Introduction to Cybersecurity

Chapter 6

Security Policies

"If you had to write one rule to protect all of your digital life, what would it be?”

“What is the most ridiculous or strict rule you have ever seen at school or work? Did it help security or just annoy people?”

“Would you rather… have your phone stolen or your work email hacked?” Why?

- Explore how policies, standards, procedures, guidelines, and regulations shape and support individual or organizational cybersecurity
- Identifying what makes security rules effective vs. excessive

This Chapter

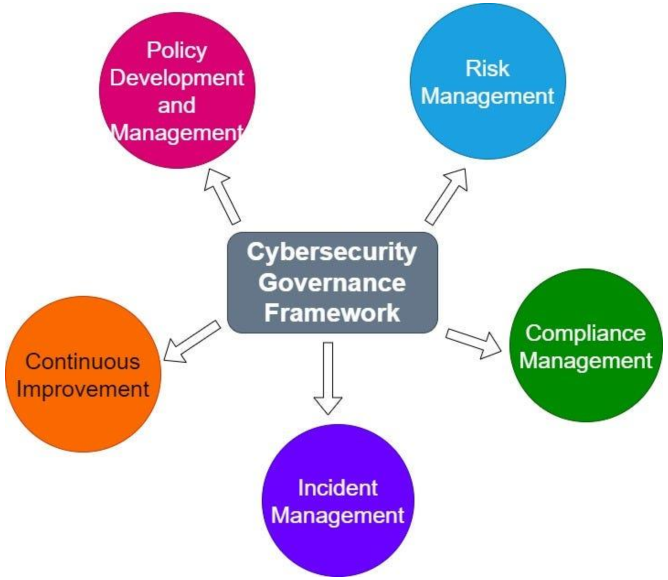
- Understand the purpose and importance of security policies
- Identify common types of cybersecurity policies (e.g., acceptable use, password, incident response)
- Recognize how standard frameworks (e.g., NIST, ISO) influence policy development
- Learn how policies are implemented and enforced in organizations
- Understand Defense in Depth

Governance

Governance

- ➢Primary framework or system through which an organization is directed and controlled
- ➢Involves decision-making processes, accountability, compliance, and the enforcement of policies and procedures to meet regulatory and strategic goals

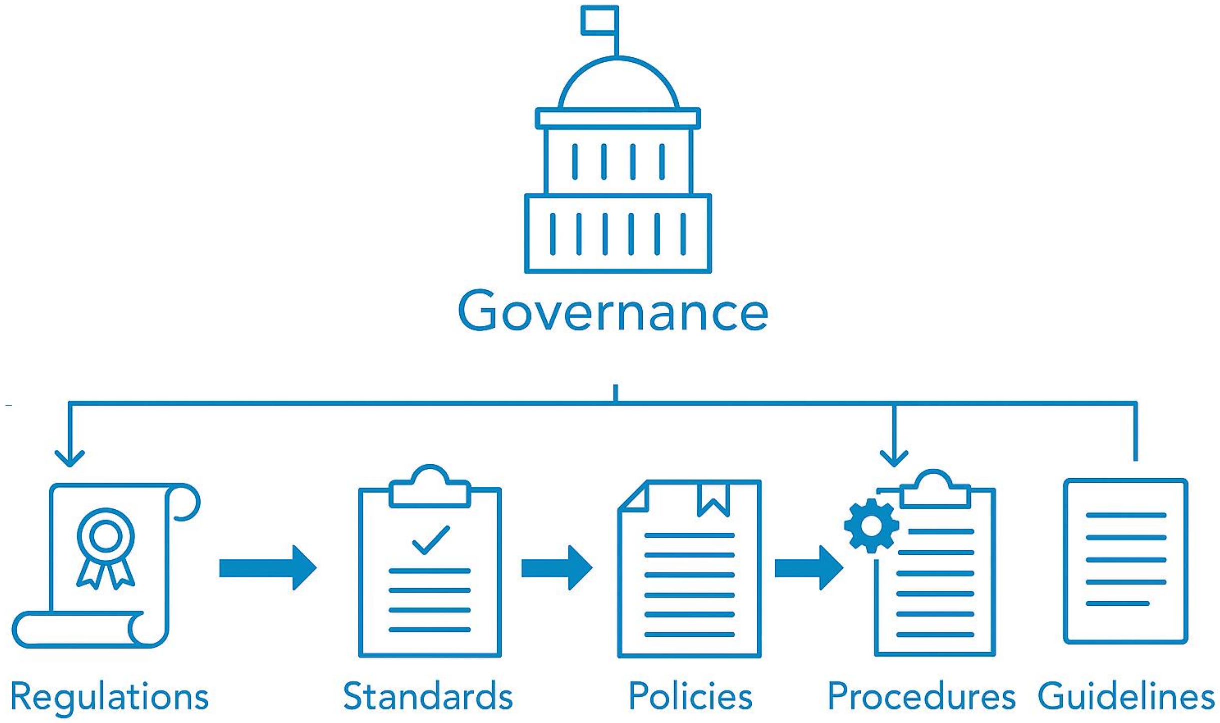
- Answers:
  - ➢Who is responsible for data protection?
  - ➢What are the rules for securing networks and systems?
  - ➢How is cyber risk managed and reported?



Example:

A hospital's board of directors establishes a governance structure to ensure patient care meets legal and ethical standards, oversees cybersecurity strategy, and monitors executive accountability

Five elements of Governance



Governance

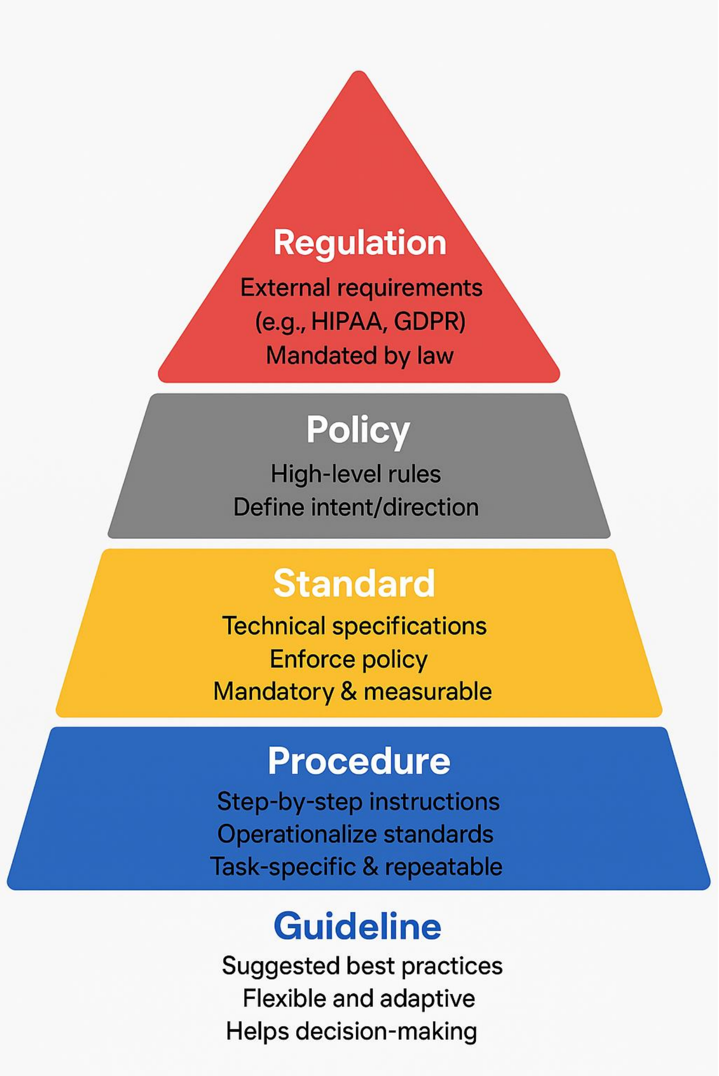
Regulations

Standards

Policies

Procedures

Guidelines



Regulation

External requirements
(e.g., HIPAA, GDPR)
Mandated by law

Policy

High-level rules
Define intent/direction

Standard

Technical specifications
Enforce policy
Mandatory & measurable

Procedure

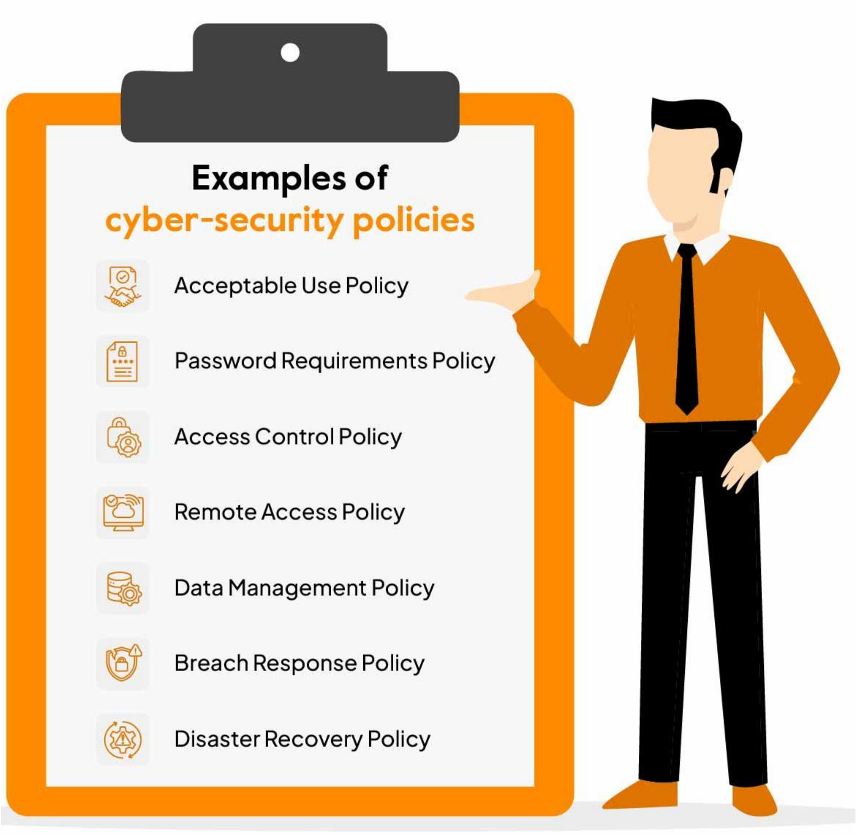
Step-by-step instructions
Operationalize standards
Task-specific & repeatable

Guideline

Suggested best practices
Flexible and adaptive
Helps decision-making

1. Policies

- A **high-level statement** created by executive management that guides decision-making and sets the direction for organizational security
- Provides guidance in all activities to ensure that the organization supports industry standards and regulations, put in place by organizational governance, such as executive management
- **Purpose**: Ensures all organizational activities align with industry standards and regulations
- Example:
  - ➢All employees must use multi-factor authentication (MFA)
  - ➢A company may have a Data Privacy Policy that outlines how employee and customer data should be collected, stored, and shared



What A Cybersecurity Policy is NOT

- It is NOT a detailed step-by-plan or procedure
- It does NOT specify precisely how a security objective will be achieved
- It is NOT (must not be) technology or vendor dependent

A cybersecurity policy sets the direction, but not the details

- It answers "What must be done?" and "Who is responsible?”
- It does not answer "How exactly is it done?"

