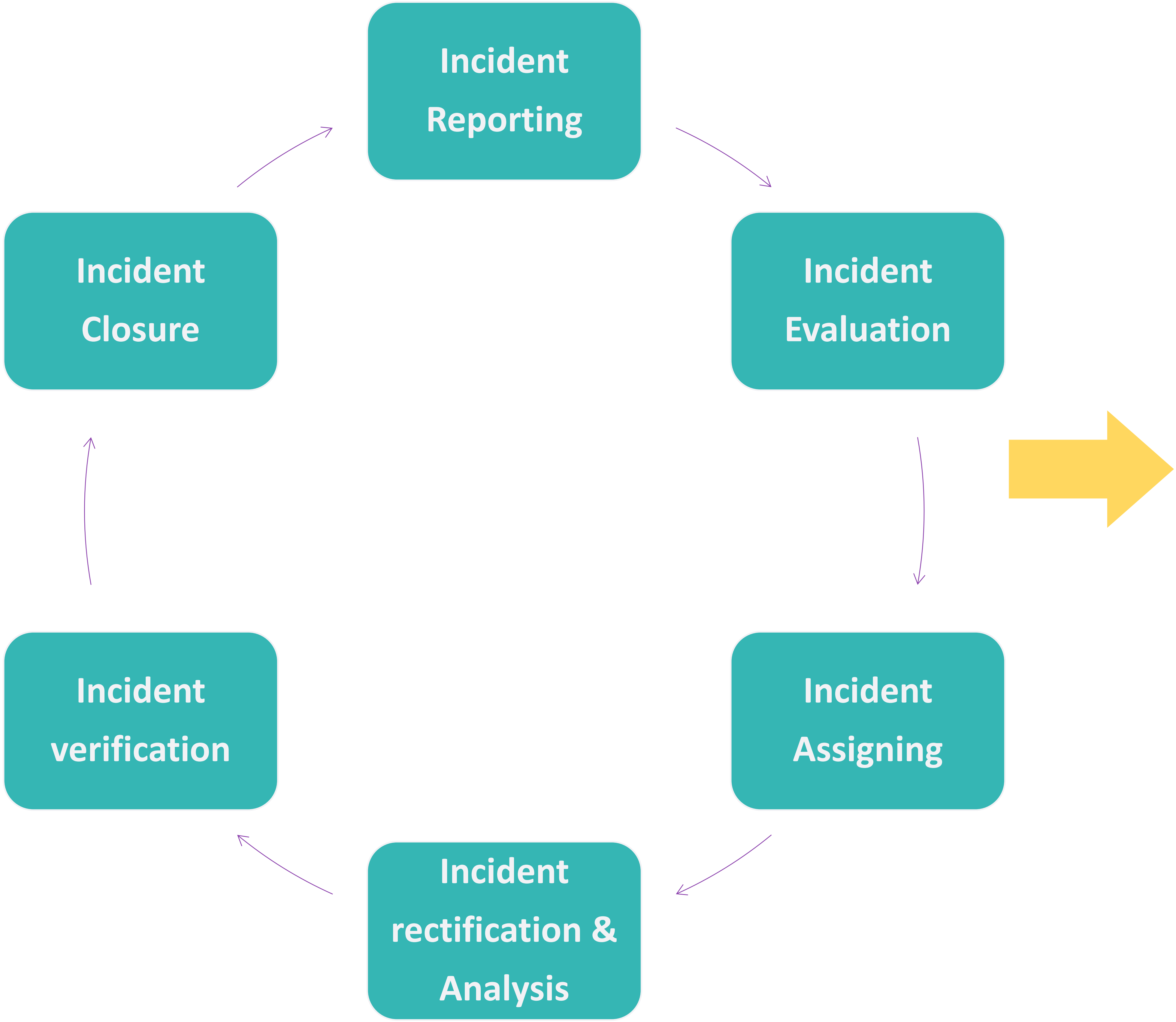
ISMS EXCERPTS – INCIDENT MANAGEMENT

aspire SYSTEMS

attention.
always.

INCIDENT MANAGEMENT



Information security incident is any violation or imminent threat of violation of our computer security policies, resource usage policies or standard security practices.

- ✓ Help in creating a secure environment.
- ✓ Report internal incidents immediately in Incident Management Systems (IMS) available in Intranet portal.
- ✓ Customers can report an incident by sending us an email to incidents@aspiresys.com
- ✓ Report the incident to appropriate function teams over phone by calling +91-44-67404000
- ✓ If there is a need to inform about an incident to customer, then the respective department who owns the incident will inform to the customer SPOC.

INCIDENT MANAGEMENT

What is an Incident?

A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Note: Refer Incident Management Procedure for more details

Examples of information security incidents are:

- Loss of service, equipment or facilities, Theft of organizational assets
- Software/Hardware malfunctions or overloads, Server unavailability
- Hacking, Virus attack, Network down, Malware attack, Ransomware attack
- Non-compliances with policies or guidelines
- Breaches of physical security arrangements
- Leaving system (desktops and laptops) unlocked and unattended
- Work bays left open without access control
- Access violations/Unauthorized entry/Entry without ID card/Tailgating
- Indiscipline/unprofessional work Ethics, Violation of code of conduct, Sharing passwords

INCIDENT CLASSIFICATION

Department	Incident Categories
Facilities	• Unauthorized Entry/Access • Accident (Fire/Vehicle, etc) • Equipment theft/Data Loss • Physical Security • Data Breach
Network & System Admin	• Server unavailability • Hack/Virus/Malware attack • Unauthorized Disclosure of data • Network/System/Email/MS Teams • Equipment theft/Data Loss • Data Breach

INCIDENT CLASSIFICATION

Department	Incident Categories
Human Resource	• Absconding Employee • Employee disciplinary related • Data Breach
Information Systems	• Unauthorized Entry/Access • Unauthorized Disclosure of data • Data Breach
Delivery	• Unauthorized Entry/Access • Unauthorized Disclosure of data • Equipment theft/Data Loss Network/System/Email/MS Teams/Virus/Malware attack • Legal and Regulatory • Data Breach

INCIDENT PRIORITIZATION

How to prioritize an incident?

Rating	Description
P1 – Critical	• Impacts the entire organization (people and systems) from performing critical business operations. • Has a large financial risk ,legal liability and immediate threat to human • safety.. • Loss of confidentiality, integrity and availability of assets.
P2 - Important	• Impacts a service line or major portion of a service line and cause of incident falls across multiple functions. • Has financial risk and legal liability. • Loss of confidentiality, integrity and availability of assets in the affected service line

INCIDENT PRIORITIZATION

Rating	Description
P3 – Normal	• Multiple projects or personnel within a service line are impacted. • Has minimum or no financial risk and legal liability. • Loss of confidentiality, integrity and availability of assets of affected projects or personnel.
P4 - Low	• Impacts one or two personnel or a single project. • Has no financial risk and legal liability. • Minimum loss in confidentiality, integrity and availability of assets of • affected project or personnel.

INCIDENT RESOLUTION

Incident Resolution

The time duration for responding to and resolving an incident depends on the priority of the incident. Below is the table indicating time duration for each incident priority:

Priority	Duration to Resolve
P1 – Critical	1 hour
P2 - Important	4 hours
P3 – Normal	1 day
P4 - Low	7 days

A incident is considered to be resolved only when the root cause is identified and when the resolution details are provided with the corrective action.

THANK YOU :)