Information Security (IS) Fundamentals

CYBER SECURITY AND ETHICAL HACKING

What is Information Security

Information security (InfoSec) covers the tools and processes that organizations use to protect information.

Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction.
The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

3 Principles of Information Security

Confidentiality

Integrity

Availability

Confidentiality

The principle of confidentiality ensures that only the people who have permission or authority to view content can do so.
Measures are designed to protect against unauthorized disclosure of information.

Those controls can include:

- Identification
- Authentication
- Authorization
- Encryption

Integrity

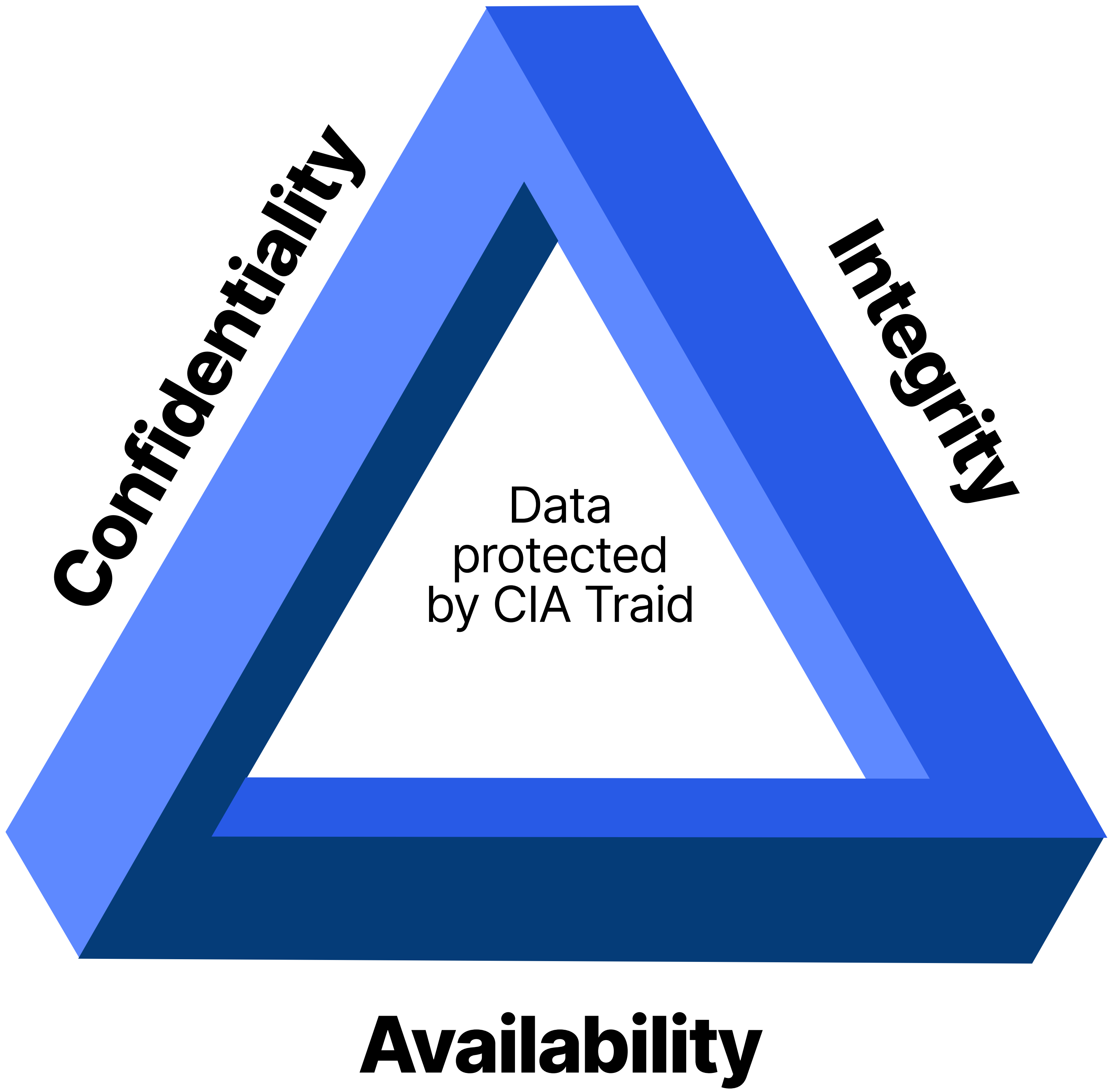
Integrity involves protection from unauthorized modifications (e.g., add, delete, or change) of data.