2. Standards

- Specific mandatory rules or technical requirements that translate policies policies into measurable, enforceable rules
- Used by governance teams to provide a framework to introduce policies and procedures in support of regulations
- Ensures uniform implementation of policies/rules across systems or departments
- Mandatory and must be enforced to be effective (this also applies to policies)

Example:

- **Internal Standard-** Organization specific
  - ➢Passwords must be at least 14 characters, contain upper/lowercase letters, and be changed every 90 days
  - ➢All external emails containing PII must be encrypted using AES-256

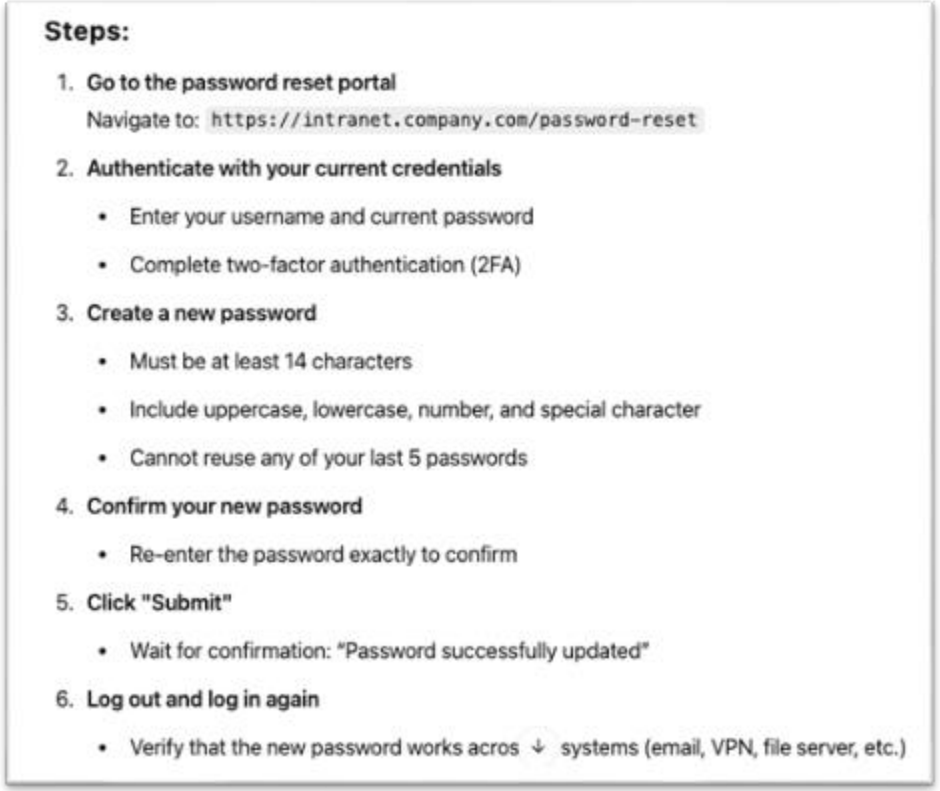
- **External Industry** Standards (Frameworks/Best Practices)
  - ➢NIST, CIS, ISO/IEC 27001to enforce internal policies and meet regulatory requirements

3. Procedures

- Detailed steps to complete a task that support departmental or organizational policies
- Ensures repeatable and consistent execution of security tasks
- Detailed enough and yet not too difficult that only a small group (or a single person) will understand.

Example

- To reset your password, follow these 6 steps…
- Installing operating systems, performing a system backup, granting access rights to a system
- An Incident Response Procedure



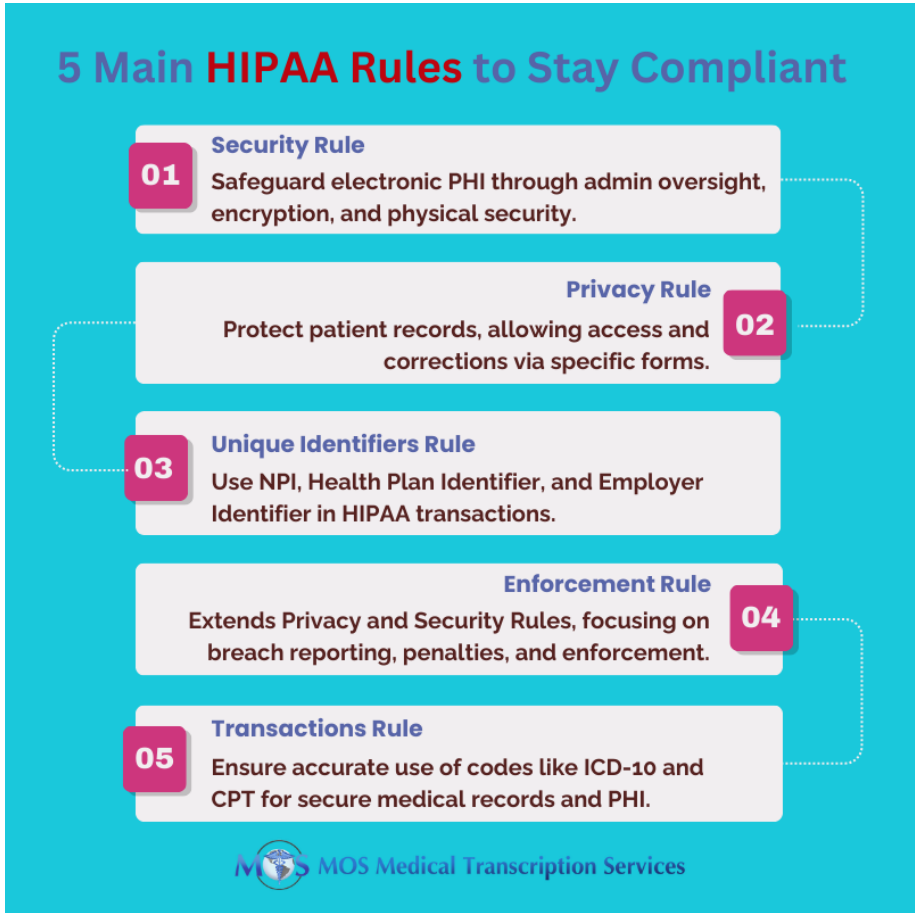
Steps:

1. **Go to the password reset portal**
   Navigate to: `https://intranet.company.com/password-reset`
2. **Authenticate with your current credentials**
   - Enter your username and current password
   - Complete two-factor authentication (2FA)
3. **Create a new password**
   - Must be at least 14 characters
   - Include uppercase, lowercase, number, and special character
   - Cannot reuse any of your last 5 passwords
4. **Confirm your new password**
   - Re-enter the password exactly to confirm
5. **Click "Submit"**
   - Wait for confirmation: "Password successfully updated"
6. **Log out and log in again**
   - Verify that the new password works acros ↓ systems (email, VPN, file server, etc.)

4. Regulations

Commonly issued in the form of laws, usually from government (not to be confused with governance), and typically carry financial penalties for noncompliance

- Legal requirements issued by government bodies
- Compliance is mandatory; noncompliance can result in legal and financial penalties.
- **Example**:
- Health Insurance Portability and Accountability Act (HIPAA) is a U.S. regulation requiring organizations to protect sensitive patient health information.



5 Main HIPAA Rules to Stay Compliant

01 **Security Rule**
Safeguard electronic PHI through admin oversight, encryption, and physical security.

02 **Privacy Rule**
Protect patient records, allowing access and corrections via specific forms.

03 **Unique Identifiers Rule**
Use NPI, Health Plan Identifier, and Employer Identifier in HIPAA transactions.

04 **Enforcement Rule**
Extends Privacy and Security Rules, focusing on breach reporting, penalties, and enforcement.

05 **Transactions Rule**
Ensure accurate use of codes like ICD-10 and CPT for secure medical records and PHI.

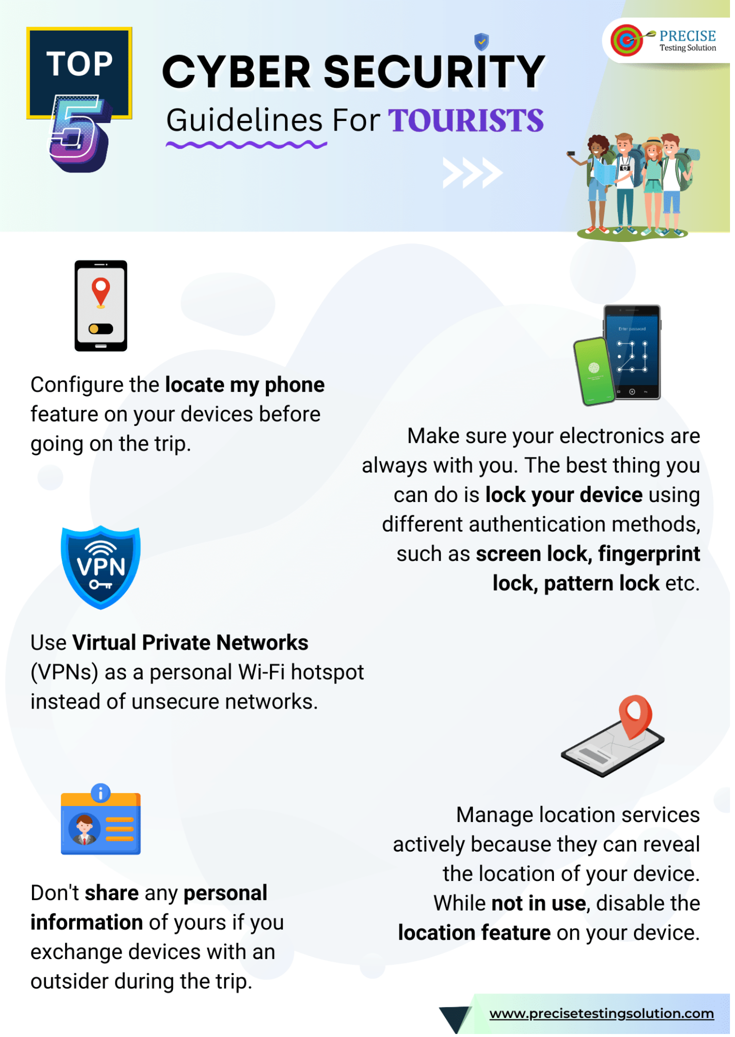
MOS Medical Transcription Services

5. Guideline

- Recommended best practices that offer flexibility and are not mandatory
- Helps staff make decisions in situations not covered by strict policies or standards
- Support decision-making in areas where strict standards/policies may not apply

Example:

- ➢Use a strong, unique password for your email account
- ➢Avoid clicking on links or attachments from unknown senders



TOP 5

CYBER SECURITY

Guidelines For **TOURISTS**

PRECISE Testing Solution

Configure the **locate my phone** feature on your devices before going on the trip.

Make sure your electronics are always with you. The best thing you can do is **lock your device** using different authentication methods, such as **screen lock, fingerprint lock, pattern lock** etc.

Use **Virtual Private Networks** (VPNs) as a personal Wi-Fi hotspot instead of unsecure networks.

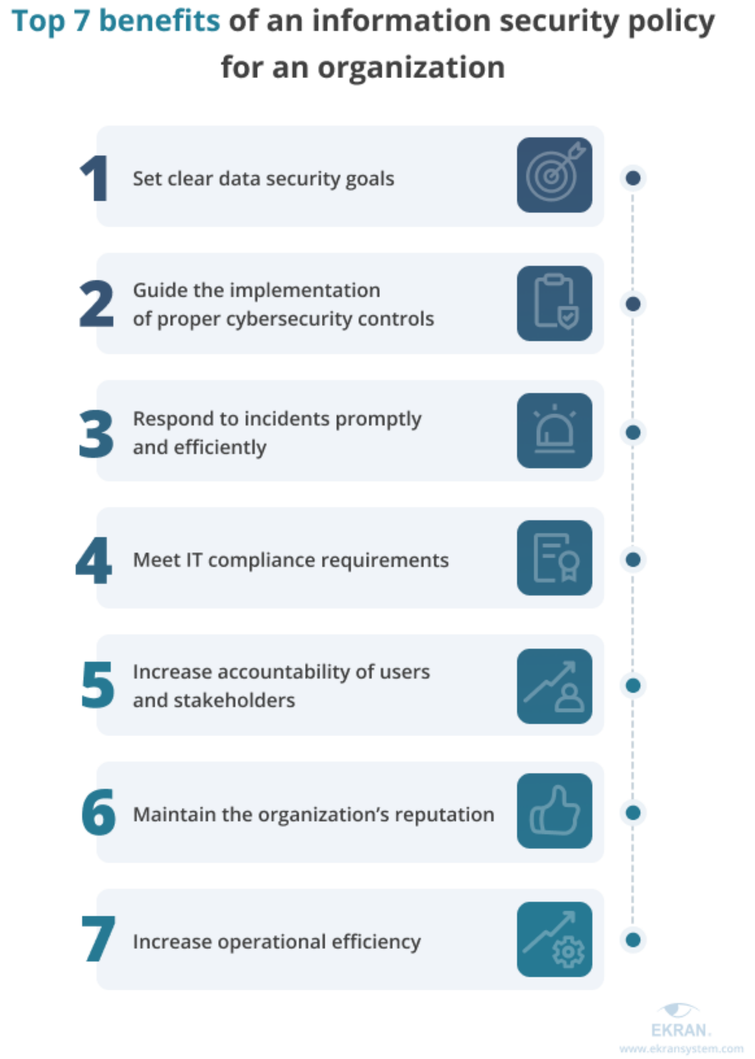
Manage location services actively because they can reveal the location of your device. While **not in use**, disable the **location feature** on your device.

