# Incident management USUP

Coordinating responses to incident reports, minimising negative impacts and restoring service as quickly as possible.

|  |
| --- |
| **Guidance Notes:**  Activities may include, but are not limited to:   * designing and implementing different processes and procedures for different categories of incidents including, but not limited to, major incidents, information or cybersecurity incidents, complex incidents, low impact incidents * establishing incident response teams or security incident response teams * routing requests for help to appropriate functions for resolution * monitoring resolution activity * informing users, customers and key stakeholders of progress towards service restoration.   Incidents can impact many areas, such as but not limited to, business operations, information security, IT systems, services, employees, customers, or other vital business functions.  Different roles/groups may be needed to diagnose and resolve incidents, such as, users, subject matter experts, service desk, support teams, suppliers, partners. Although they play a part in the incident management process, they do not necessarily need incident management skills. |

## Level 1

Follows agreed procedures to identify, register and categorise incidents.   
Gathers information to enable incident resolution and allocates incidents as appropriate.

## Level 2

Provides first line investigation and gathers information to enable incident resolution and allocate incidents.   
Advises relevant people of actions taken.

## Level 3

Prioritises and diagnoses incidents. Investigates causes of incidents and seeks resolution.   
Escalates unresolved incidents.   
Facilitates recovery, following resolution of incidents. Documents, communicates outcomes and closes resolved incidents.

## Level 4

Monitors incident queues. Ensures that incidents are handled according to agreed procedures.   
Contributes to developing, testing, and improving incident management procedures.   
Ensures that resolved incidents are properly documented and closed.   
Supports team members in the correct use of the incident process.

## Level 5

Responsible for the operation of the incident management process.   
Leads incident communications, ensuring al parties are aware of incidents and their role in the process.   
Leads the review of major incidents and informs service owners of outcomes. Ensures incident resolution within service targets. Analyses metrics and reports on the performance of the incident management process.   
Develops, maintains and tests incident management policy and procedures.