The principle of integrity is designed to ensure that data can be trusted to be accurate and that it has not been inappropriately modified.

Availability

Availability is protecting the functionality of support systems and ensuring data is fully available at the point in time (or period requirements) when it is needed by its users.

The objective of availability is to ensure that data is available to be used when it is needed to make decisions.



The CIA Triad defines three key principles of data security

Information security controls

Authentication

The process of authentication is when the system identifies someone with one or more than one factors. For example, ID and password combinations, face recognition, thumb impression etc. These factors can not always be trusted as one could lose them or it might be accessed by any outsider. For these circumstances, one can use multi factor authorisation which is done by combining any two or more of the above factors.

Access Control

It refers to limiting access to data or information.
One could find two type of lists :

- Access Control List (ACL) - This is just the list of individuals who are eligible to access the information
- Role- Based access Control List (RBAC) - This list comprises of the names of authorized personnel and their respective actions they are authorized to perform over the information.

Encryption

Encrypting your content lets you control its confidentiality and integrity. Encryption turns a plain text piece of content into a cipher. A hacker who gets access to a plain text document, such as a sales contract, spreadsheet, or email, can read it easily. But someone who gets access to a cipher won't make heads or tails of it, unless they also happen to have the decryption key.

Information Security Standards

- ISO
- IT Act
- Copyright Act
- Patent Law
- IPR

ISO

International Organization for Standardization. Established On 23 February 1947

ISO 27001

This standard allows us to prove the clients and stakeholders of any organization to managing the best security of their confidential data and information.

ISO 27000

This standard provides an explanation of terminologies used in ISO 27001.

ISO 27002

It includes the selection, implementation, operating and management of controls taking into consideration the organization's information security risk environment(s).

ISO 27005

This standard supports the general concepts specified in 27001. It is designed to provide the guidelines for implementation of information security based on a risk management approach.

ISO 27032

It is the international Standard which focuses explicitly on cybersecurity. This Standard includes guidelines for protecting the information beyond the borders of an organization such as in collaborations, partnerships or other information sharing arrangements with clients and suppliers.

IT Act

The Information Technology Act also known as ITA-2000, or the IT Act main aims is to provide the legal infrastructure in India which deal with cybercrime and e-commerce.

The IT Act is based on the United Nations Model Law on E-Commerce 1996 recommended by the General Assembly of United Nations. This act is also used to check misuse of cyber network and computer in India. It was officially passed in 2000 and amended in 2008.

It has been designed to give the boost to Electronic commerce, e-transactions and related activities associated with commerce and trade. It also facilitate electronic governance by means of reliable electronic records.

Copyright Act

The Copyright Act 1957 amended by the Copyright Amendment Act 2012 governs the subject of copyright law in India. This Act is applicable from 21 January 1958. Copyright is a legal term which describes the ownership of control of the rights to the authors of "original works of authorship" that are fixed in a tangible form of expression.

An original work of authorship is a distribution of certain works of creative expression including books, video, movies, music, and computer programs. The copyright law has been enacted to balance the use and reuse of creative works against the desire of the creators of art, literature, music and monetize their work by controlling who can make and sell copies of the work.

Patent Law

Patent law is a law that deals with new inventions. Traditional patent law protect tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers.

As time increases patent law have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms.