Don't **share** any **personal information** of yours if you exchange devices with an outsider during the trip.

www.precisetestingsolution.com

Exploring Security Policies

- ➢**Security policies:** Written documents that identify a security plan
- ➢All policies must support any regulatory and contractual obligations of the organization
- ➢ A security policy should:
  - ➢Identify all of a company's assets
  - ➢Identify all potential threats to those assets
  - ➢Define rules, expectations, and the overall approach to maintaining data confidentiality, integrity, and availability
  - ➢Outline employee responsibilities
  - ➢Help everyone understand the processes to protect the organization



Top 7 benefits of an information security policy for an organization

1. Set clear data security goals
2. Guide the implementation of proper cybersecurity controls
3. Respond to incidents promptly and efficiently
4. Meet IT compliance requirements
5. Increase accountability of users and stakeholders
6. Maintain the organization's reputation
7. Increase operational efficiency

Data use/usage policy

- Set of guidelines and rules that dictate how an organization's data can and should be used
- **Focus**: Primarily concerns how an organization uses, handles, stores, and manages the data it collects
- **Content**: May include details about data access controls, data security measures, compliance with regulations, and ethical considerations in data usage
- **Audience**: Often aimed at internal stakeholders, such as employees and partners, to guide them on how to appropriately handle and use the data they have access to

For example:

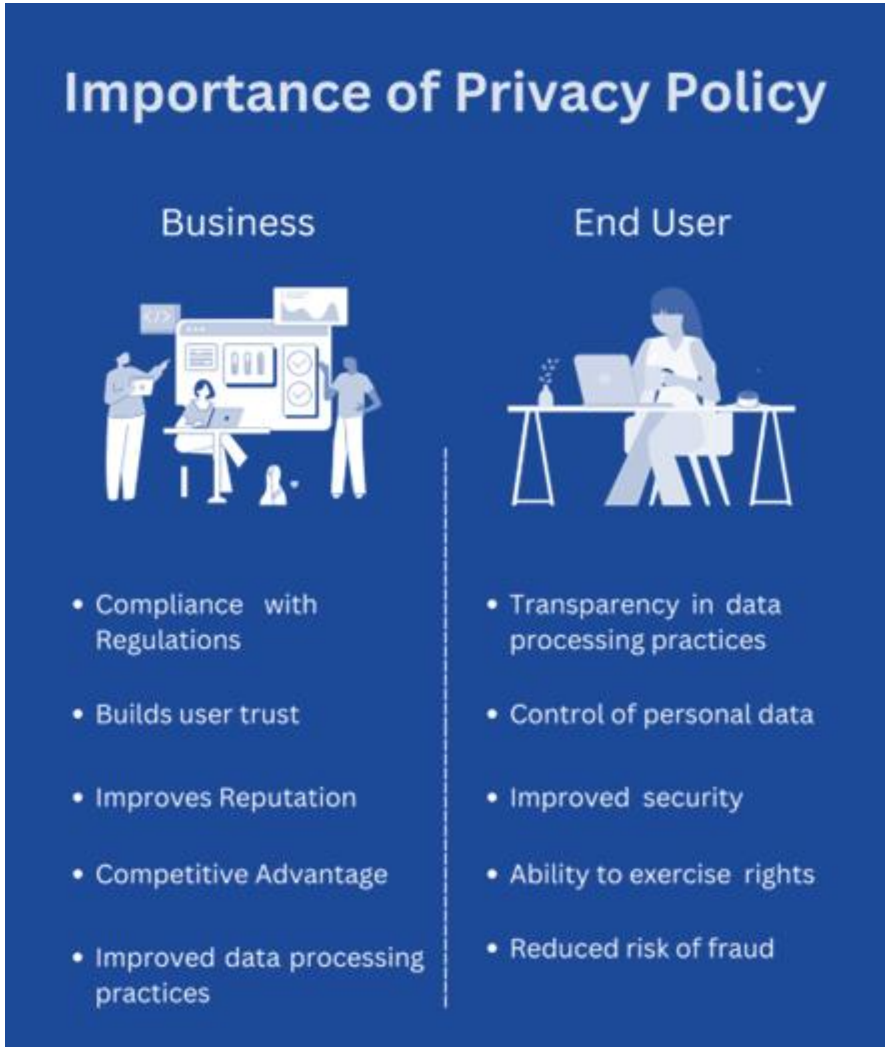
- ➢Classifying credit card data as confidential can help ensure compliance with the PCI DSS
- ➢ One of the requirements of this standard is to encrypt credit card information

https://ourdataourselves.tacticaltech.org/data-use-policy/

Privacy Policy

- Legal document that explains how a website or app collects and uses personal information
- **Focus**: Concentrates on how an organization collects, uses, stores, and protects the personal information of its customers or user
- **Content**:
  - ➢ What information is collected
  - ➢ Why the information is collected
  - ➢ How the information is used
  - ➢ Whether the information is shared with others
  - ➢ The methods used to collect the data
- **Audience**: Directed primarily at external parties, particularly the users or customers

https://policies.google.com/privacy



Importance of Privacy Policy

Business

- Compliance with Regulations
- Builds user trust
- Improves Reputation
- Competitive Advantage
- Improved data processing practices

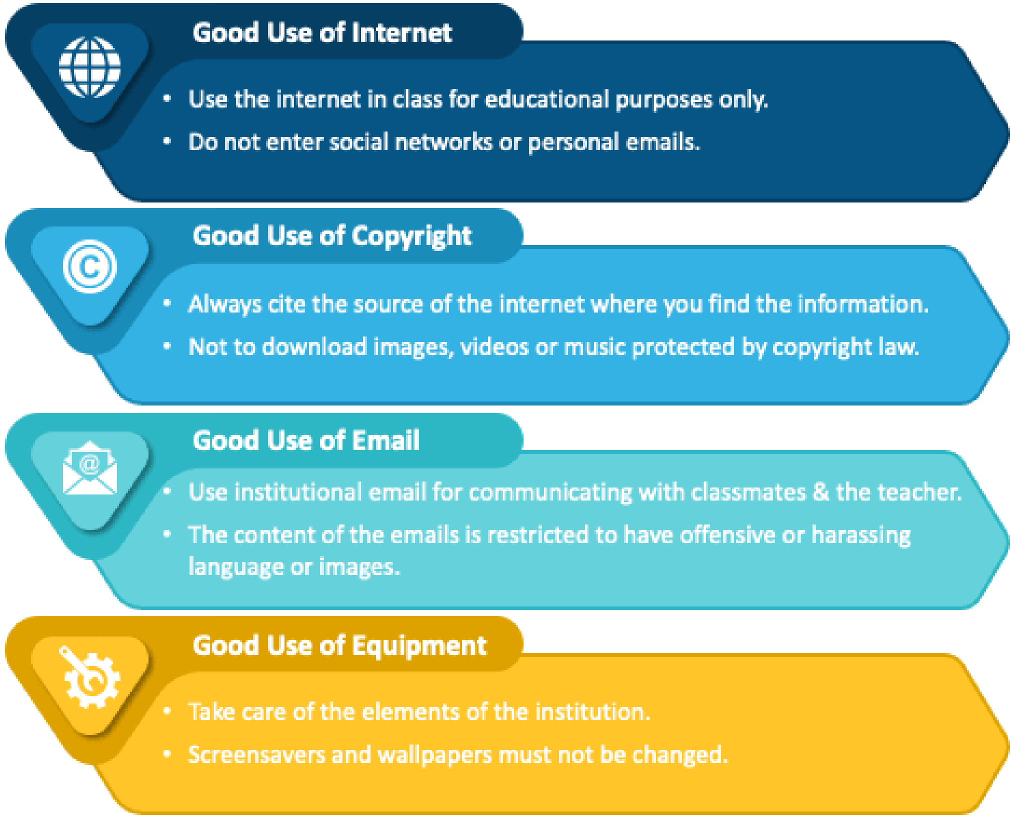
End User

- Transparency in data processing practices
- Control of personal data
- Improved security
- Ability to exercise rights
- Reduced risk of fraud

Acceptable use policy

- Set of rules that outlines how users can and can't use an organization's IT resources
- Outlines the acceptable behaviors and prohibited activities for users of IT resources, including computers, networks, email services, and internet access

- AUPs can include rules about:
  - Accessing restricted information
  - Accessing company resources
  - Using company assets for business/company use
  - Opening questionable email attachments
  - Using public Wi-Fi services



Good Use of Internet

- Use the internet in class for educational purposes only.
- Do not enter social networks or personal emails.

Good Use of Copyright

- Always cite the source of the internet where you find the information.
- Not to download images, videos or music protected by copyright law.

Good Use of Email

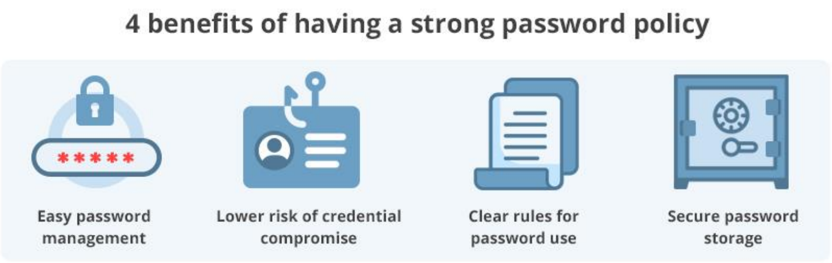
- Use institutional email for communicating with classmates & the teacher.
- The content of the emails is restricted to have offensive or harassing language or images.

Good Use of Equipment

- Take care of the elements of the institution.
- Screensavers and wallpapers must not be changed.

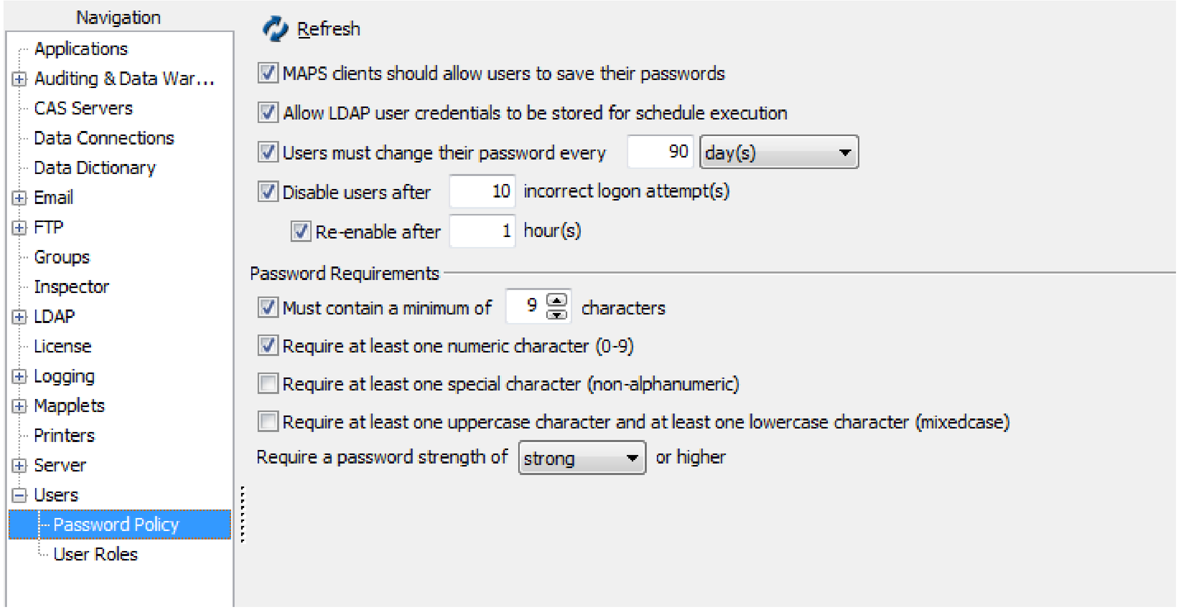
Password policy

- Set of rules created to enhance security by encouraging users to employ strong passwords and use them properly


