**Incidents**

Any Process or Event that has made a Security breach in terms of Data or any other aspect in the Organization can be raised as an Incident. An Incident can also be raised on anything, if that has compromised on the productivity (ie., Internet Speed, Slowness of the Application tool,....)

Incidents are broadly classified as follows.

* Security Incidents
* Auto Incidents

**Security Incidents**

A Security Incident is an event that indicates that the Organization's Data or the Performance have been compromised.

**Auto Incidents**

Auto-Incidents are those Incidents that are automatically generated by the HRMS System.

**Roles and Users Involved in Incidents**



**Process Involved In Incidents**

The various process involved in Incidents are listed as follows

* Incident Creation
* Assigning the Incidents
* Addressing the Incidents
* Incident Closure

**Incident Creation**



The Incident can be created by performing the following steps

1. Select the **ISMS Tab**.
2. Click Incident Request in the left pane, the Incident Creation form is displayed.
3. Check if the Employee name and Id are populated. If not populated, it would be because of HRMS Connectivity Issue. So Create the Incident after some time.
4. Fill the mandatory fields.
* Incident Date
* Incident Location
* Criticality of the Incident

 **5.** The **Incident Category Field** - Based on the Incident Category, Incidents are auto assigned.
 **6.** Click **submit button** to create the incident.

An attachment option is provided in the incident creation form, so this can further support the incident description.

**Assigning the Incidents**

Assigning the Incidents can be done in two ways.

* Automatically Assigning at the time of Incident Creation.
* Assigning by those having IDRG role.

**Automatically Assigning at the time of Incident Creation**

 The Incidents are automatically assigned at the time of Incident Creation based on the **Incident Category Field.**

**Assigning by those having IDRG role** The Incidents created can be assigned to different Departments or People by those having **IDRG role**.

The Created Incidents can also be closed automatically by rejecting them by those having **IDRG role**.



The IDRG Head performs the following steps to assign the Incident.

1. Select the DSS role as **IDRG** and Click on the **OK** button.
2. The IDRG Head can assign the Incident to respective departments or people. If the IDRG Head rejects the Incident, the Incident is automatically closed.

**Addressing the Incidents**



The following steps are performed to address the Incidents.

1. Select the DSS role and click on **OK button.** The Assignee’s role and the DSS user role should be same.
2. After entering all the CAPA details. Click on the **Submit button** to submit the CAPA.
3. The CAPA details are displayed in the grid.
4. Once the Preventive Action is Completed, the **Preventive Action Has Been Completed Checkbox** is selected and the **Submit button** is clicked.

**Incident Closure**

The Incidents can be Closed only by the IDRG head after receiving an email confirmation from the person created the incident.

It can be closed either by rejecting the Incidents at the time of creation or by accepting the CAPA given by the Incident Assignee’s.



* If the Incident is **Accepted**, the Assignee’s CAPA had been accepted and the Incident closes.
* If the Incident is **Declined**, the Assignee’s CAPA had been rejected and the Assignee’s has to give a CAPA again.
* If the Incident is put **ON Hold,** the Assignee’s CAPA is being reviewed and will be soon Accepted or Declined.