Operations Security

- **Operations Security:** is used to identify the controls over hardware, media, and the operators with access privileges to any of these resources.

- To prevent people either inadvertently or intentionally compromising the confidentiality, integrity, or availability of data or the systems and media holding that data.

- **Audit and monitoring:** are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

Administrative Personnel Controls

- They represent important operations security concepts that should be mastered by security team or SOC:

Need to know

Least privilege

Separation of duties

Job rotation

Mandatory Leave/Forced Vacation

Non-Disclosure Agreement

Background Checks

Monitoring of Special Privileges

Need-to-know

- Individual personnel should have access to only the information that they require in order to perform their stated duties.
- It is usually used with **Mandatory access control (MAC)** as clearance level alone is insufficient when dealing with the most sensitive of information.
- while there may be a large number of individuals (some of high rank), only a subset "need to know" specific information. The others have no "need to know," and therefore no access.
- The advantage of need-to-know-based access control is reduced risk.

Least Privilege

- Ensuring that no role is given more privileges than necessary to carry out authorised tasks.

- It is most obvious in Discretionary Access Control (DAC) environments

- Access to systems, services, applications and data should be explicitly authorised
  - ✓ The identification and design of specific roles
  - ✓ Default or inappropriate access controls are key attack routes for malware installation and espionage
  - ✓ If an account is compromised then the fewest resources should be available to an attacker possible.

- **Problems:**
  - ✓ What if a key user is absent and you need their privileges to perform a critical function?
  - ✓ What if users begin sharing passwords?

Example:

As an example, imagine that an employee has been away from the office for training, and has submitted an expense report indicating $1,000,000 was needed for reimbursement. This individual happens to be a person who, as part of her daily duties, had access to print reimbursement checks, and would therefore meet the principle of least privilege for printing her own reimbursement check.

Should she be able to print herself a nice big $1,000,000 reimbursement check? While this access may be necessary for her job function, and thus meet the requirements for the principle of least privilege, **additional controls are required.**

Separation of Duties

- Setting up roles within an organisation such that no individual can subvert a critical process

- Separation of duties is to take a duty or task and separate it so that two or more persons must be present in order to complete it.

  - ✓ In popular culture, tasks that require separation of duties like: Deployment of a nuclear weapon
  - ✓ Issuing an arrest warrant. Law enforcement documents a probable cause to arrest an individual, which is signed by a judge.

- No critical business process should rely on one individual. Especially where there is the potential for some benefit

- Employing separation of duties reduces the likelihood that an improper task or fraud will be performed.

Separation of Duties (Cont.)

- **Example:** companies have a CEO but have a board and chairperson as well

- **Example:** a cashier can sell you an item but only a supervisor can issue a refund

- For availability, "backup" should be available for people who do occupy critical roles

Job Rotation

- It is the practice of moving individual workers through a range of assignments over time.
- Critical functions or responsibilities are not continuously performed by the same single person without interruption.
- This practice adds value to the organization by exposing employees to a wider variety of activities, providing additional opportunities for excellence and reducing monotony and boredom.
- It reduces risk an fraud by moving people out of specific tasks.

Mandatory Leave/Forced Vacation

- It is closely related to rotation of duties and is the practice of keeping employee far away from work.

- To reduce or detect personnel single points of failure, and detection and deterrence of fraud.

- Discovering a lack of depth in personnel with critical skills can help organizations understand risks associated with employees unavailable for work due to unforeseen circumstances.

Non-Disclosure Agreement

- It is a **work-related contractual agreement** that ensures that, prior to being given access to sensitive information or data, an individual or organization appreciates their legal responsibility to maintain the confidentiality of sensitive information.

- Non-Disclosure Agreements (NDA) are often signed by job candidates before they are hired, as well as consultants or contractors.

- NDA is a directive security control

Background Check

- ❑ known as background investigations or preemployment screening

- ❑This might include a criminal record check, verifying employment history, obtaining credit reports, and in some cases requiring the submission of a drug screening.

