1.0 Purpose of Incident Management

The Incident Management process will ensure effective handling and resolving of Incidents.

2.0 Definition

Incident = an unplanned interruption to a service, a reduction in the quality of a service, or an event that has not yet impacted the service to the customer. Note that degradation of service is also regarded as an incident.

Or=Any unplanned event that results in injury or ill-health to people, or damage or loss to property, plant, materials or the environment.

Or =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

3.0 Scope

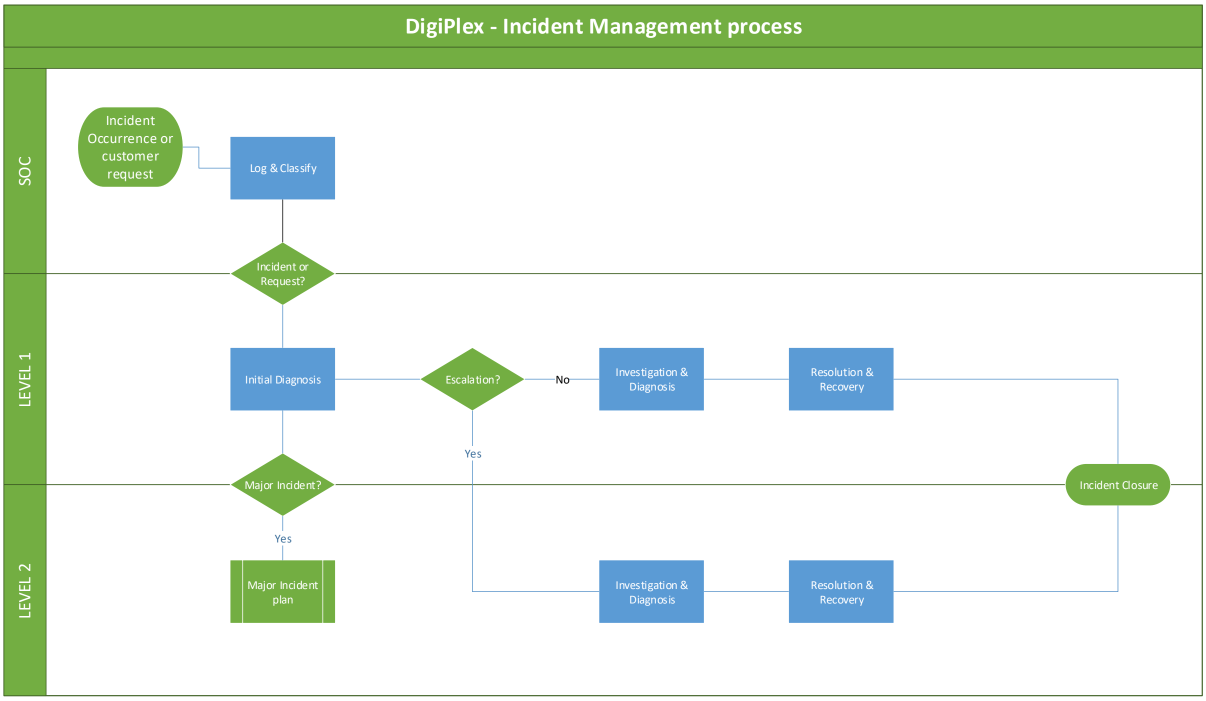
Incidents involves incidents directly on the Service Environment or DigiPlex internal service infrastructure.

4.0 Role descriptions

Role	Responsibilities	Comments
Incident Reporter	The Person or Company that reports the incident	Should be kept informed regularly during the lifecycle of the Incident

SOC	The defined single source of contact for receiving and dispatching all incidents	
Analysts	Resources involved in the diagnosing, investigation and resolving of incidents	May be a person belonging to any one of our teams in DigiPlex
Incident Manager	The role responsible for the Incident process is followed, the backlog is kept under control and that all incidents is taken care of	

5.0 Process Overview



5.1 How to submit an Incident:

Incidents are reported by any stakeholder. All incidents must be registered in ServiceNow, either directly in ServiceNow, sending an email to helpdesk@digiplex.com or using the self-service portal on https://digiplex.service-now.com/sp

5.2 Log and Classify

Logging

Effective Incident resolution requires as precise information as possible. When in dialogue with the customer or the one who reports the incidents, try to include a short description that clearly states the symptoms, what you've tried to do to fix the incident and how it affects the customer. Ensure a common understanding with you and the customer what the situation is, and how urgent it is.
Also, ensure that you have the right contact details for further communication, see that you have the **Company** Field and **Caller** Field correctly filled in.