4 benefits of having a strong password policy
*****
Easy password management
Lower risk of credential compromise
Clear rules for password use
Secure password storage

Components:

- ➢ Password Complexity Requirements
- ➢ Password Lifetime/Expiration
- ➢ Password History and Reuse Limitations
- ➢ Management of Default Passwords
- ➢ User Education and Training Guidelines
- ➢ Password Reset Procedures
- ➢ Account Lockout Mechanisms
- ➢ Password Recovery Processes



☑ MAPS clients should allow users to save their passwords

☑ Allow LDAP user credentials to be stored for schedule execution

☑ Users must change their password every 90 day(s)

☑ Disable users after 10 incorrect logon attempt(s)

☑ Re-enable after 1 hour(s)

Password Requirements

☑ Must contain a minimum of 9 characters

☑ Require at least one numeric character (0-9)

☐ Require at least one special character (non-alphanumeric)

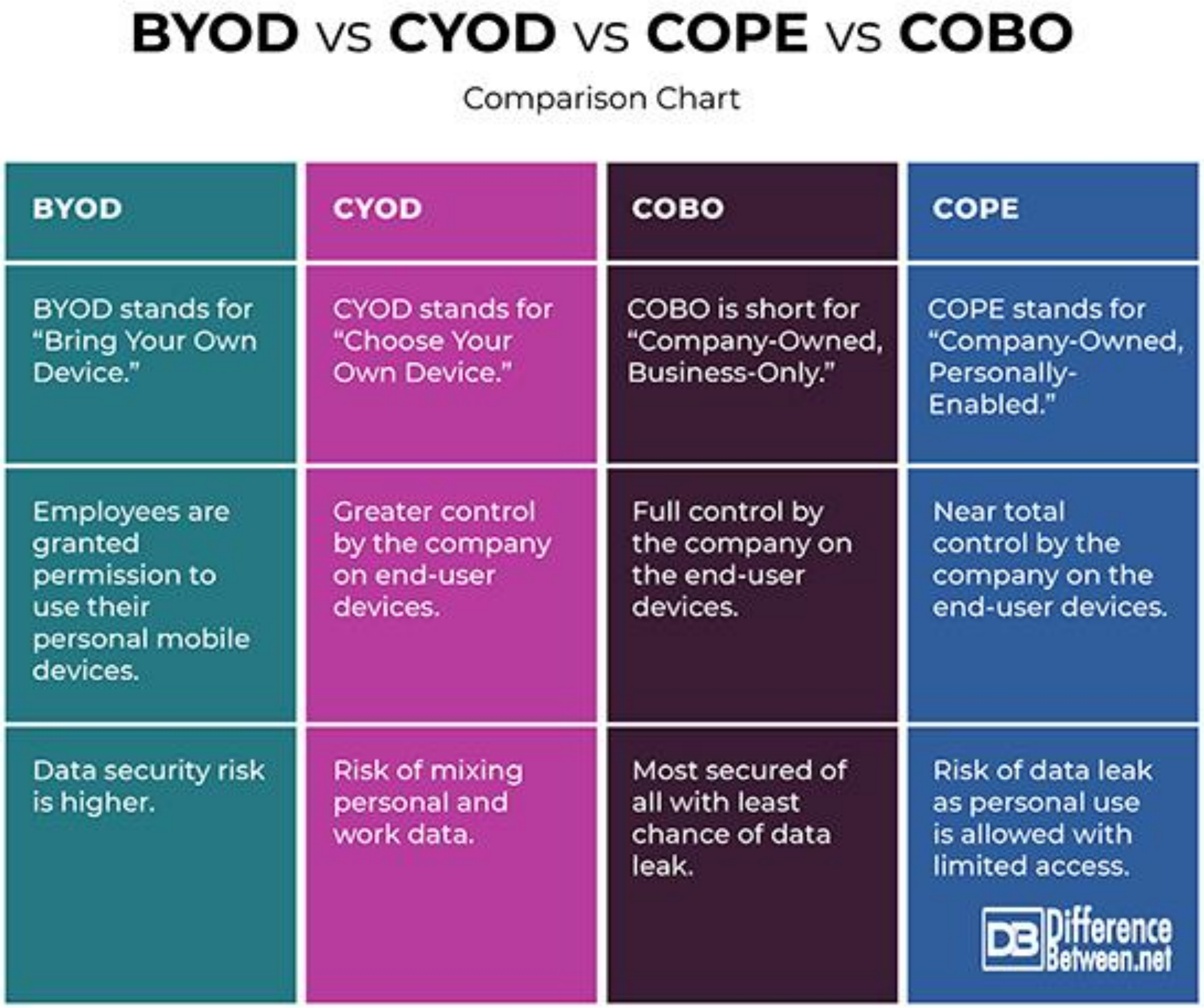
☐ Require at least one uppercase character and at least one lowercase character (mixedcase)

Require a password strength of strong or higher

BYOD policy

- BYOD policy
  - ➢A Bring Your Own Device policy is a corporate IT policy that allows employees to use their own devices for work
  - ➢Covers aspect as: device eligibility, allowed applications, user responsibilities, device inspection and access rights, consequences of non-compliance, policy acceptance and user agreement
- Mandatory vacations
  - ➢Require employees to take time away from the job
  - ➢Helps reduce fraud and discover malicious activities while the employee is away
- Job rotation Policy
  - ➢Require employees to change roles on a regular basis
  - ➢Helps ensure that employees cannot continue with fraudulent activity indefinitely

https://www.devicemagic.com/blog/bring-your-own-device-policy-pros-cons/



BYOD vs CYOD vs COPE vs COBO

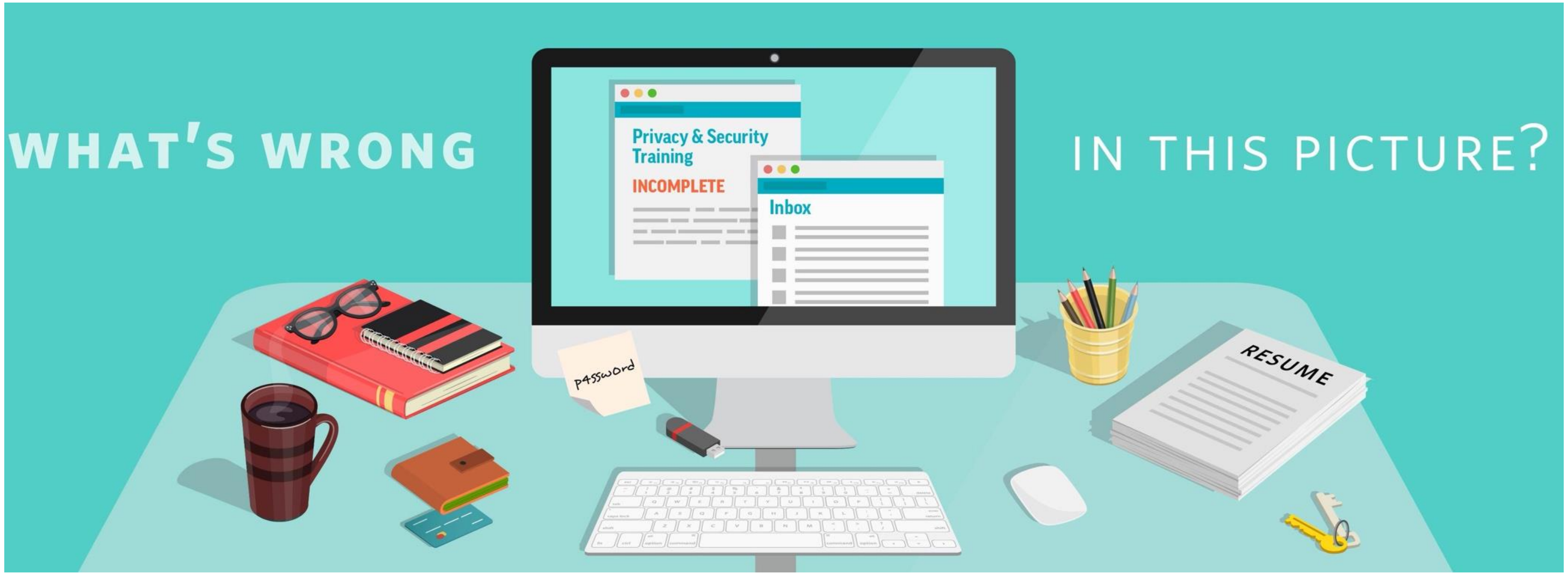
Comparison Chart

BYOD	CYOD	COBO	COPE
BYOD stands for “Bring Your Own Device.”	CYOD stands for “Choose Your Own Device.”	COBO is short for “Company-Owned, Business-Only.”	COPE stands for “Company-Owned, Personally-Enabled.”
Employees are granted permission to use their personal mobile devices.	Greater control by the company on end-user devices.	Full control by the company on the end-user devices.	Near total control by the company on the end-user devices.
Data security risk is higher.	Risk of mixing personal and work data.	Most secured of all with least chance of data leak.	Risk of data leak as personal use is allowed with limited access.

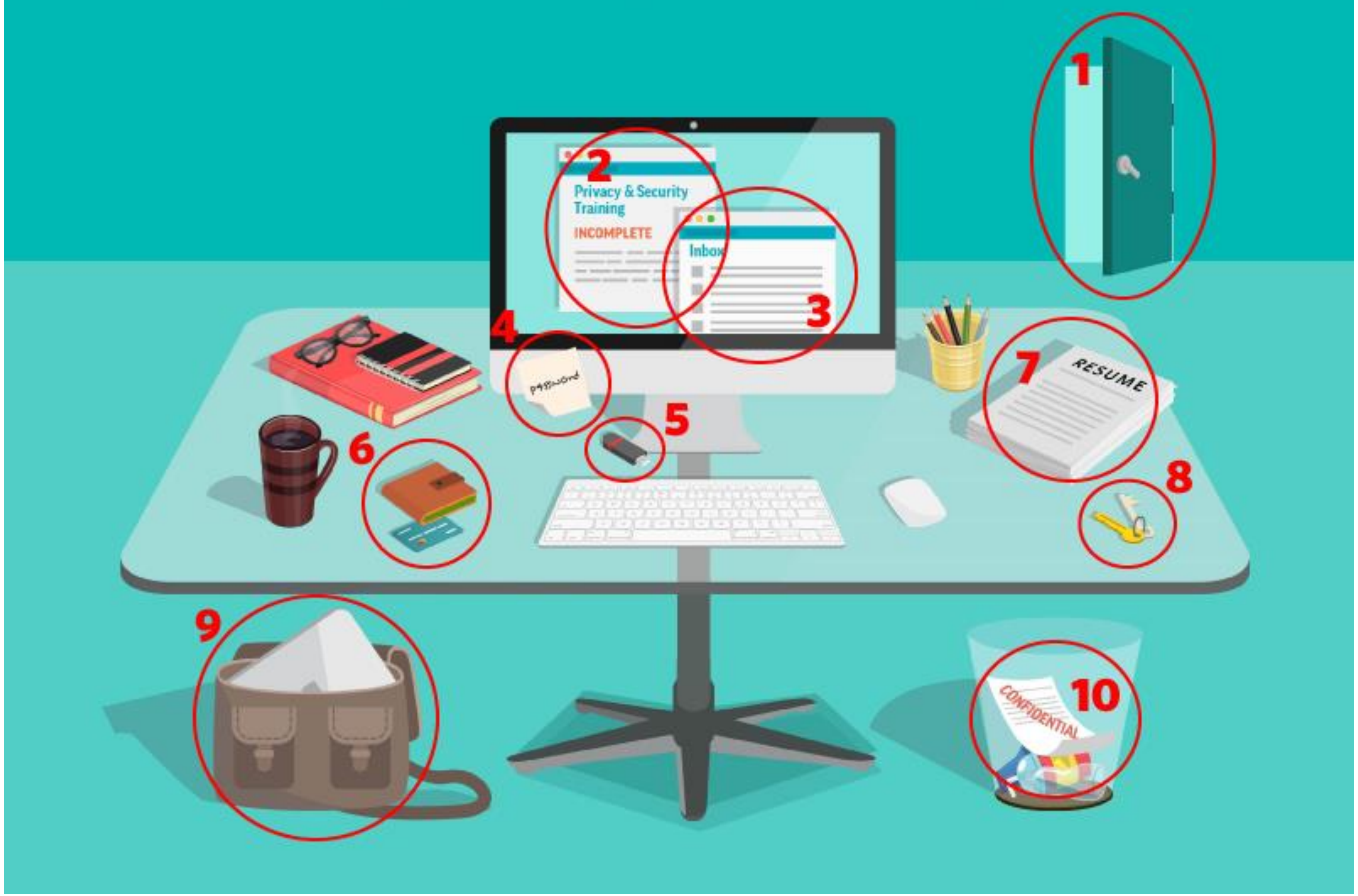
Source: https://www.differencebetween.net/business/difference-between-byod-cyod-cope-and-cobo/

Clean desk policy

- Clean desk policy
  - Requires users to organize their areas
  - Reduces risk of possible data theft
  - Reminds users to secure sensitive data
  - May include a statement about not writing down passwords



WHAT'S WRONG IN THIS PICTURE?