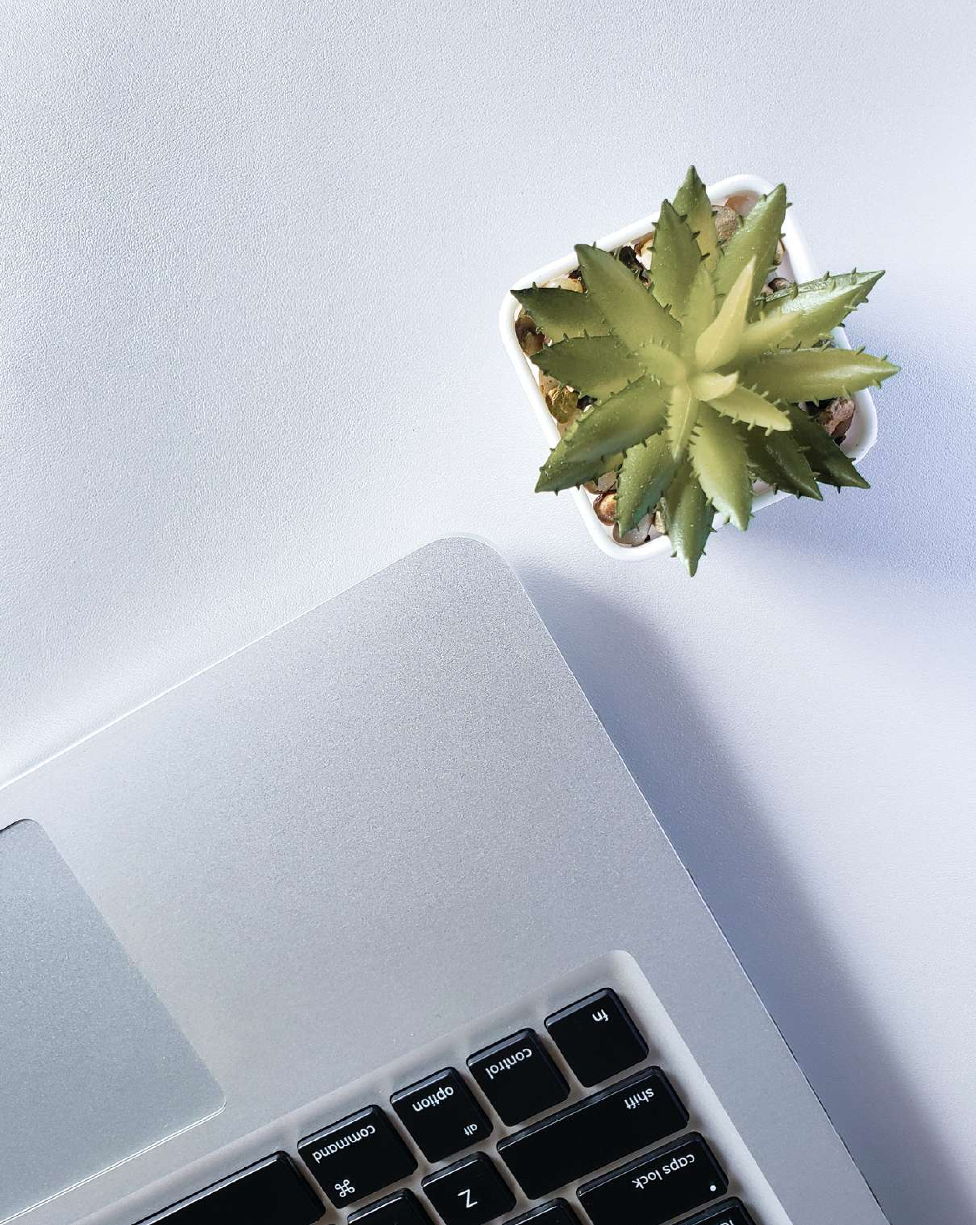
It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

IPR - Intellectual property rights

A right that allow creators, or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas, or other intangible assets or investment in a creation. These IPR rights are outlined in the Article 27 of the Universal Declaration of Human Rights.

It provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions. These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

Information Valuation and Asset Classification

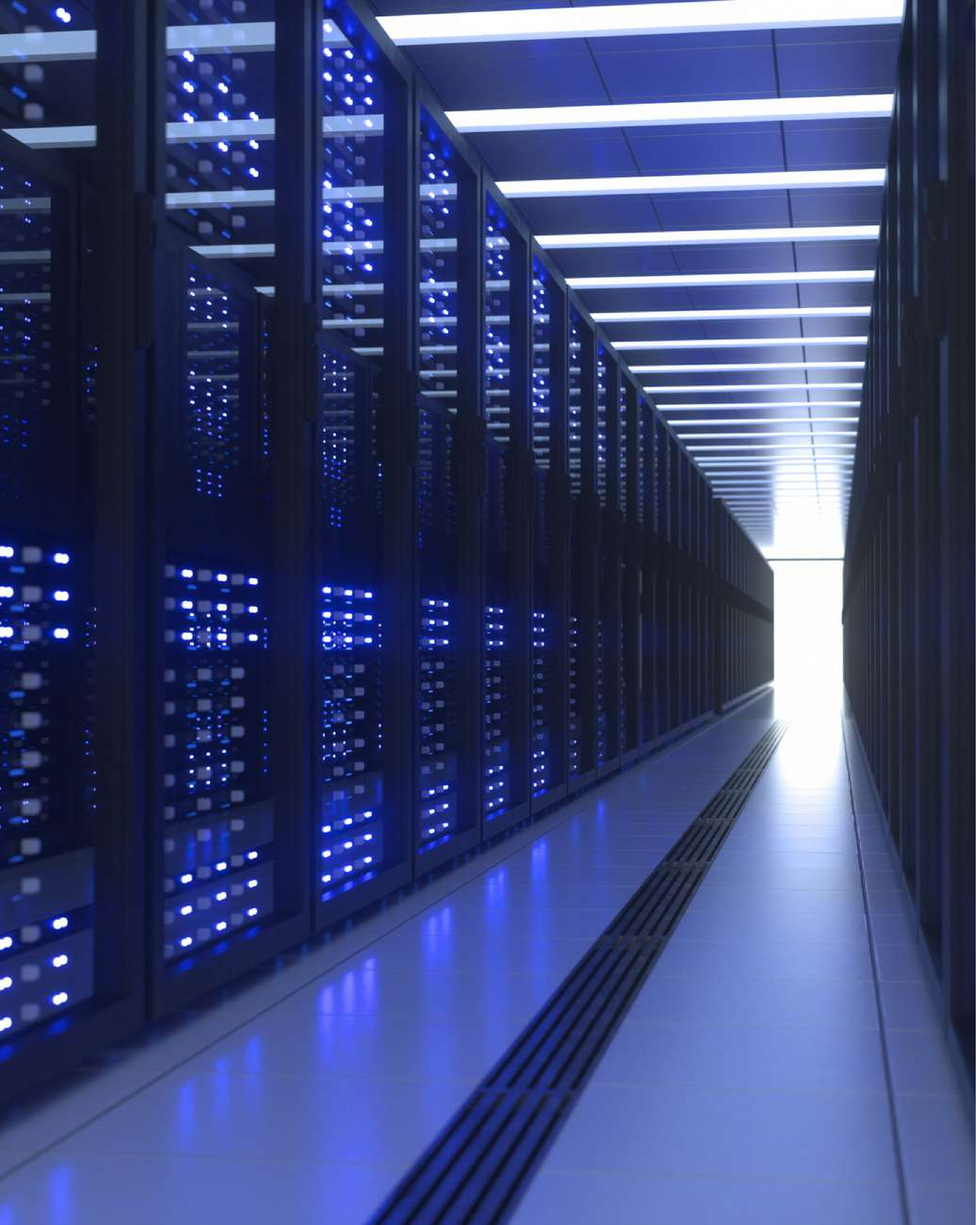


What Is Information Classification?

