

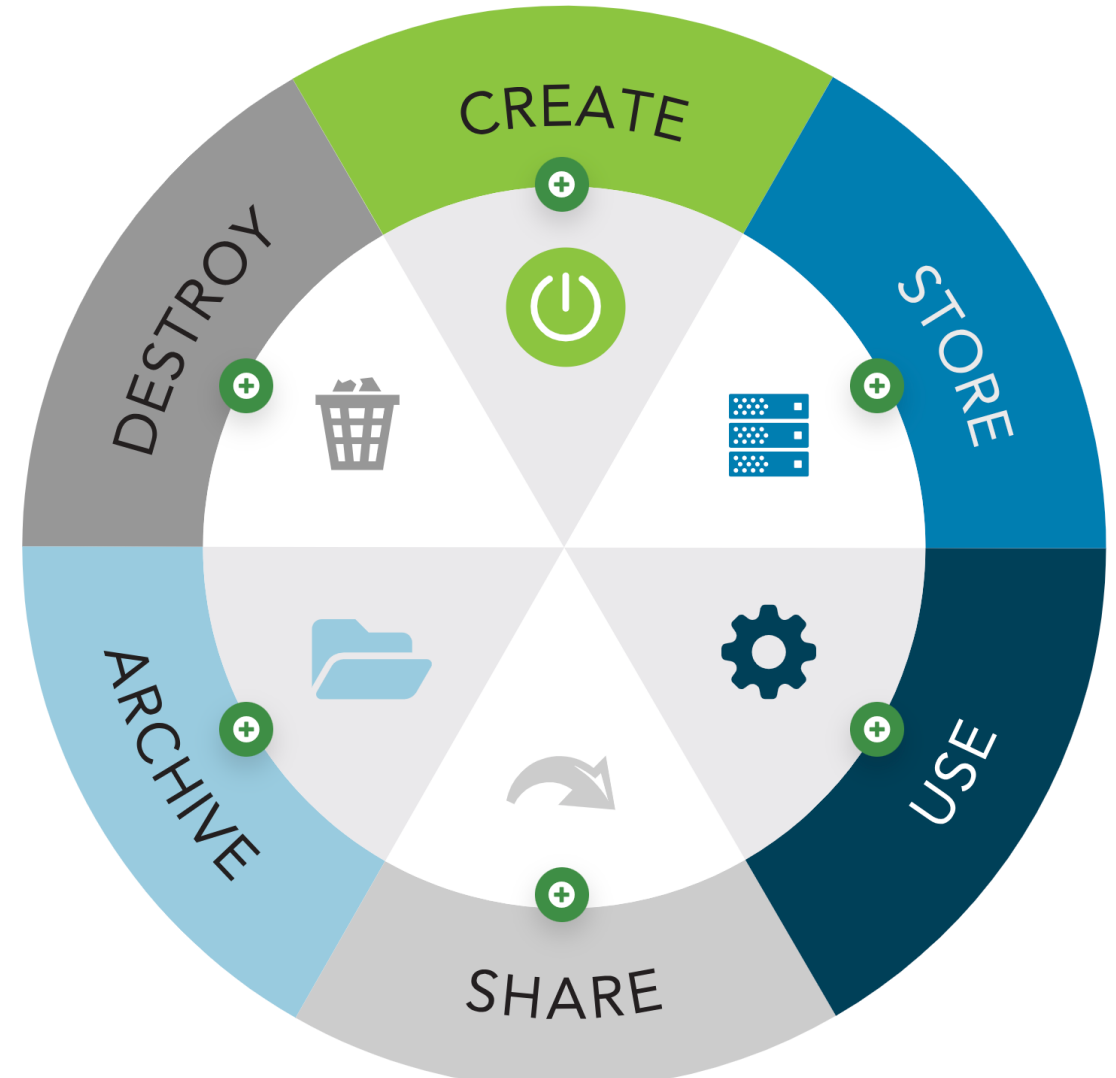
Cybersecurity Fundamentals

Module 5: Security Operations

Data Handling

- Data Lifecycle :

- Create : Creating the knowledge, which is usually tacit knowledge at this point.
- Store : Storing or recording it in some fashion (which makes it explicit).
- Use : Using the knowledge, which may cause the information to be modified, supplemented or partially deleted.
- Share : Sharing the data with other users, whether as a copy or by moving the data from one location to another.
- Archive : Archiving the data when it is temporarily not needed.
- Destroy : Destroying the data when it is no longer needed.