Other Security policies

- **Remote access policy (RAP):** details if and how network resources are remotely accessed

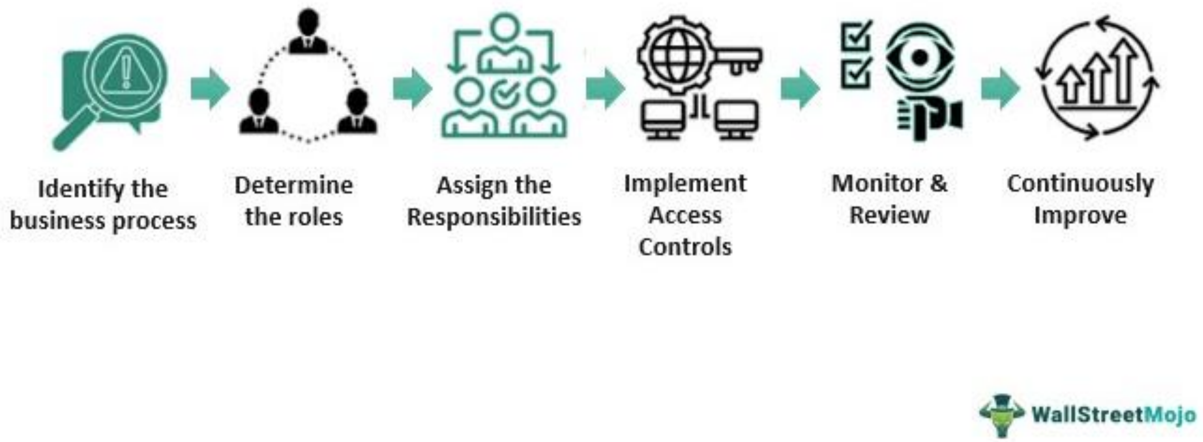
- **Onboarding policy:** details how a new employee accesses network resources

- **Offboarding policy:** details the removal of network resource access for a resigning or resigned employee

- **Credential policy**: details processes for identity and authentication (or credentials) management

Separation of duties Policy

- ➢Cybersecurity risk management technique that reduces the risk of errors and insider threats
- ➢Prevents any single person or entity from being able to complete all the functions of a process
- ➢Divides tasks between employees



Identify the business process

Determine the roles

Assign the Responsibilities

Implement Access Controls

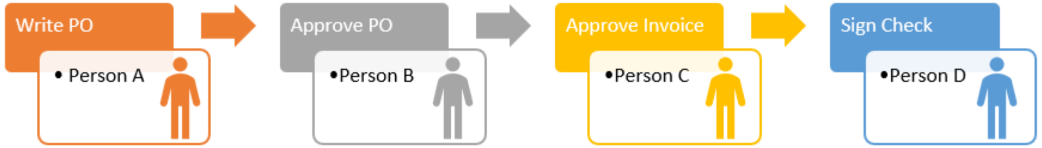
Monitor & Review

Continuously Improve

WallStreetMojo

Examples:

- ➢In Cloud Key Management Service, ensuring that a user doesn't have all the permissions needed to access and decrypt data
- ➢In the financial industry, ensuring that staff who enter invoices don't also approve them



Write PO
- Person A

Approve PO
- Person B

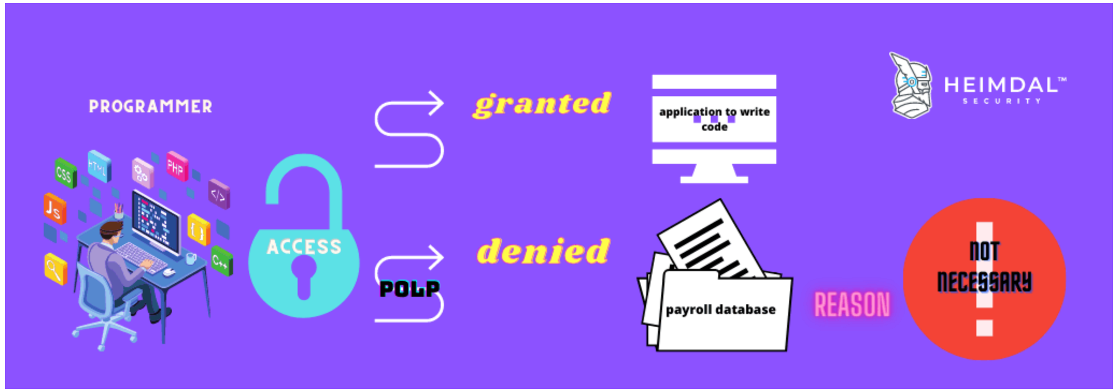
Approve Invoice
- Person C

Sign Check
- Person D

Least Privilege Policy

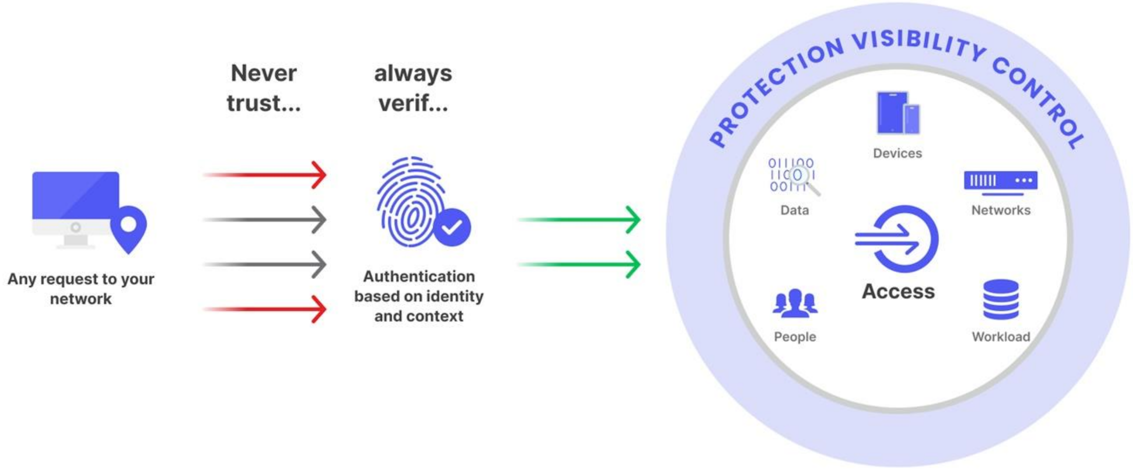
- Principle of least privilege (POLP) is an information security concept that gives users, typically employees, the minimum level of access that they will need to complete their job responsibilities
- CISA (Cybersecurity and Infrastructure Security Agency) recommends using least privilege as a cybersecurity best practice
- Minimizes potential damage from accidents or malicious actions

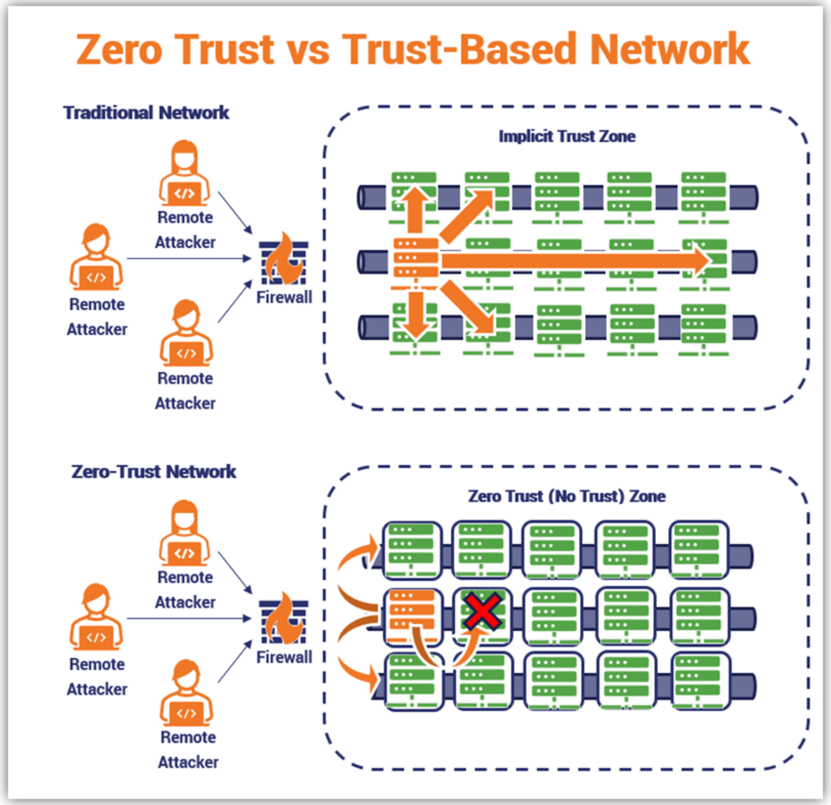
- Benefits
  - ➢Reduced attack surface
  - ➢Enhanced security
  - ➢Improved performance
  - ➢Reduced system downtime
  - ➢Improved audit readiness
  - ➢Reduced risk from user errors



Zero Trust Architecture

- Never trust, always verify – assumes no user or device is trustworthy by default, even inside the network
  - Unlike traditional security models that rely on a defined network perimeter, Zero Trust operates on the principle that no user or system should be automatically trusted
  - NIST 800-207- Zero Trust Architecture- comprehensive guide for implementing Zero Trust

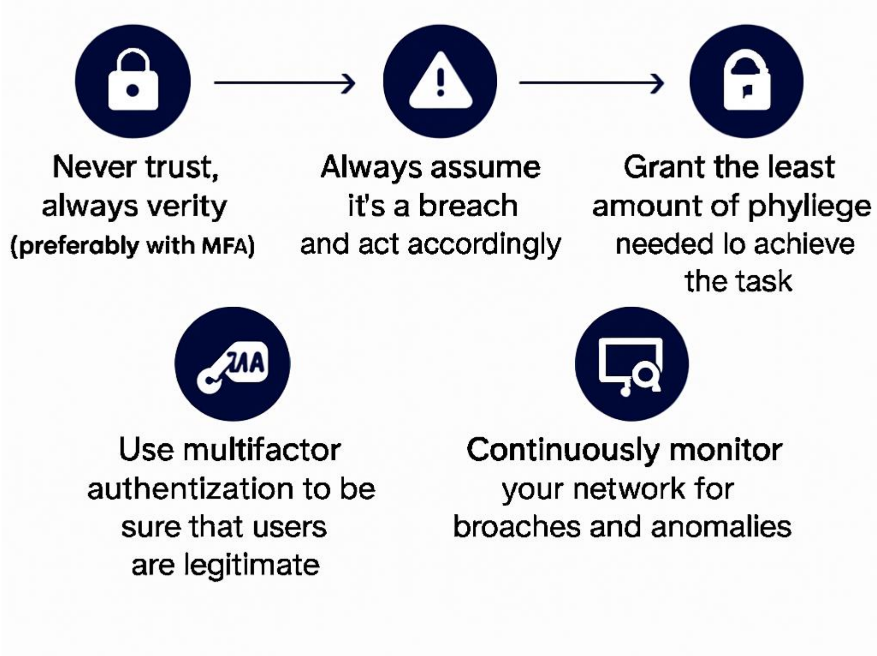

Never trust...
always verif...
Any request to your network
Authentication based on identity and context
PROTECTION VISIBILITY CONTROL
Devices
Data
Networks
Access
People
Workload



https://www.thesslstore.com/blog/the-rise-of-zero-trust-threats-are-no-longer-perimeter-only-concerns/