- ❑The sensitivity of the position being filled or data to which the individual will have access strongly determines the degree to which this information is scrutinized and the depth to which the investigation will report.

- Ongoing, or postemployment, investigations seek to determine whether the individual continues to be worthy of the trust required of their position

Monitoring of Special Privileges

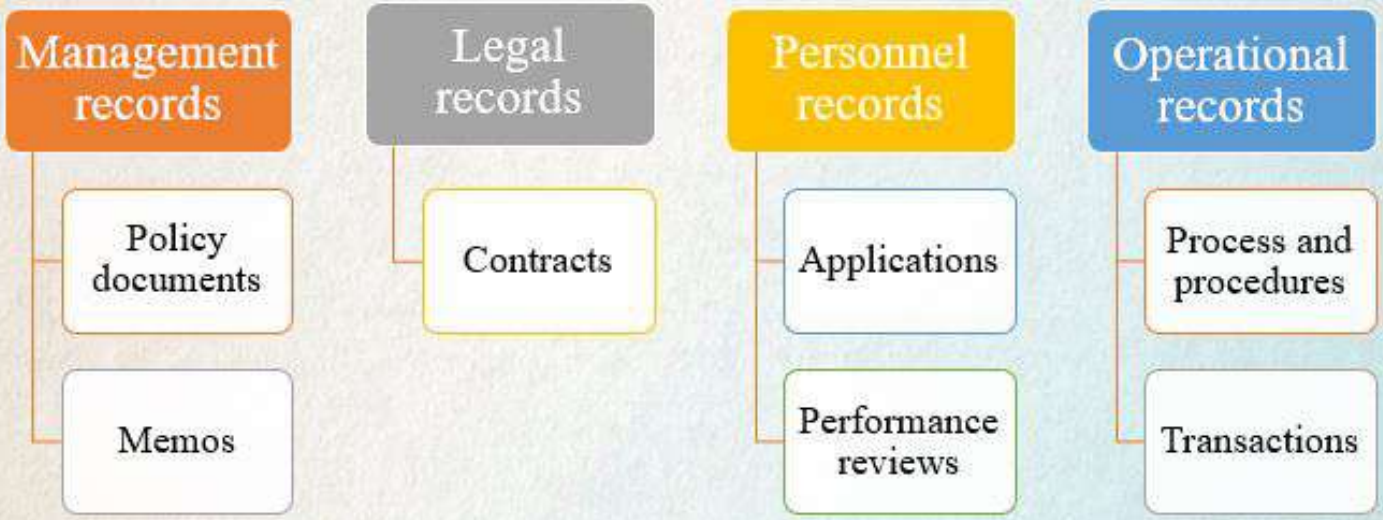
- Because administrators' capabilities are greater than most other users, a mistake can be far more costly, resulting in a partial or complete loss or corruption of data, or more subtle errors that may not be immediately obvious.

- For this reason it is especially important for an organization to implement controls to monitor actions carried out by administrators. (i.e. System Administer)

- The reasons for monitoring these functions include:
  - ✓Accountability.
  - ✓Audit logging.
  - ✓Troubleshooting.

Records Management Controls

- Business records are the information that is produced in support of business operations. Business records will consist of many types of information including:



❑ Records management including:

Data classification

- Establishing sensitivity levels and handling procedures.

Access management

- Choosing who may access information

Records retention

- How long information must be kept

Backups

- Making sure information is not lost due to a failure or malfunction.

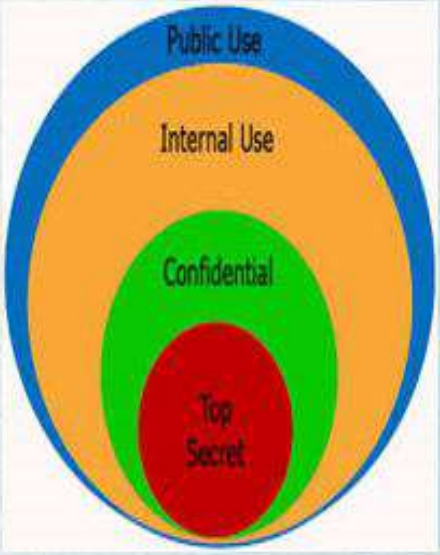
Data destruction.