Data Classification or Information Classification is the process of classifying corporate information into significant categories to ensure critical data is protected.

For example, financial files within an organization should not be kept together with files from the public relations department. Instead, they should be maintained in separate folders, which are accessible only by individuals who are entitled to working with each kind of data.

Thus, the stored information stays safe and can be easily accessed when needed.



Asset Classification

All the Company's information, data and communication must be classified strictly according to its level of confidentiality, sensitivity, value and criticality.

Information may be classified as HIGHLY RESTRICTED, CONFIDENTIAL, INTERNAL USE ONLY, and PUBLIC.

HIGHLY RESTRICTED

This classification label applies to the most private or otherwise sensitive information of the Company. Information under this classification shall be strictly monitored and controlled at all times. (e.g. merger and acquisition documents, corporate level strategic plans, litigation strategy memos, reports on breakthrough new product research, and Trade Secrets such as certain computer programs.)

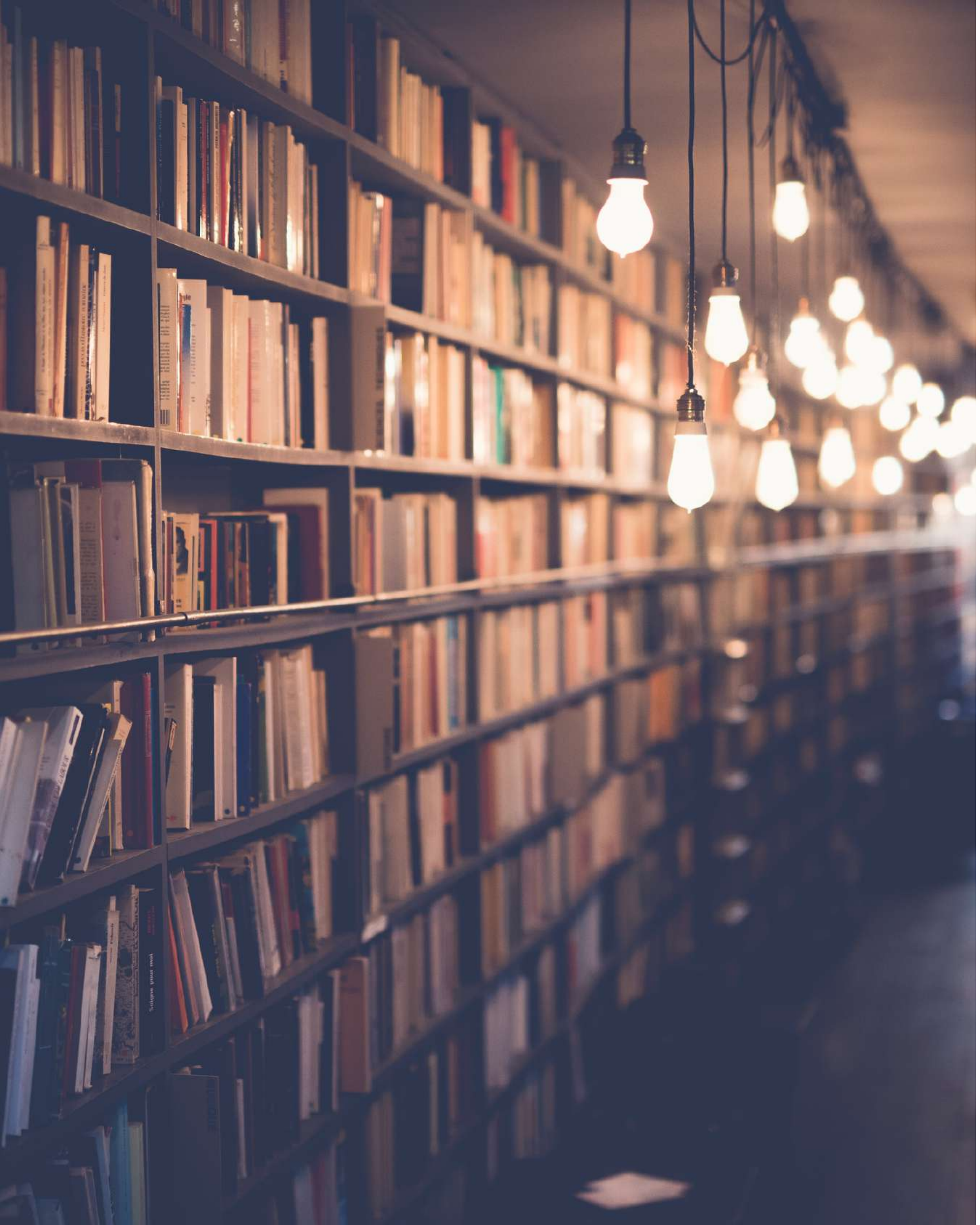
CONFIDENTIAL

This classification label applies to Company information, which is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access.

(e.g. employee performance evaluations, customer transaction data, strategic alliance agreements, unpublished internally generated market research, computer passwords, identity token personal identification numbers (PINs), and internal audit reports).

INTERNAL USE ONLY

This classification label applies to information intended for use within the Company, and in some cases within affiliated organizations, such as business partners of the Company. Assets of this type are widely-distributed within the Company and may be distributed within Company without permission from the information asset owner. (e.g. telephone directory, dial-up computer access numbers, new employee training materials, and internal policy manuals.)



PUBLIC

This classification applies to information that has been explicitly approved by the Company's management for release to the public. Assets of this type may be circulated without potential harm. (e.g. product and service brochures, advertisements, job opening announcements, and press releases.)

Physical security definition

Physical security is the protection of people, property, and physical assets from actions and events that could cause damage or loss.

This contains security from fire, natural disasters, robbery, theft, destruction, and terrorism.

Best practices for converged security

- Install access control and surveillance for any space
- Ensure that both internal teams and security system providers adhere to best practices for cybersecurity, including using multi-factor authentication (MFA
- Restructure security teams so that physical security and IT leaders work together
- Establish formal collaboration to give teams a better way to share information
- Leverage data compiled from integrated systems for a more complete picture of security posturing across the entire organization.