Five Key Tenets of Zero Trust

1. **Never trust, always verify** – authenticate and authorize based on all available data points, including user identity, location, device health, and the service or workload the user is interacting with
2. **Assume breach** – Continuously verify and validate each request
3. **Grant least privilege –** Only the access needed for the specific task
4. **Use MFA** – Ensure users are who they claim to be
5. **Monitor continuously** – Continuously monitor your network for breaches and anomalies


Never trust, always verity (preferably with MFA)
Always assume it's a breach and act accordingly
Grant the least amount of phyllege needed lo achieve the task
Use multifactor authentization to be sure that users are legitimate
Continuously monitor your network for broaches and anomalies

Policy Template

SANS Institute Security Policy Templates
SANS provides a comprehensive set of information security policy templates that are free to use and can be tailored to your organization's needs. These templates cover various aspects of cybersecurity, including acceptable use, data protection, and incident response

https://www.sans.org/information-security-policy/

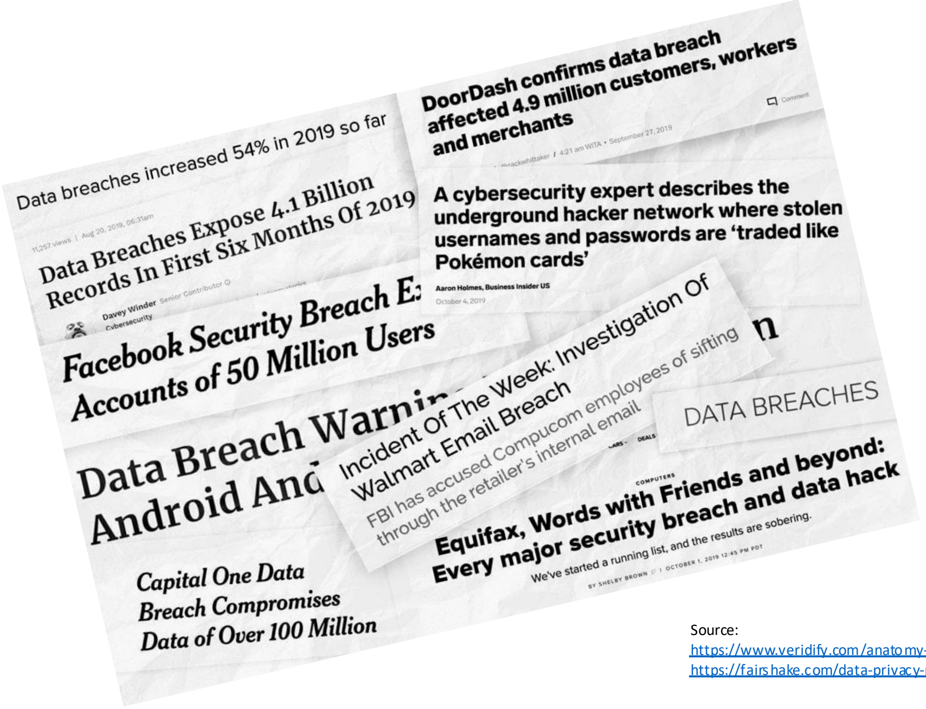
CIS Policy Template Guide
Center for Internet Security (CIS) provides a Policy Template Guide that aligns with the NIST Cybersecurity Framework. This guide includes customizable templates to help organizations develop policies corresponding to various cybersecurity controls

https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2024/08/cis-ms-isac-nist-cybersecurity-framework-policy-template-guide-2024.pdf

Protecting Data

- Classifying data types
- PII and Health Information
- Data governance
- Privacy enhancing technologies
- Data retention policies
- Data sanitization

Data at rest **Data in transit** **Data in use**


Data breaches increased 54% in 2019 so far

11,257 views | Aug 20, 2019, 06:31am

Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019

Davey Winder Senior Contributor
Cybersecurity

DoorDash confirms data breach affected 4.9 million customers, workers and merchants

@zackwhittaker / 4:21 am WITA • September 27, 2019

Comment

A cybersecurity expert describes the underground hacker network where stolen usernames and passwords are 'traded like Pokémon cards'

Aaron Holmes, Business Insider US
October 4, 2019

Facebook Security Breach E
Accounts of 50 Million Users

Data Breach Warnin
Android And

Incident Of The Week: Investigation Of Walmart Email Breach

FBI has accused Compucom employees of sifting through the retailer's internal email

DATA BREACHES

CARS DEALS

COMPUTERS

Equifax, Words with Friends and beyond: Every major security breach and data hack

We've started a running list, and the results are sobering.

BY SHELBY BROWN | OCTOBER 1, 2019 12:45 PM PDT

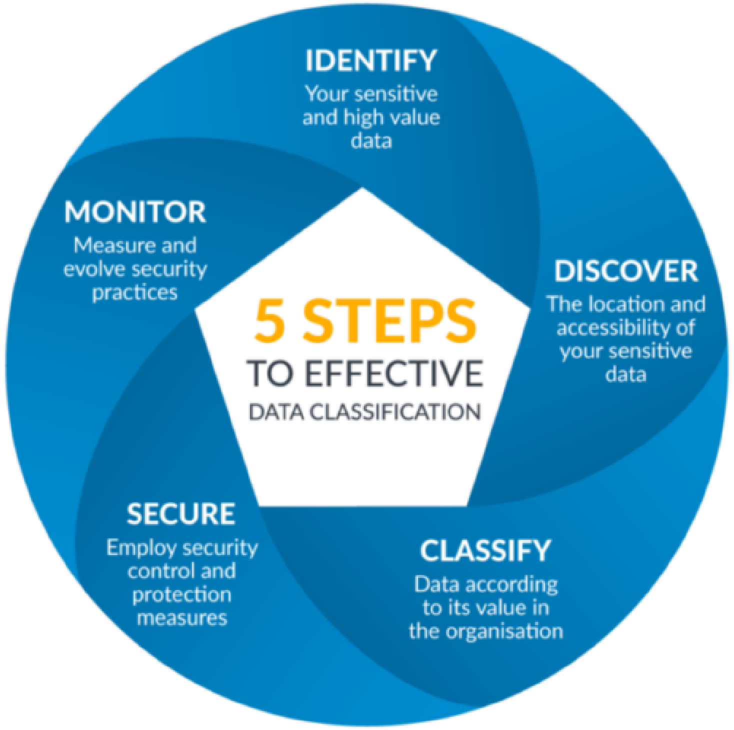
Capital One Data Breach Compromises Data of Over 100 Million

Source:
https://www.veridify.com/anatomy-of-a-data-breach/
https://fairshake.com/data-privacy-rights-guide/

Classifying Data Types

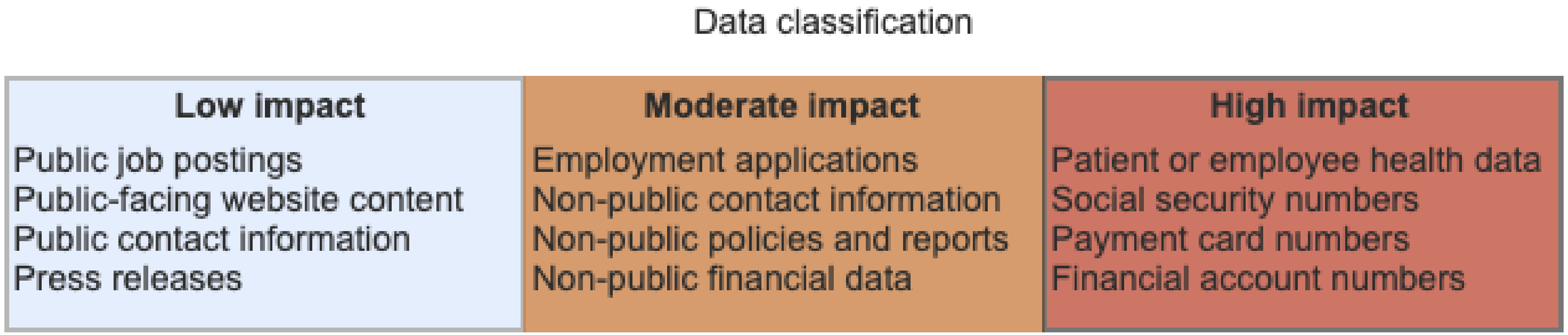
- **Data classification**: process of labeling data based on its sensitivity, type, and business value
- Helps organizations make informed decisions about how to manage, protect, and share data
- Data classifications defined in security policy
  - ➢Public, Private, Confidential, Financial information, Customer
- Data is classified as low, medium, or high based on its overall classification (NIST 800-53)

Can you think of any low, moderate or high impact data?


IDENTIFY
Your sensitive and high value data
DISCOVER
The location and accessibility of your sensitive data
CLASSIFY
Data according to its value in the organisation
SECURE
Employ security control and protection measures
MONITOR
Measure and evolve security practices
5 STEPS
TO EFFECTIVE
DATA CLASSIFICATION

High, Moderate, and Low impact data based on the NIST SP 800-60 guidelines

Security Objective	Low Impact	Moderate Impact	High Impact
Confidentiality	Limited harm	Serious harm	Severe/Catastrophic
Integrity	Limited harm	Serious harm	Severe/Catastrophic
Availability	Limited harm	Serious harm	Severe/Catastrophic

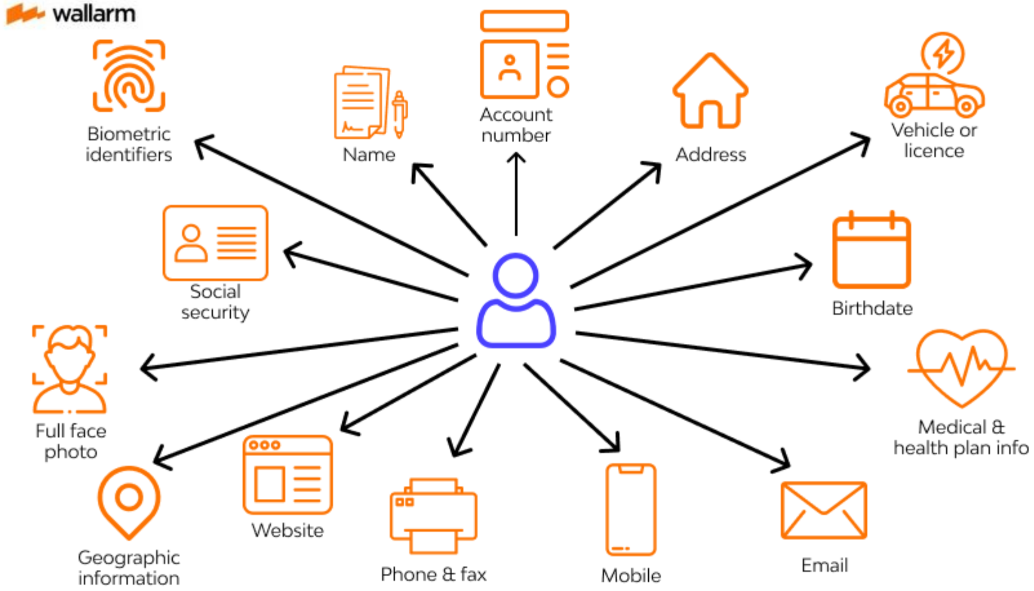


Data classification

Low impact	Moderate impact	High impact
Public job postings	Employment applications	Patient or employee health data
Public-facing website content	Non-public contact information	Social security numbers
Public contact information	Non-public policies and reports	Payment card numbers
Press releases	Non-public financial data	Financial account numbers

PII and Health Information

- Personally identifiable information (PII)
  - ➢Any data that can be used to identify a specific individual, either directly or indirectly
  - ➢Breaches can lead to identity theft, fraud
  - ➢Protected under laws like GDPR, CCPA, and NIST standards
  - ➢Includes information such as:
    - ▪ Full name, birthdate, address, biometric data, identifying numbers
  - ➢Requires special handing
  - ➢Employees should be trained not to give out PII

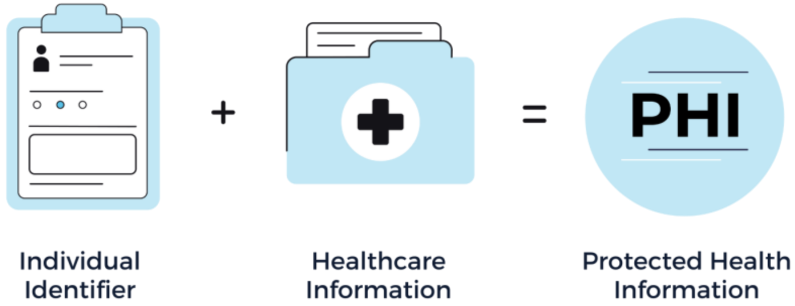


PII and Health Information

Protected Health Information (PHI)

- Subset of PII that includes health-related information created, received, or maintained by healthcare entities
- Must be linked to an individual to qualify as PHI
- Covered under HIPAA
- Only applies when handled by covered entities (healthcare providers, insurers, etc.)