- How information must be safely discarded when no longer needed.

Data classification

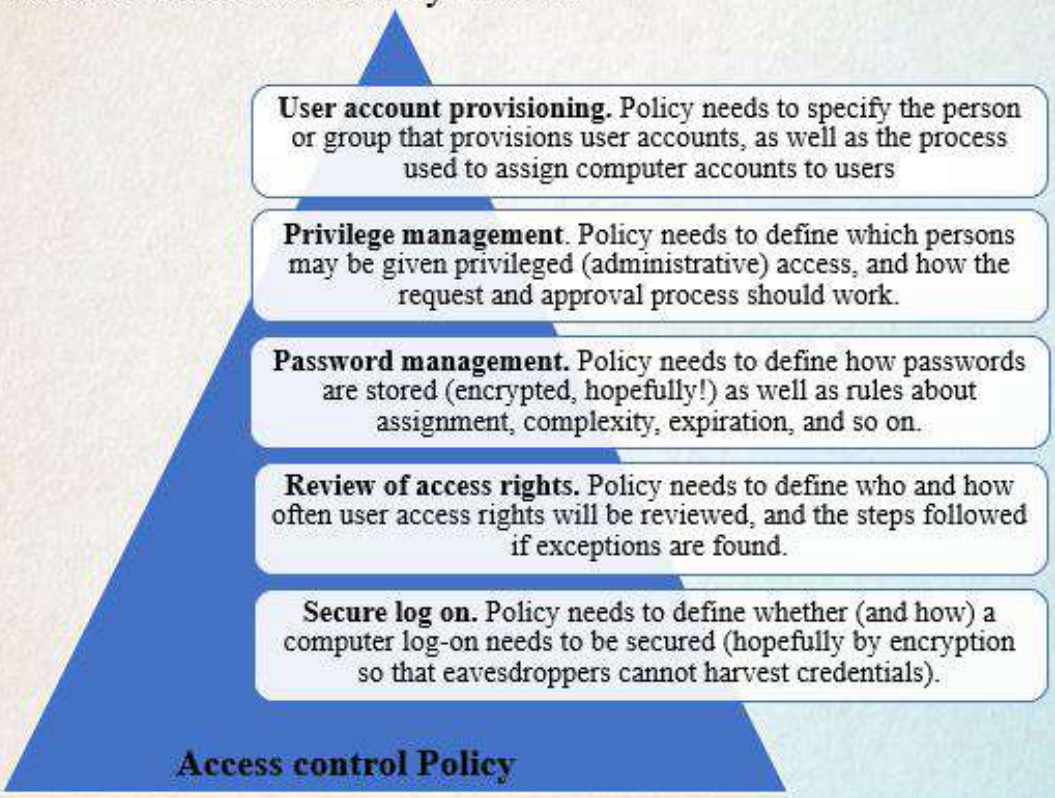
- Example: Government security clearances
  - ✓ Protected
  - ✓ Confidential / highly protected/ secret
  - ✓ Top secret

Public	Internal Only	Confidential	Restricted
Data that may be freely disclosed to the public For example: marketing materials, contact information, price lists, etc.	Internal data not meant for public disclosure For example: battlecards, sales playbooks, organizational charts, etc.	Sensitive data that if compromised could negatively affect operations For example: contracts with vendors, employee reviews, etc.	Highly sensitive corporate and customer data that if compromised could put the organization at financial or legal risk For example: IP, credit card information, social security numbers, PHI)



Access Management

- It refers to the policies, procedures, and controls that determine how information is accessed and by whom.



Record Retention

- Organizations need to develop policies that specify how long different types of records must be retained.