Hardware Asset Management

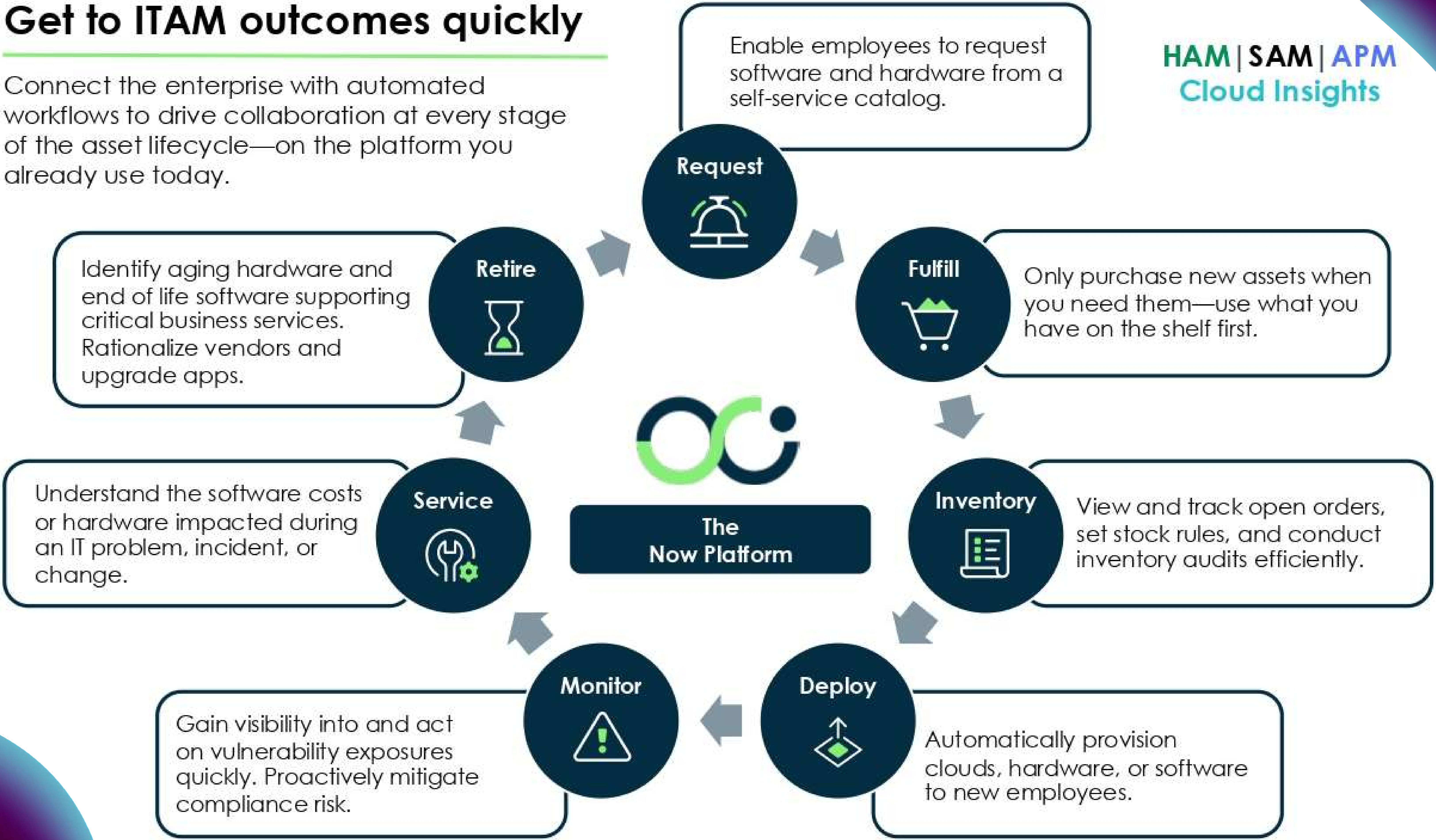
Hardware asset management (HAM) describes the processes, tools, and strategies of managing the physical components of computers and related systems.
Some examples of hardware assets

- **End-user devices:** personal computers, laptops, tablets, smartphones, and SIM cards
- **Network and telecom equipment:** routers, switches, load balancers, and video- conferencing and voice over Internet protocol (VoIP) systems
- **Data center hardware:** servers, storage and backup systems, utilities, and security equipment
- **Significant peripherals:** personal printers, monitors, scanners, and multifunction printing systems

Get to ITAM outcomes quickly

Connect the enterprise with automated workflows to drive collaboration at every stage of the asset lifecycle—on the platform you already use today.

HAM | SAM | APM
Cloud Insights



Request
Enable employees to request software and hardware from a self-service catalog.

Fulfill
Only purchase new assets when you need them—use what you have on the shelf first.

Inventory
View and track open orders, set stock rules, and conduct inventory audits efficiently.