- Examples:
  - Insurance policy number, medical record number, test results, device serial numbers, biometrics



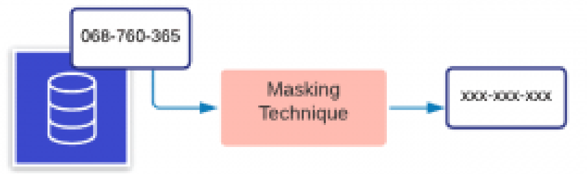
Data Governance

Regulations and standards

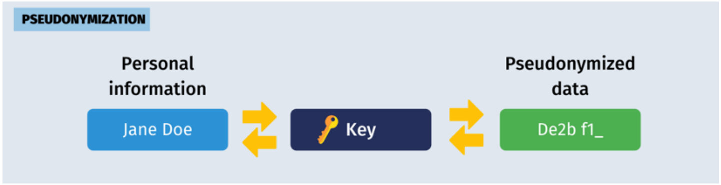
- Health insurance portability and accountability act (HIPAA)
    - ➢ US federal regulation consisting of standards to protect sensitive patient information and data
- General data protection regulation (GDPR)
    - ➢ European Union (EU) law consisting of privacy and data protection standards
- Sarbanes-Oxley Act (SOX)
    - ➢ Protects financial information of public companies
- PCI DSS (Payment Card Industry Data Security Standard)
    - ➢ Information security standard designed to reduce payment card fraud by increasing security controls around cardholder data
- Federal information security management act (FISMA)
    - ➢ US federal regulation defining information and data security policies for federal agencies.

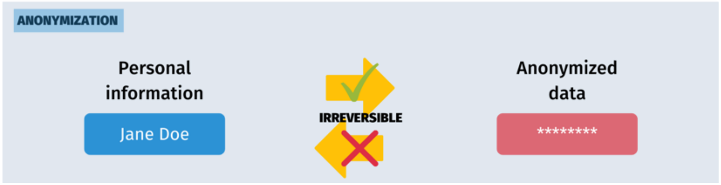
Privacy Enhancing Technologies

- **Data masking**: Hide parts of data to prevent exposure
  - ➢Ex: masking the last four digits of a credit card number with asterisks



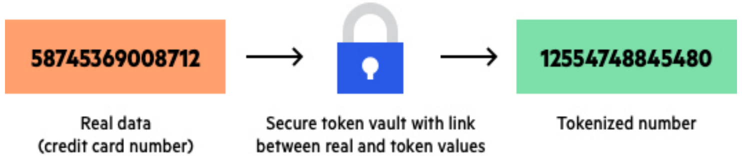
- **Pseudonymization**: Replaces identifying information with random codes
  - ➢Ex: “Age” data could be encrypted with an X key and the “Last name” and “First name” values with a Y key





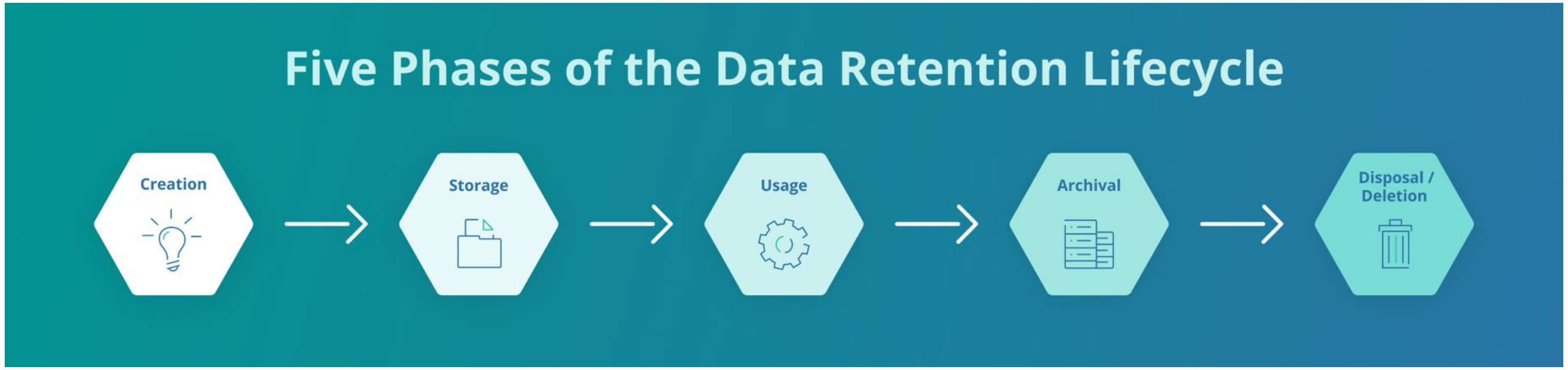
- **Anonymization**: Permanently remove personal identifiers
  - ➢Ex: Remove names, addresses, or phone numbers

- **Tokenization**: Encrypts PII and replaces a pseudonym with an unrecognizable token
  - Ex: A customer's 16-digit credit card number can be replaced with a 16-digit token. For example, 1234-4321-8765-5678 could be replaced with 6f7%gf38hfU



Data Retention Policies

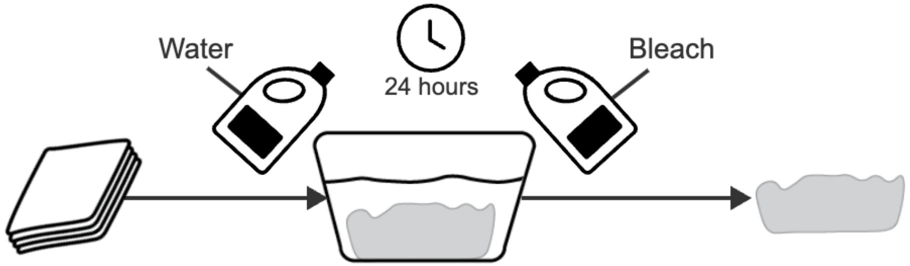
- Goal
  - ➢Identify where data is stored
  - ➢Identify how long it is stored
  - ➢How it is ultimately archived or destroyed
- Retention policies include
  - ▪ Guidelines for storing, archiving, and destroying data
  - ▪ Regulatory compliance (e.g., GDPR, HIPAA, SOX)
  - ▪ Legal defense readiness (evidence preservation)
  - ▪ Support for disaster recovery plans
  - ▪ Ensuring access to mission-critical data



Secure Data Destruction

Paper documents:

- Burning
  - ➢Burning turns paper to ash in a high-temperature incinerator
- Shredding
  - ➢Shredding turns paper into small confetti-like shreds using rotating blades
- Pulping
  - ➢Pulping turns paper into a soft mush, called pulp, by soaking the paper in water and bleach



Secure Data Destruction

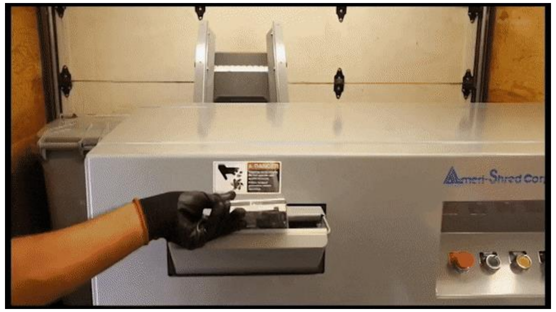
Digital documents:

- **Hardware shredding:** turns hardware into small metal pieces using specialized blades

- **Pulverizing**: turns hardware into tiny fragments or powder by crushing

- **Degaussing**: wipes data from magnetic media using strong magnetic fields

- **Puncturing**: punches multiple pins into the hard drive, and the chips contained within them



Business continuity

- **Business continuity (BC)**: organization's ability to remain functional during a disaster or an incident.
- Two events impact BC:
  - **Disaster**: an environmental, accidental, or intentional catastrophic event
  - **Incident**: an accidental or intentional security-related event

- BC relies on two abilities:
  - **Disaster recovery (DR)**: organization's ability to return to normal operations after a disaster
  - **Incident response (IR)**: organization's ability to recognize and respond to an incident

- Three plans enable an organization to respond to a disaster or an incident:
  - I**ncident response plan (IRP)**: set of processes an organization follows to recognize, respond, and recover from an incident
  - B**usiness continuity plan (BCP)**: set of processes an organization follows to maintain BC during a disaster or incident
  - D**isaster recovery plan (DRP):** set of processes an organization follows to return to normal operations post-disaster

Example: A hospital is hit with a ransomware attack that encrypts patient records and locks staff out of critical systems

1. **Incident Response Plan (IRP**)[Stop the attack and contain damage]
   - Cybersecurity team identifies the attack and isolates infected systems
   - They notify law enforcement and begin forensic analysis
   - Internal communication plans are used to keep staff updated
   - They restore partial access to critical functions using backups

2. **Business Continuity Plan (BCP) is activated**[Keep hospital running during the crisis]
   - Hospital shifts operations to manual recordkeeping
   - Alternate facilities are used for emergency procedures
   - Critical systems like life-support and diagnostics are prioritized for restoration

3. **Disaster Recovery Plan (DRP) follows** [Restore systems and return to normal operations]
   - Once the threat is neutralized, IT begins full system restoration from clean backups
   - Patient data is recovered and verified
   - Hospital conducts a post incident analysis to improve future resilience

Defense in Depth: Definition

- Defense in Depth is a cybersecurity strategy that uses multiple layers of defense across the technology stack to protect systems and data — so if one layer fails, others still provide protection
- Aim is to increase the time and effort required for an attacker to breach defenses, reducing the likelihood of a successful attack

Think of it like protecting a castle:

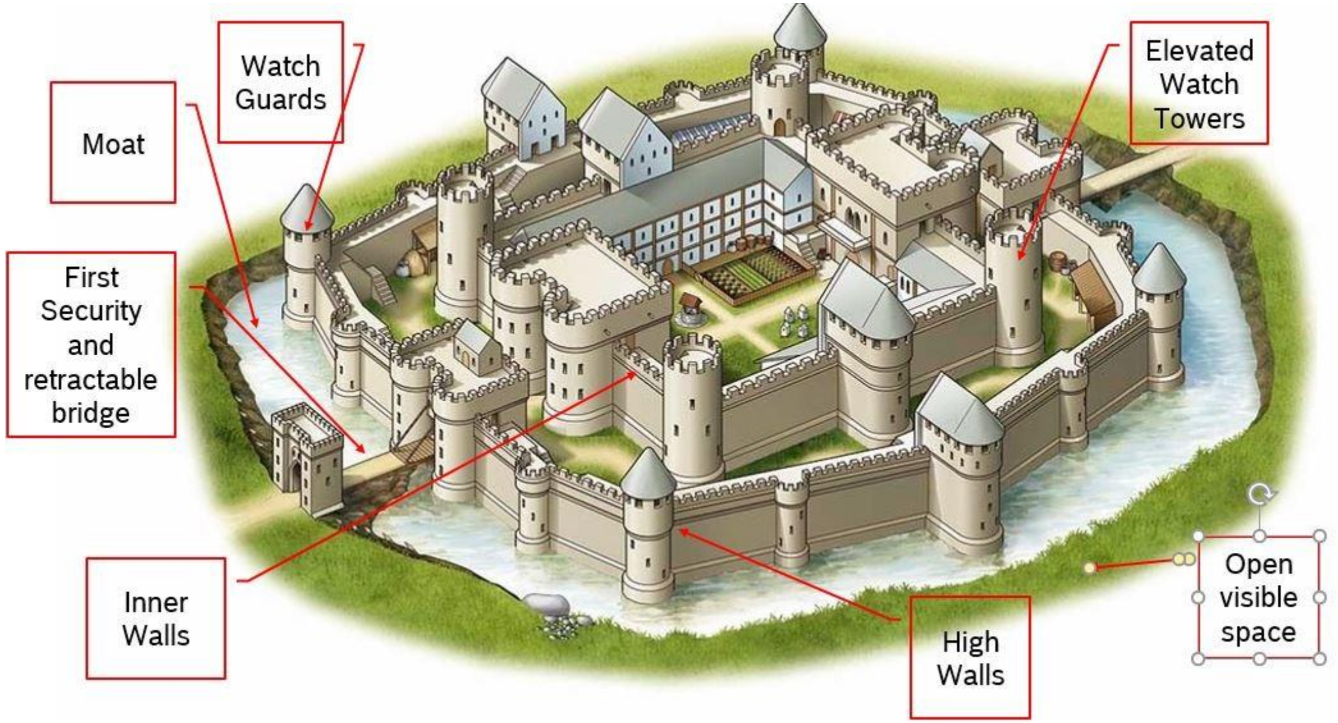
What would you do to protect a castle?