Data Handling Practices : Classification

- Classification is the process of recognizing the organizational impacts if the information suffers any security compromises related to its characteristics of confidentiality, integrity and availability.
- More efficient design and implementation of security processes



Data Handling Practices : Labeling

- Security labels are part of implementing controls to protect classified information.
- Data Sensitivity Levels and Labels :
 - Highly restricted: Compromise of data with this sensitivity label could possibly put the organization's future existence at risk. Compromise could lead to substantial loss of life, injury or property damage, and the litigation and claims that would follow.
 - Moderately restricted: Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue or disruption of planned investments or activities.
 - Low sensitivity (sometimes called "internal use only"): Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts.
 - Unrestricted public data: As this data is already published, no harm can come from further dissemination or disclosure.



Data Handling Practices : Retention

- Information and data should be kept only for as long as it is beneficial
- Certain industry standards, laws and regulations define retention periods
- It is an organization's responsibility to define and implement its own data retention policy
- Organizations should conduct a periodic review of retained records in order to reduce the volume of information stored and to ensure that only necessary information is preserved
- Records retention policies indicate how long an organization is required to maintain information and assets. Policies should guarantee that:
 - Personnel understand the various retention requirements for data of different types throughout the organization.
 - The organization appropriately documents the retention requirements for each type of information.
 - The systems, processes and individuals of the organization retain information in accordance with the required schedule but no longer.

Data Handling Practices : Destruction

Data that might be left on media after deleting is known as [remanence](#) and may be a significant security concern. Steps must be taken to reduce the risk that data remanence could compromise sensitive information to an acceptable level. This can be done by one of several means:

- Clearing the device or system, which usually involves writing multiple patterns of random values throughout all storage media (such as main memory, registers and fixed disks). This is sometimes called “overwriting” or “zeroizing” the system, although writing zeros has the risk that a missed block or storage extent may still contain recoverable, sensitive information after the process is completed.
- Purging the device or system, which eliminates (or greatly reduces) the chance that residual physical effects from the writing of the original data values may still be recovered, even after the system is cleared. Some magnetic disk storage technologies, for example, can still have residual “ghosts” of data on their surfaces even after being overwritten multiple times. Magnetic media, for example, can often be altered sufficiently to meet security requirements; in more stringent cases, [degaussing](#) may not be sufficient.
- Physical destruction of the device or system is the ultimate remedy to data remanence. Magnetic or optical disks and some flash drive technologies may require being mechanically shredded, chopped or broken up, etched in acid or burned; their remains may be buried in protected landfills, in some cases.

Logging and Monitoring Security Events

- Logging is the primary form of instrumentation that attempts to capture signals generated by events.
- Information that may be relevant to being recorded and reviewed include (but is not limited to):
 - user IDs
 - system activities
 - dates/times of key events (e.g., logon and logoff)
 - device and location identity
 - successful and rejected system and resource access attempts
 - system configuration changes and system protection activation and deactivation events
- Log reviews are an essential function not only for security assessment and testing but also for identifying security incidents, policy violations, fraudulent activities and operational problems near the time of occurrence.
- Controls are implemented to protect against unauthorized changes to log information.

Logging and Monitoring Security Events :

Events

SHOW 20 ENTRIES



ACTIONS ▾

☐	DATE ▾	STATUS ⬆	INTENT & STRATEGY ⬆	METHOD ⬆	RISK ⬆	OTX	SOURCE	DESTINATION	
☐	2020-01-24 20:10:08	open	AlienVault HIDS: SQL injection attempt.		HIGH (4)	N/A	alienvault	Host-172-20-1-131	
☐	2020-01-24 20:10:08	open	AlienVault HIDS: SQL injection attempt.		HIGH (4)	N/A	alienvault	Host-172-20-1-131	
☐	2020-01-24 20:10:08	open	AlienVault HIDS: Multiple SQL injection attempts from same source ip.		HIGH (4)	N/A	alienvault	Host-172-20-1-131	
☐	2020-01-24 20:10:08	open	AlienVault HIDS: SQL injection attempt.		HIGH (4)	N/A	alienvault	Host-172-20-1-131	