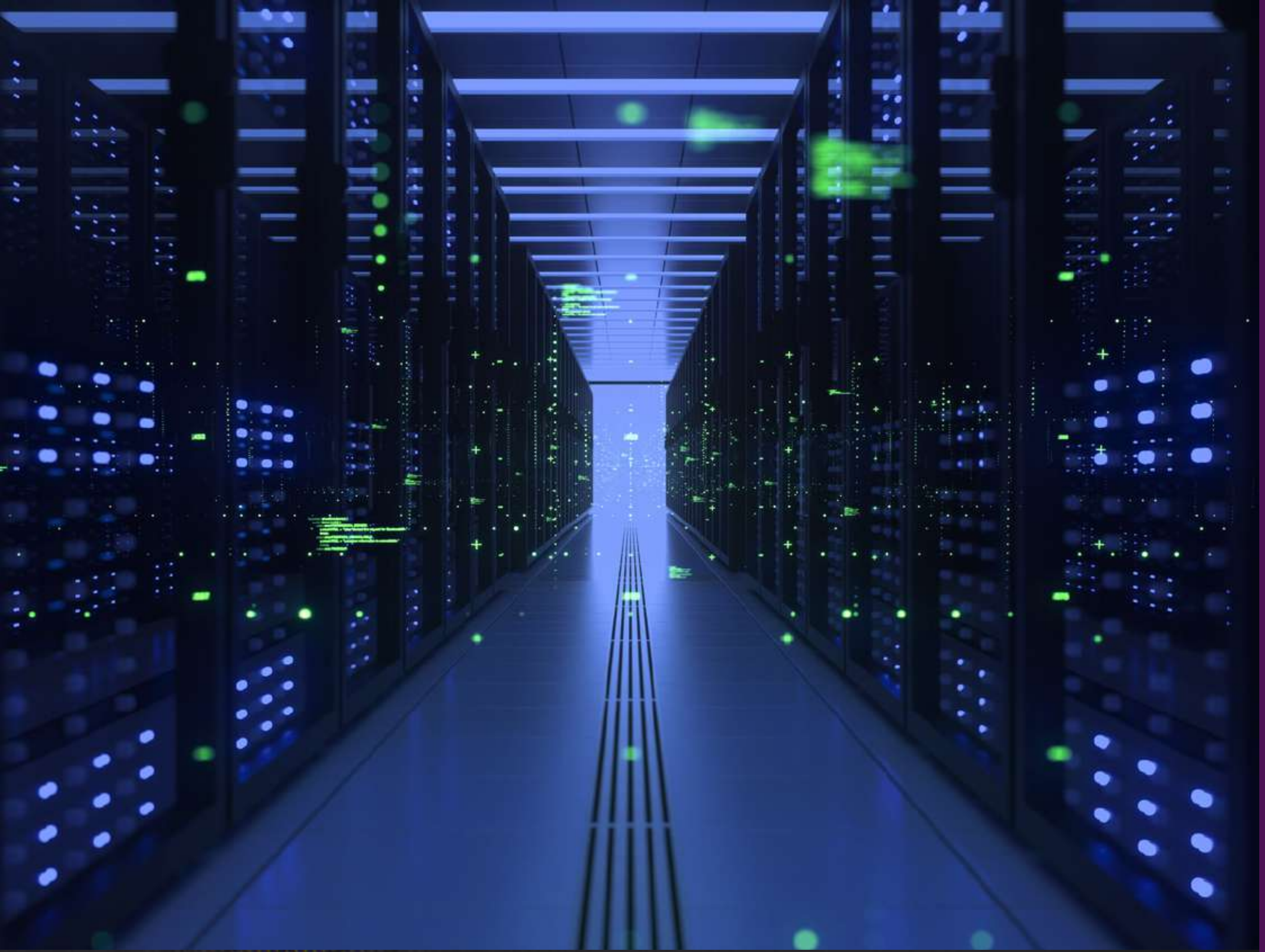
Deploy
Automatically provision clouds, hardware, or software to new employees.

Monitor
Gain visibility into and act on vulnerability exposures quickly. Proactively mitigate compliance risk.

Service
Understand the software costs or hardware impacted during an IT problem, incident, or change.

Retire
Identify aging hardware and end of life software supporting critical business services. Rationalize vendors and upgrade apps.

The Now Platform



Basic Security Requirement

Antivirus Software - Install antivirus software and set to automatic updates.

Application Patches - Install critical application patches. When available, enable automatic update functionality.

Clear text Authentication - Encrypt passwords when authenticating.

Institutional Accounts - Only employees or affiliates may have institutional accounts

Logging - Log to the central logging servers

Network Services - Secure network services on your computer

Passwords - Use strong passwords for authentication.

Operating System Patches - When available, enable automatic update functionality.

Training - Complete Training Requirements appropriate for your position

Information Security (IS) Fundamentals

CYBER SECURITY AND ETHICAL HACKING