individual responsibilities, and expectations is something that requires periodic reinforcement through refresher training.

Because the security policy is a high-level directive that sets the overall support and executive direction with respect to security, it is important that the meaning of this message be translated and supported. Second-level policies such as password, access, information handling, and acceptable use policies also need to be covered.

The collection of policies should paint a picture describing the desired security culture of the organization.

The training should be designed to ensure that people see and understand the whole picture, not just the elements.




Principles of Computer Security, Fifth Edition

## Role-based Training

- Training needs to be targeted to the user with regard to their role in the subject of the training.
- Role-based training is an important part of information security training.
- Applies to:
  - Data Owner                      - User
  - System Administrator            - Privileged User
  - System Owner                      - Executive User

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

If a person has job responsibilities that may impact information security, then role-specific training is needed to ensure that the individual understands the responsibilities as they relate to information security. Some roles, such as system administrator or developer, have clearly defined information security responsibilities. The roles of others, such as project manager or purchasing manager, have information security impacts that are less obvious, but these roles require training as well. In fact, the less-obvious but wider-impact roles of middle management can have a large effect on the information security culture, and thus if a specific outcome is desired, it requires training.




Principles of Computer Security, Fifth Edition

## Compliance with Laws, Best Practices, and Standards

- Wide array of laws, regulations, contractual requirements, standards, and best practices associated with information security.
  - Organization must build them into their own policies and procedures.
- External requirements impart a specific training and awareness component upon the organization.
  - Payment Card Industry Data Security Standard (PCI DSS), Gramm Leach Bliley Act (GLBA), or Health Insurance Portability Accountability Act (HIPAA)

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There is a wide array of laws, regulations, contractual requirements, standards, and best practices associated with information security. Each places its own set of requirements upon an organization and its personnel. The only effective way for an organization to address these requirements is to build them into their own policies and procedures. Training to one's own policies and procedures would then translate into coverage of these external requirements.



Principles of Computer Security, Fifth Edition

## User Habits


- Front-line security tool in engaging the workforce to improve the overall security posture of an organization.
- Individual user responsibilities vary between organizations and the type of business in which each organization is involved.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

User habits are a front-line security tool in engaging the workforce to improve the overall security posture of an organization.

Individual user responsibilities vary between organizations and the type of business in which each organization is involved.

## Slide 7



Principles of Computer Security, Fifth Edition

### User Habits

- Lock doors.
- Do not leave sensitive information inside your car unprotected.
- Secure storage media
- Shred paper before discarding it.
- Do not divulge sensitive information to individuals who do not have an authorized need to know it.
- Protect laptops and other mobile devices
- Be aware of who is around you
- Be aware of the correct procedures to report suspected or actual violations of security policies
- Follow procedures established to enforce good password security practices.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are certain very basic responsibilities that all users should be instructed to adopt.

Lock the door to your office or workspace, including drawers and cabinets.

Do not leave sensitive information inside your car unprotected.

Secure storage media containing sensitive information in a secure storage device.

Shred paper containing organizational information before discarding it.

Do not divulge sensitive information to individuals (including other employees) who do not have an authorized need to know it. Do not discuss sensitive information with family members. (The most common violation of this rule occurs in regard to HR information, as employees, especially supervisors, may complain to their spouse or friends about other employees or about problems that are occurring at work.)

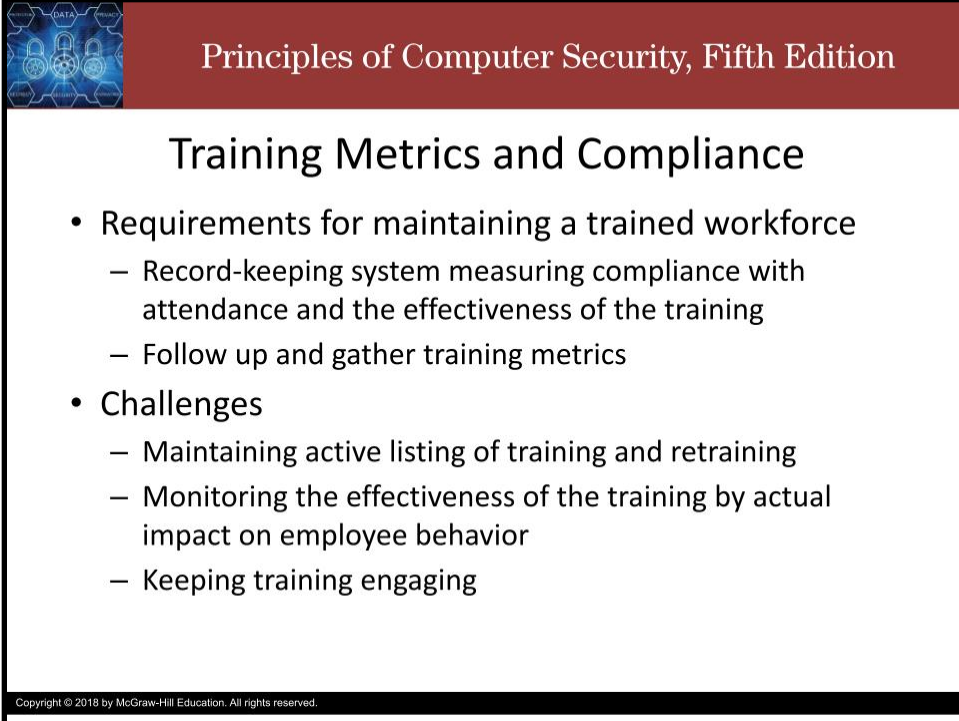
Protect laptops and other mobile devices that contain sensitive or important organization information wherever the device may be stored or left. (It's a good idea to ensure that sensitive information is encrypted on the laptop or mobile device so that, should the equipment be lost or stolen, the information remains safe.)