Logging and Monitoring Security Events : Event Detail

The screenshot displays the OSSIM web interface at the URL https://172.20.1.127/ossim/#analysis/security_ev. The interface includes a navigation bar with tabs for DASHBOARDS, ANALYSIS (selected), ENVIRONMENT, REPORTS, and CONFIGURATION. Below the navigation bar, there are two panels showing asset information and service status. The left panel displays 'Asset Value: 2' and 'OTX IP Reputation: No'. The right panel also shows 'Asset Value: 2' and 'OTX IP Reputation: No'. Both panels indicate 'No services available' under the 'SERVICE' column. At the bottom, a table provides detailed event information across six columns: USERDATA1, USERDATA2, USERDATA3, USERDATA4, USERDATA5, and USERDATA6.

USERDATA1	USERDATA2	USERDATA3	USERDATA4	USERDATA5	USERDATA6
(Host-172-20-1-131) 172.20.1.131->\xampp\apache\logs\access.log	Multiple common web attacks from same source ip.	web,accesslog,attack,	GET	/error/core/includes/gfw_s_marty.php?config[gfwroot]=../../../../boot.ini%00	404

Logging and Monitoring Security

Events :

Raw Log

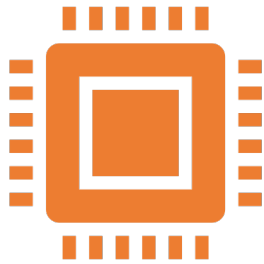
RAW LOG

```
AV - Alert - "1579914608" --> RID: "31103"; RL: "6"; RG: "web,accesslog,attack,sql_injection,"; RC: "SQL injection attempt."; USER: "None";  
SRCIP: "172.20.1.127"; HOSTNAME: "(Host-172-20-1-131) 172.20.1.131->\xampp\apache\logs\access.log"; LOCATION: "(Host-172-20-1-131)  
172.20.1.131->\xampp\apache\logs\access.log"; EVENT: "[INIT]172.20.1.127 - - [26/Jun/2021  
:10:43:10 -0700] "GET  
/dashboard/pages.php?id=-999999+union+select+0x53514c2d496e6a65637469666e2d54657374,2,3--  
HTTP/1.1" 404 1057 "-" "Mozilla/5.0 [en] (X11, U;  
OpenVAS-VT 9.0.3)"[END]";
```

e

Ln 10, Col 59	100%	Unix (LF)	UTF-8
---------------	------	-----------	-------

Event Logging Best Practices



Ingress monitoring refers to surveillance and assessment of all inbound communications traffic and access attempts.

Firewalls
Gateways
Remote authentication servers
IDS/IPS tools
SIEM solutions
Anti-malware solutions



Egress monitoring is used to regulate data leaving the organization's IT environment. The term currently used in conjunction with this effort is data loss prevention (DLP) or data leak protection.

Email (content and attachments)
Copy to portable media
File Transfer Protocol (FTP)
Posting to web pages/websites
Applications/application programming interfaces (APIs)