Classification

Correctly classifying an Incident helps out with sorting, filtering and searching for Incidents. In addition, it allows for reporting and trend-analysis. It is therefore important that you classify the incident as precise as you can by using the following fields:

- **Business Service** (Setting the Business service will dictate the timeframe (SLA) of an incident and how fast to respond on it)
- **Urgency** is a measure of how long it will be until an Incident has a significant impact on the business. Urgency also dictates the Priority of the Incident)
- **Impact** is a measure of the effect of an Incident on business service.
- **Priority** is a category used to identify the importance of an Incident. Priority is based on Impact and Urgency and is used to identify the required time for actions to be taken.

See the matrix below.

- **Category** & **Type** (Used for trend-analysis. When selecting a Category, the values in the Type field will vary depending on which category you selected. Note: when it is an incident, ensure that you use a category other than Inquiry/Help.)
- **Note:** *When it is a **Health & Safety** issue, ensure that you use this category and choose between two different Types, Accident or Near-accident. An automatic notification is forwarded to HR.*

  For **Security Information** make sure you also use the correct Business service. *This category is to be used when you have 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.*

- **Site** and **Location** (Site is either of the DigiPlex sites, and Location is used to e.g. specify which module where the Incident resides)
- **Affected CI** (A CI is the faulty component/equipment)

To help prioritizing the incident correctly, ask yourself questions like:

- Is the incident about a critical Business Service?
- Is the service available and running on backup power?
- Is the service only partly available or running on redundant power?

- Is there a total outage situation for the specific service?
- Are there multiple customers affected?
- Does it have other impact to business?

Note that a situation with a high urgency and high impact, will require triggering the Major Incident Procedure.

Prioritizing an Incident

Impact Urgency	High 1	Medium 2	Low 3
High **1**	1	2	3
Medium **2**	2	3	4
Low **3**	3	4	5

Priority Code	Description	Target Resolution Time
1	**Critical** **(Major Incident)**	**1 hour**
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

Link to: Major Incident/Business Continuity Plan Incident Priority Level

Incident or Request?

Incidents demand other response-times and priorities than Requests. If it is «just» a Request, use the Category «Inquiry / Help» and follow the process for Request Handling.

Initial Diagnosis

In this stage it is important that you use everything you can to get the service up and running as soon as possible (and within agreed, priorities, timeframes according to time-frames specified earlier and SLA's).

This may include using standardized methods and mindsets for error-solving. First of all, ensure that you have understood the situation clearly from the Logging step. In the case of any uncertainties, double check with the customer or colleague who registered the Incident. This is to avoid jumping to conclusions or working based on assumptions.

Use whatever procedures, knowledge, routines and checklists that you have at hand. Ask a colleague for help. Ask yourself questions to clarify:

- When did this happen?

- Does anyone else have the same issue?
- What are the symptoms
- What can be out ruled for sure

Ensure short and precise logging of your findings and results along the way, using the **Work Notes** field.

5.3 Escalation

If you're not able to sort out the reason and probable solution for the incident in due time, escalate to the **right team** for further Investigation and Diagnosis. Note that if you have a timeline that dictates how fast we're supposed to act on an incident, allow the next team enough time to perform their Investigation and Diagnosis to avoid breaching the SLA.

Ensure that the team or person you escalate to has the:

- Right competence
- Right privileges
- Right access
- Right supplier contacts available
- Right other relevant assistance available

5.4 Investigation & Diagnosis

Investigation & Diagnosis involves the deeper analysis and searching for errors in situation that requires this. Use whatever tools you need to get to the cause of the incident and take corrective measures.

Note, at this stage it is normal to identify whether this situation requires a more thorough Problem Analysis through the Problem Management process. In this case, ensure that someone is still trying to get to a workaround for the immediate (and often temporary) solution for the customer, while others try to find the real underlying cause and the best solution through structured Problem Management. To raise a Problem ticket from the Incident, use the ribbon-menu in ServiceNow and select «Create Problem». This will send the newly created issue to the proper Problem Management Team.

5.5 Resolution & Recovery

At this stage you should have identified a temporary or permanent solution to get the service up and running. Log your findings and result in the Closure Notes section fields. Make it clear (Closure Code) if the solution was permanent or a workaround. Make a clear statement about what the solution was in the Closure Notes field. This field is visible for customers, so make sure that what you write here is clearly understandable.

Remember to include verification from customer that the service is back to acceptable levels of operation if possible.