Be aware of who is around you when discussing sensitive corporate information. Does everybody within earshot have the need to hear this information? Enforce corporate access control procedures. Be alert to, and do not allow, piggybacking, shoulder surfing, or access without the proper credentials.

Be aware of the correct procedures to report suspected or actual violations of security policies.

Follow procedures established to enforce good password security practices. Passwords are such a critical element that they are frequently the ultimate target of a social engineering attack. Though such password procedures may seem too oppressive or strict, they are often the best line of defense.

## Slide 8



Principles of Computer Security, Fifth Edition

### Training Metrics and Compliance

- Requirements for maintaining a trained workforce
  - Record-keeping system measuring compliance with attendance and the effectiveness of the training
  - Follow up and gather training metrics
- Challenges
  - Maintaining active listing of training and retraining
  - Monitoring the effectiveness of the training by actual impact on employee behavior
  - Keeping training engaging

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Many laws, regulations, and best practices have requirements for maintaining a trained workforce. Having a record-keeping system to measure compliance with attendance and to measure the effectiveness of the training is a normal requirement.

Simply conducting training is not enough.

Following up and gathering training metrics to validate compliance and the security posture is an important aspect of security training management.


A number of factors deserve attention when you're managing security training.

Due to the diverse nature of role-based requirements, maintaining an active, up-to-date listing of individual training and retraining requirements is one challenge.

Creating an effective training and awareness program when measured by actual impact on employee behavior is also challenging.

Training needs to be current, relevant, and interesting enough to engage employee attention. Simple repetition of the same training material has not proven to be effective, so the program needs to be regularly updated in order to remain effective over time.

## Slide 9



### Principles of Computer Security, Fifth Edition

## Attribution

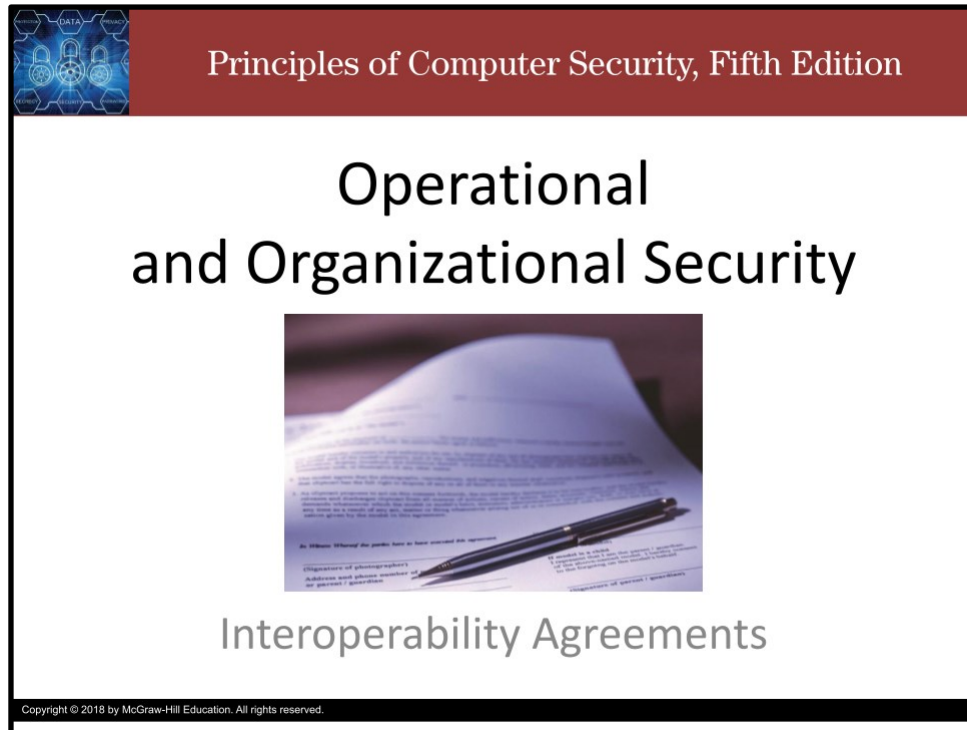
- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