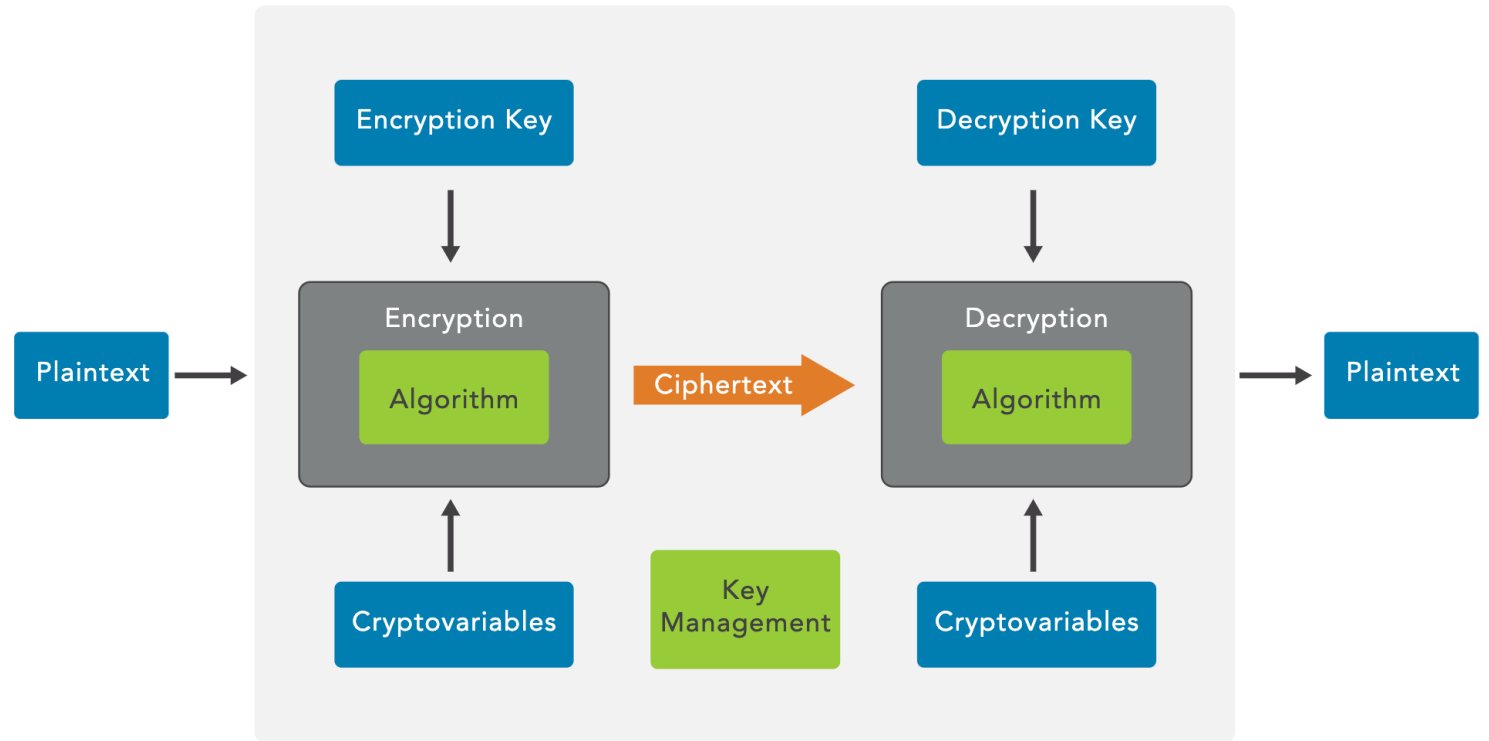
Knowledge Check : Logging

Which of the following does not normally influence an organization's retention policy for logs?