- The types of records that may be included in a records retention schedule are:
  - ✓Payroll records
  - ✓Personnel records
  - ✓Financial records
  - ✓Legal contracts
  - ✓E-mail
  - ✓Audit reports
  - ✓Audit logs from applications

Backups

- **Backup:** is the process of copying important information from a computer or storage system to another device for recovery or archival purposes.
- The causes for information loss include:
  - ✓ Equipment malfunctions.
  - ✓ Software bugs.
  - ✓ Human error.
  - ✓ Disasters.
- **Data Restoration:** When data is lost or damaged, backup copies of the data can be copied from the backup media back into the system.
- Protection of Backup Media (i.e., such as locked doors, surveillance cameras, and visitor logs.
- **Offsite Storage of Backup Media:** Distance from business location, Security of transportation, Security of storage center, Resilience against disasters

Data Destruction

- Instruction on how to properly discard the information.
- Information being discarded is of varying levels of sensitivity, according to a data classification or data sensitivity policy.

Degaussing

is a process of erasing the data on magnetic media by exerting a strong magnetic field that effectively erases any stored data.

Applies to magnetic-based media such as hard drives and backup tapes.

Shredding.

Applies to paper records as well as some electronic media such as CD/DVD-ROM, floppy disc, and backup tape.

Wiping.

Applies to files on magnetic-based media such as hard drives.

Examples of methods available to destroy information

Anti-Virus and Anti-Malware

- Anti-virus or Anti-malware: software is used to detect and remove malicious code including computer viruses. Similarly, anti-spyware detects and removes spyware.

- Malware has the capacity to disrupt the operation of user workstations as well as servers, which could result in:
  - ✓ Loss of business information
  - ✓ Disclosure or compromise of business information
  - ✓ Corruption of business information
  - ✓ Disruption of business information processing

- **Central Anti-Malware Management**: In all but the very smallest organizations, anti-malware software is usually controlled or managed through a central console.

Risks and Remote Access

- The connectivity to a network or system from a location away from the network or system, usually from a location apart from the organization's premises.