Defense in Depth: Definition

- Each layer works together to delay or stop attackers, just like layered castle defenses

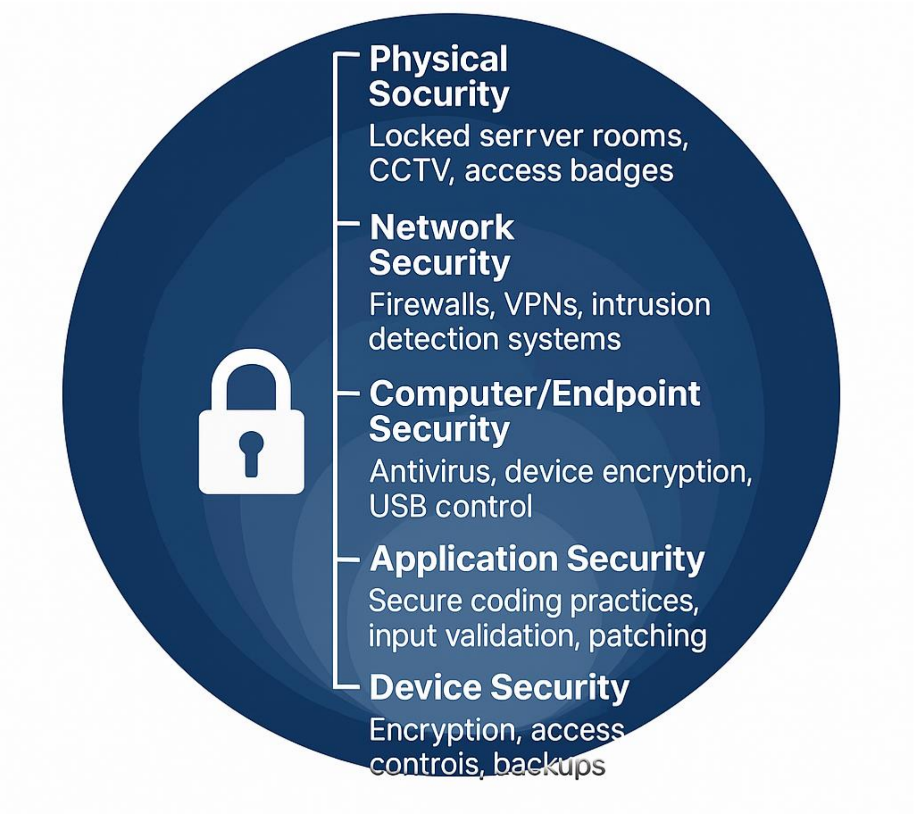
Think of it like protecting a castle:

- Moat = Firewalls
- Walls = Network segmentation
- Guards = Authentication
- Locked doors = Encryption
- Alarms = IDS/monitoring
- Escape plans = Backups & recovery



6 Common Layers of Defense in Depth

1. **Physical Security-** Locked server rooms, CCTV, access badges
2. **Network Security**- Firewalls, VPNs, intrusion detection systems
3. **Computer/Endpoint Security**- Antivirus, device encryption, USB control
4. **Application Security**- Secure coding practices, input validation, patching
5. **User Security**- Training, strong passwords, MFA
6. **Device Security-** Encryption, access controls, backups


Physical Socurity
Locked serrver rooms, CCTV, access badges
Network Security
Firewalls, VPNs, intrusion detection systems
Computer/Endpoint Security
Antivirus, device encryption, USB control
Application Security
Secure coding practices, input validation, patching
Device Security
Encryption, access controis, backups

Security Architecture

Defense in Depth isn’t just a standalone concept- it is woven into the Security Architecture

The Four Pillars of Security Architecture in Defense in Depth

1. **People-** Employees who are aware of cybersecurity threats and trained in safe practices
2. **Process-** Established protocols and procedures to manage security
3. **Technology-** Security tools and software that prevent, detect, and respond to attacks
4. **Partners-** Collaborating with external security firms or vendors to enhance security measures.

How Does Defense in Depth Fit In?

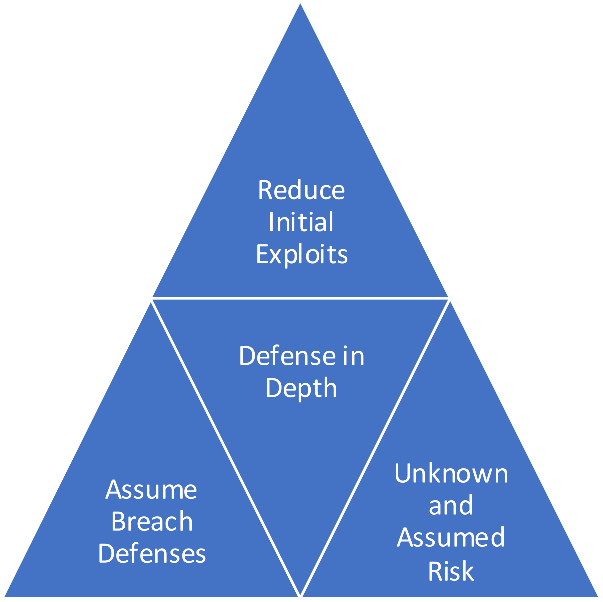
1. **Reduce Initial Exploits:** Defense in Depth aims to minimize the chances of successful attacks by reducing opportunities for initial exploitation.
   - Includes proactive measures like secure coding practices, vulnerability scanning, and regular security assessments

2. Assume Breach Defenses: Defense in Depth operates on the assumption that, at some point, a breach will occur

- By preparing for this scenario, organizations can implement controls that limit the damage if an attacker gains access

3. Unknown and Assumed Risk: Not all risks are known, and some may be unavoidable

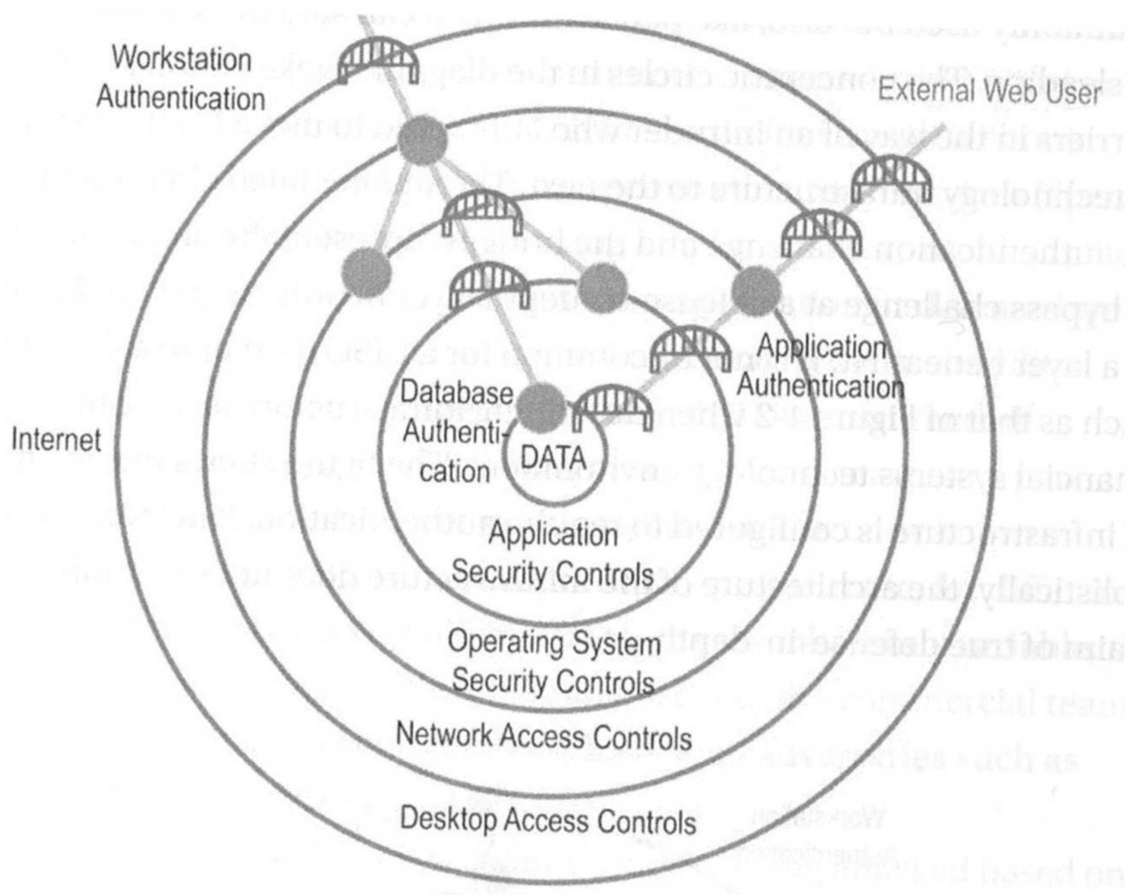
- Defense in Depth takes this into account by having multiple controls in place, each addressing different types of risks



By addressing each of these aspects, Defense in Depth makes it much harder for attackers to achieve their objectives, even if they overcome one layer of security

Understanding Access Paths in Defense in Depth

- Access Paths represent the different layers of authentication and security controls that a user or system must pass through to access sensitive data
- Each layer adds another level of defense, ensuring that only authorized users can reach critical resources.

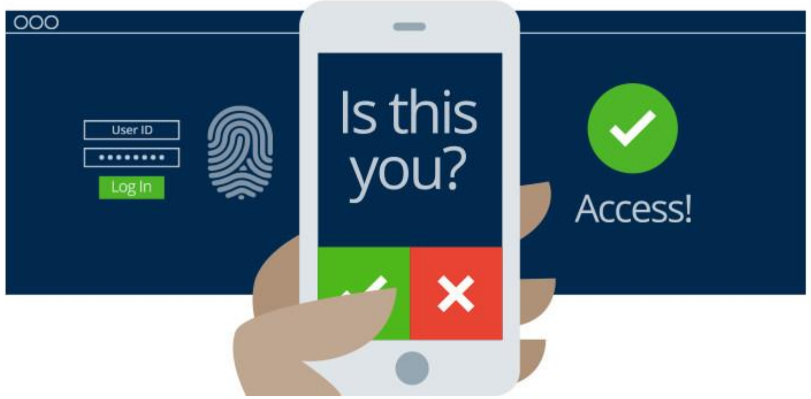


Workstation Authentication
External Web User
Application Authentication
Database Authentication
DATA
Internet
Application Security Controls
Operating System Security Controls
Network Access Controls
Desktop Access Controls

Defense in Depth: Authentication

- Authentication is a critical aspect of Defense in Depth, ensuring that only verified users can access systems and data. It typically involves multiple factors to verify identity, which strengthens security by requiring users to prove who they are in different ways

- Types of Authentication Factors
  - Something you know
    - password
  - Something you have
    - token (Yubikey)
  - Something you are
    - biometric (finger)



Summary

- Understand the purpose and importance of security policies
- Identify common types of cybersecurity policies (e.g., acceptable use, password, incident response)
- Recognize how standard frameworks (e.g., NIST, ISO) influence policy development
- Learn how policies are implemented and enforced in organizations
- Understand Defense in Depth