- A. Laws
- B. Audits
- C. Corporate governance
- D. Regulations



Encryption n Overview

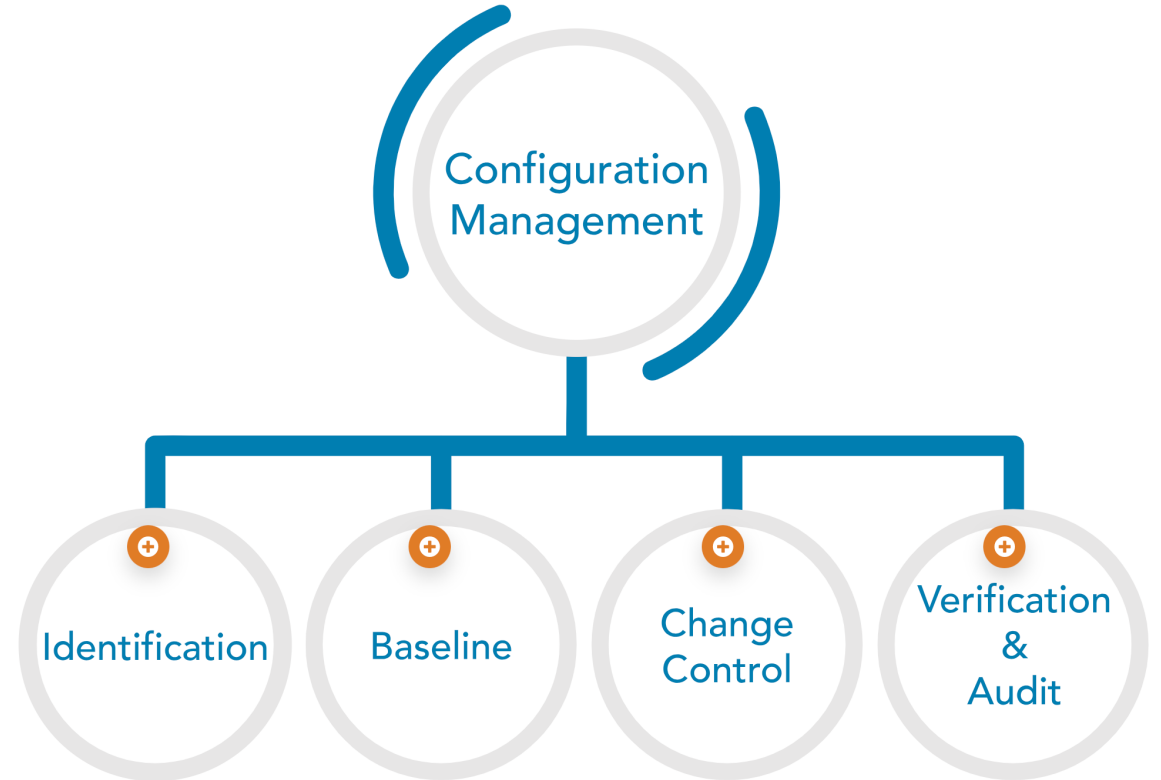


How Passwords Work

Plaintext	Hashed
Password	8be3c943b1609fffbfc51aad66d0a04adf83c9d
Password123	b2e98ad6f6eb8508dd6a14cfa704bad7f05f6b1
ThisIsMo\$tSecur3	d03409b4b6baec178a26fcc5221b1a6d32e27712

Configuration Management Overview

- Inventory. You can't protect what you don't know you have.
- Baseline. The baseline is a total inventory of all the system's components, hardware, software, data, administrative controls, documentation and user instructions.
- Update
- Patch. Update, upgrade or modification to a system or component.