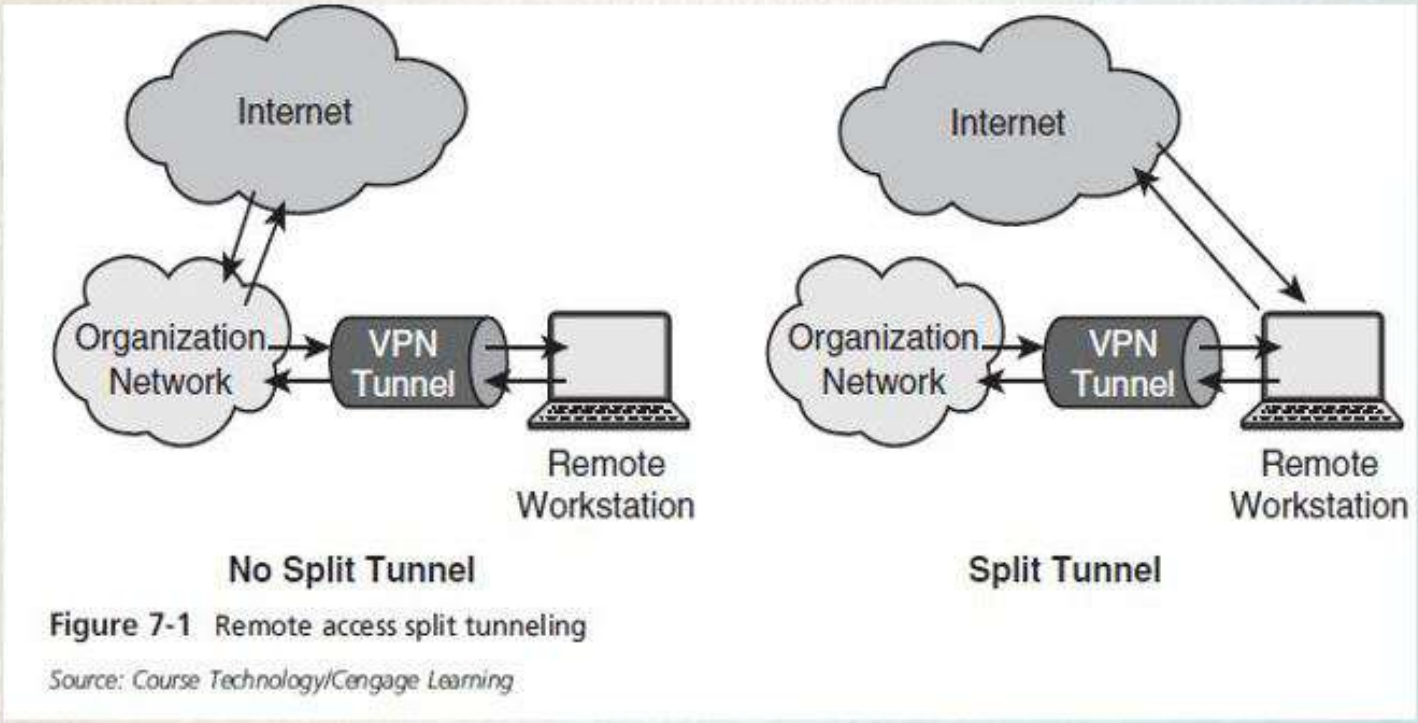


Figure 7-1 Remote access split tunneling

Source: Course Technology/Cengage Learning

High Availability Architectures

- Well organized computer operations departments can develop quite a good record of application uptime, but in order to keep systems running smoothly, period maintenance is required for the installation of patches, software updates, hardware upgrades, and so on. And, unexpected failures do sometimes occur, seemingly at the most inopportune times.
- Options available include:
  - ✓ Fault tolerance (Failure-prone components are duplicated)
    - ✓ Multiple power supplies
    - ✓ Multiple network interfaces
    - ✓ Multiple processor units.
    - ✓ RAID (Redundant Array of Inexpensive Disks)
  - ✓ Clusters (active-active or active-passive.)
  - ✓ Failover
  - ✓ Replication

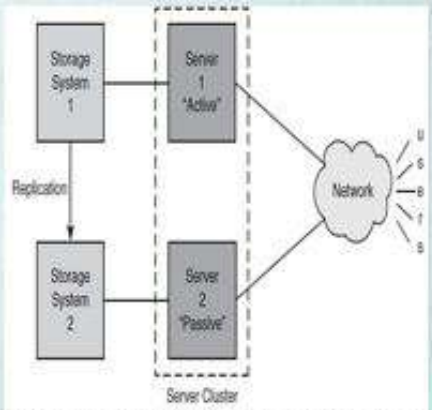


Figure 7-2 Clustering and replication working together to form a highly available architecture

Business Continuity Management

- **A business continuity plan:** is the result of a management activity where analysis is performed to better understand the risks associated with potential disaster scenarios and the steps that can be taken to reduce the impact of a disaster should one occur.

- Each company should have a continuity and disaster recovery plan to restore normal modes of operation with minimum cost and disruption to normal business activities after an unexpected adverse event (threat, disaster..etc).

- A common outcome of a business continuity is the implementation of "**a high-availability architecture**" that will permit critical business functions to continue operating even when a disaster strikes.

Vulnerability Management

- It is the process of identifying vulnerabilities in a system and then acting to mitigate those vulnerabilities.

- Vulnerabilities can be discovered in one of two basic ways:

  - ✓ Passive means: manufacturer and independent resource
  - ✓ Active means: penetration testing scans or application vulnerability scans.

- The remediation or mitigation of vulnerabilities should be prioritized based on both risk to the organization and ease of remediation procedures.

Change management

- The purpose of the change control process is to understand, communicate, and document any changes with the primary goal of being able to understand, control, and avoid direct or indirect negative impact that the change might impose.

- **Plan include:**
  - ✓ Identification and inventory of changes requests
  - ✓ Analysis and documentation pf the complete impact of requested changes
  - ✓ Approval or rejection of change request
  - ✓ Tracking changes and updating of project documentation to account for approved changes
  - ✓ How stakeholders will be informed of changes.