# Operational and Organizational Security: Interoperability Agreements


Slide 1



The image shows the cover of a book titled "Principles of Computer Security, Fifth Edition". The cover has a dark red header with the title in white. Below the header, the main title "Operational and Organizational Security" is written in large black font. Underneath the main title is a photograph of an open document with a pen resting on it. At the bottom of the cover, the subtitle "Interoperability Agreements" is written in a smaller black font. A small copyright notice is visible at the very bottom of the cover.

Principles of Computer Security, Fifth Edition

## Operational and Organizational Security




### Interoperability Agreements

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss interoperability agreements.





Principles of Computer Security, Fifth Edition

## Interoperability Agreements

- Many business operations involve actions by many different parties.
- Actions require communication between the parties.
  - Define the responsibilities and expectations of the parties
  - Define business objectives
  - Define environment within which the objectives will be pursued
- Written agreements ensure understanding between the parties.
  - E.g. SLA, BPA, MOU, ISA, NDA

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Many business operations involve actions by many different parties.

These actions require communication between the parties.

This communication defines the responsibilities and expectations of the parties, the business objectives, and the environment within which the objectives will be pursued.

Written agreements are used to ensure that these elements are understood between the parties.

Numerous forms of legal agreements and contracts are used in business, but with respect to security, some of the most common ones are the service level agreement, business partnership agreement, memorandum of understanding, interconnection security agreement, and nondisclosure agreement.



Principles of Computer Security, Fifth Edition

## Service level agreements (SLA)

- Contractual agreements between entities that describe specified levels of service that the servicing entity agrees to guarantee for the customer
- Good SLAs
  - Unambiguously describe the entire set of required product or service functions
  - Provide a clear means of determining whether a specified function or service has been provided at the agreed-upon level of performance
  - Defines penalties for the service provider for not meeting the requisite service level.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Service level agreements are contractual agreements between entities that describe specified levels of service that the servicing entity agrees to guarantee for the customer.

SLAs are typically included as part of a service contract and set the level of technical expectations.


An SLA can define specific services, the performance level associated with a service, issue management and resolution, and so on.

A good SLA does three things:

It describes the entire set of product or service functions in sufficient detail that their requirement will be unambiguous.

It provides a clear means of determining whether a specified function or service has been provided at the agreed-upon level of performance.

It specifies the consequences for the service provider for not delivering the function or service at the requisite level.



Principles of Computer Security, Fifth Edition


## Business partnership agreement (BPA)

- Legal agreement between partners establishing the terms, conditions, and expectations of the relationship between the partners
  - Sharing of profits and losses, the responsibilities of each partner, the addition or removal of partners, and any other issues

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A business partnership agreement is a legal agreement between partners establishing the terms, conditions, and expectations of the relationship between the partners.

The details can cover any issue, such as the sharing of profits and losses, the responsibilities of each partner, and the addition or removal of partners.



Principles of Computer Security, Fifth Edition

## Memorandum of understanding (MOU)


- Legal document used to describe a bilateral agreement between parties
- Written agreement expressing a set of intended actions between the parties with respect to some common pursuit or goal
- More formal and detailed than a simple handshake
- Generally lacks the binding powers of a contract

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A memorandum of understanding is a legal document used to describe a bilateral agreement between parties.

It is a written agreement expressing a set of intended actions between the parties with respect to some common pursuit or goal.

It is more formal and detailed than a simple handshake, but generally lacks the binding powers of a contract.



Principles of Computer Security, Fifth Edition

### Interconnection security agreement (ISA)


- Specialized agreement between organizations that have interconnected IT systems.
- Purpose is to document the security requirements associated with the interconnection.
- ISA as part of an MOU can detail specific technical security aspects of a data interconnection.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An interconnection security agreement is a specialized agreement between organizations that have interconnected IT systems.

The purpose of the ISA is to document the security requirements associated with the interconnection.

A part of an MOU, an ISA can detail specific technical security aspects of a data interconnection.



Principles of Computer Security, Fifth Edition

## Nondisclosure Agreement (NDA)

- Standard corporate documents used to explain the boundaries of corporate secret material
  - corporate secret material = information over which control should be exercised to prevent disclosure to unauthorized parties.
- Frequently used to delineate the level and type of information, and with whom it can be shared.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Nondisclosure agreements are standard corporate documents used to explain the boundaries of corporate secret material – information over which control should be exercised to prevent disclosure to unauthorized parties.

NDA's are frequently used to delineate the level and type of information, and with whom it can be shared.



## Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Thank you and take care.