Common Security Policies

Data Handling
Policy

Password
Policy

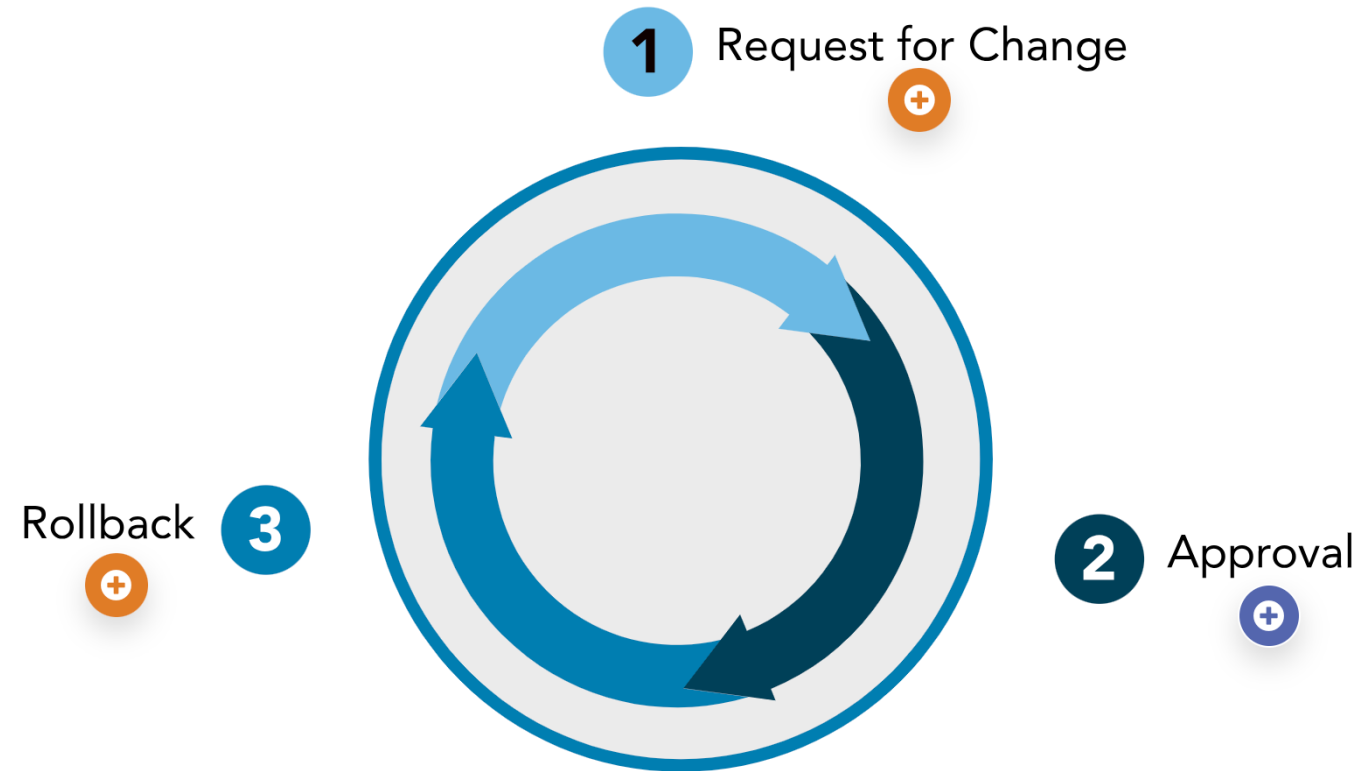
Acceptable
Use Policy

Bring Your
Own Device
(BYOD) Policy

Privacy Policy

Change
Management
Policy

Change Management Components



Knowledge Check : Privacy Policy

True or False? A privacy policy protects PII/ePHI from disclosure



Knowledge Check : Change Management Policy

For what purpose is a process required with a change management policy?

- A. To define the standards for using the organization's network and computer systems.
- B. To help protect the organization in the event it faces legal action.
- C. To establish the appropriate use of the organization's data.
- D. To ensure that systems changes are done without adversely affecting business operations.

Security Awareness Training

The purpose of awareness training is to make sure everyone knows what is expected of them, based on responsibilities and accountabilities, and to find out if there is any carelessness or complacency that may pose a risk to the organization.

- **Education:** The overall goal of education is to help learners improve their understanding of these ideas and their ability to relate them to their own experiences and apply that learning in useful ways.
- **Training:** Focuses on building proficiency in a specific set of skills or actions, including sharpening the perception and judgment needed to make decisions as to which skill to use, when to use it and how to apply it. Training can focus on low-level skills, an entire task or complex workflows consisting of many tasks.
- **Awareness:** These are activities that attract and engage the learner's attention by acquainting them with aspects of an issue, concern, problem or need.

The Importance of Security Training



The weakest link in any organization is the human, and each one of us, regardless of if we are the new intern or the executive in the corner office, each one of us has our own responsibilities about security.



Everyone contributes to improving the security environment, administratively, physically and technically.



Employees cannot follow policies and procedures if they have not received training on what the policies and procedures are.

Security Awareness Training Example :

Fire Safety

- Education may help workers in a secure server room understand the interaction of the various fire and smoke detectors, suppression systems, alarms and their interactions with electrical power, lighting and ventilation systems.
- Training would provide those workers with task-specific, detailed learning about the proper actions each should take in the event of an alarm, a suppression system going off without an alarm, a ventilation system failure or other contingency. This training would build on the learning acquired via the educational activities.
- Awareness activities would include not only posting the appropriate signage, floor or doorway markings, but also other indicators to help workers detect an anomaly, respond to an alarm and take appropriate action. In this case, awareness is a constantly available reminder of what to do when the alarms go off.

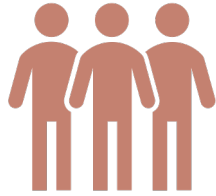
Security Awareness Training Example : Anti-Phishing Campaign

- Education may be used to help select groups of users better understand the ways in which social engineering attacks are conducted and engage those users in creating and testing their own strategies for improving their defensive techniques.
- Training will help users increase their proficiency in recognizing a potential phishing or similar attempt, while also helping them practice the correct responses to such events. Training may include simulated phishing emails sent to users on a network to test their ability to identify a phishing email.
- Raising users' overall awareness of the threat posed by phishing, vishing, SMS phishing (also called "smishing") and other social engineering tactics. Awareness techniques can also alert selected users to new or novel approaches that such attacks might be taking.

Security Awareness Training Programs



Phishing



Social Engineering :

Vishing

Pretexting

Quid pro quo

Tailgating



Password Protection