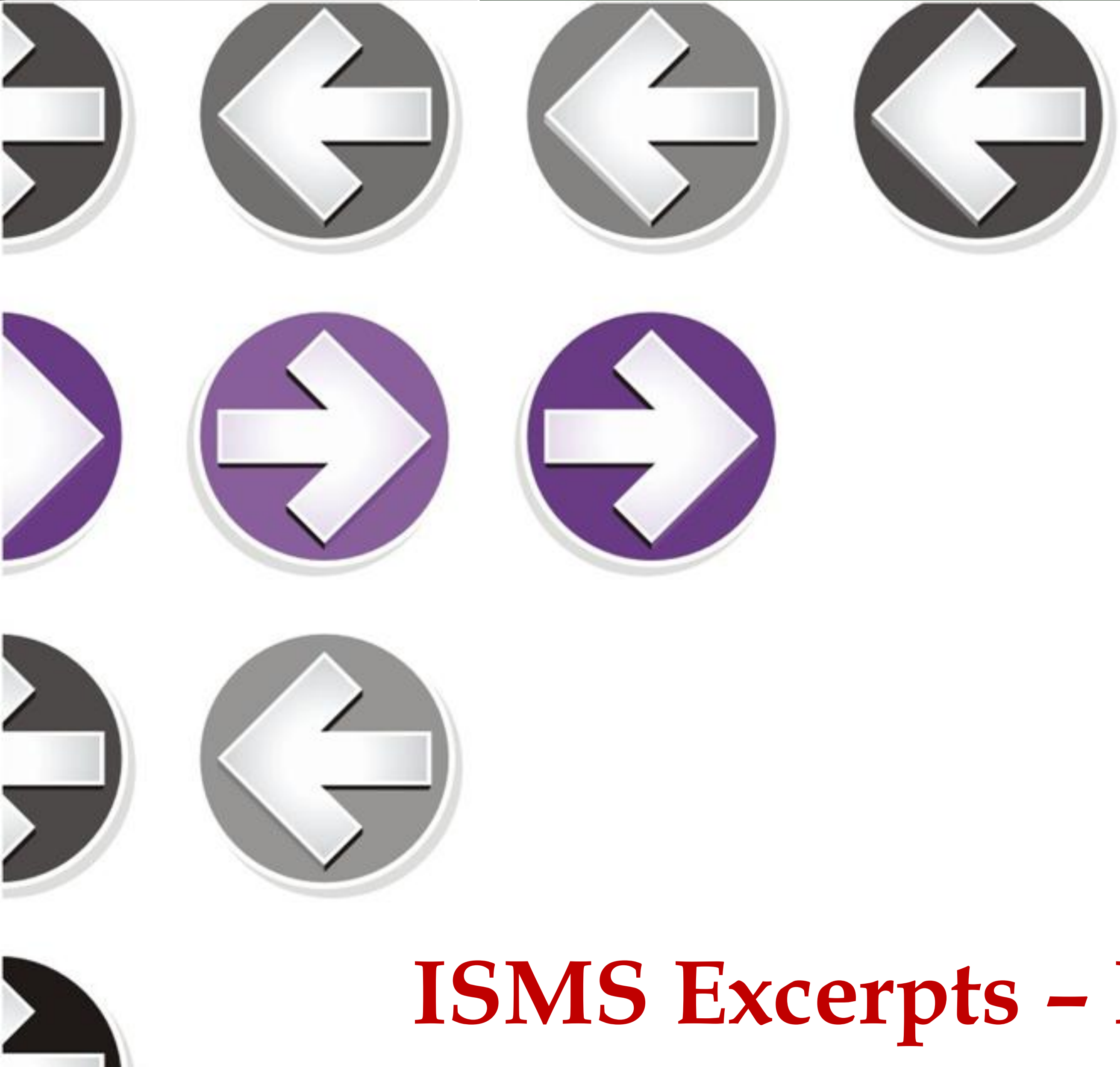
aspire SYSTEMS
attention. always.



aegis

ISMS Excerpts – Incident Management Procedure

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.

Examples of information security incidents are:

- Loss of service, equipment or facilities
- System malfunctions or overloads
- Human errors
- Non-compliances with policies or guidelines
- Breaches of physical security arrangements
- Uncontrolled system changes
- Malfunctions of software or hardware
- Access violations

"Information Security is Everyone's Responsibility"

INCIDENT MANAGEMENT

Incident Classification

Incidents are classified based on the department under which the incident falls as explained in the subsequent slide

“Information Security is Everyone’s Responsibility”

INCIDENT CLASSIFICATION

aspire SYSTEMS
attention. always.

Department	Incident Categories
Facilities	▪ Unauthorized Entry ▪ Entry without ID card ▪ Equipment Failure ▪ Theft of organizational assets ▪ Others
Network & System Admin	▪ Server unavailability ▪ Hacking ▪ Virus Attack ▪ Link down ▪ Unauthorized access ▪ Network devices down ▪ Others
Human Resource	▪ Absconding Employee ▪ Engaging in business with client without consent from Aspire ▪ Indiscipline/Unprofessional work ethics ▪ Others
Information Systems	▪ Unauthorized/Undesired Access ▪ Data Access/Manipulation ▪ Others

"Information Security is Everyone's Responsibility"

INCIDENT PRIORITIZATION

How to prioritize an incident?

Rating	Description
Immediate	▪ 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.
High	▪ 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.
Medium	▪ 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.
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.

"Information Security is Everyone's Responsibility"

INCIDENT REPORTING

Incident can be Reported through

- Helpdesk System
- Phone

- Helpdesk System
  - You can raise a ticket in the Helpdesk system. Login to the helpdesk system through http://systems.aspiresys.com
  - “Create tickets by choosing “Incident” category against the appropriate department”

- Phone
  - Report the incident to appropriate function teams over phone. In such cases, the employee can call any of the following numbers:
    - **+91-44-67404000**
    - **+91-44-47456000**

“Information Security is Everyone’s Responsibility”

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
Immediate	1 hour
High	4 hours
Medium	1 day
Low	7 days

"Information Security is Everyone's Responsibility"

aspire SYSTEMS

attention. always.