# Create a Missed SLA Form Procedure

Service Level Management

**Purpose**

The Missed SLA Form is used when an Investigation ticket is created to research a missed or breached SLA. Information from the Metric Data Definition spreadsheet, the CI Unavailability record, and the monitoring tool are added to the form by the Service Level Management team. Any Incident or Change tickets which pertain to the application being researched are included as part of the research. The Missed SLA Form is attached to the Work Log of the Investigation Incident ticket after Service Level Management has received information pertaining to the outage from Application Support or Incident Management.  
***Note:*** *If the “Actual %” is less than 100% but is above the compliance target percentage, the SLA is considered “Missed”. If the “Actual %” is less than the compliance target, the SLA is considered “Breached”.*

For more information see:

[Create an Investigation Ticket for Missed / Breached SLA Procedure](https://confluence.jacksonnational.com/pages/viewpage.action?pageId=575465311)

**Related Policy**

* [IT Service Management Policy](https://sharepoint.jackson.com/sites/itsmsd/servicelevelmanagement/Shared%20Documents/Pre%20December%202019/SLM%20Documents/Policy%2C%20Process%2C%20Procedures/SLM_Service%20Level%20Management%20Process.doc?d=wa1eaba53e1dc4b30abda2a0886981cc9)

**Audience**

The following groups are responsible for adhering to this document:

* Service Level Management

**Procedure**

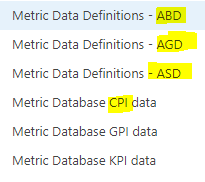
|  |  |
| --- | --- |
| Step | Action |
| 1 | Create the Missed SLA form:   1. Copy the “Missed SLA Form” located at:   [O:\share\Service Delivery\Service Level Management\SLA Reporting\SLA Working Spreadsheet\Missed SLA Forms](file:///O:\share\Service%20Delivery\Service%20Level%20Management\SLA%20Reporting\SLA%20Working%20Spreadsheet\Missed%20SLA%20Forms)   1. Paste the file in the same location, renaming it to represent the date of the missed / breached SLA and the service name. *Example:* 05-05-2020 STP.docx 2. Service Level Management fills in the section highlighted in yellow on the form.   Open the Metric Data Definition spreadsheet located on SharePoint to obtain information needed for the Missed SLA form. See **Appendix A** for more information.   1. Start filling out the Missed SLA Form:  * **Service Name** – Enter the service name from the ITSM Service Catalog.   It is the same name used in the MDD spreadsheet.   * **Breached or Missed SLA –** View the Detail Record for the specified   application to acquire the daily percentage for the date  being researched. This will determine if the SLA was  “missed” or “breached” based on data found in the  MDD spreadsheet.  For more information see:  [Detail Record Documentation](https://confluence.jacksonnational.com/display/CPENABLE/04+-+Detail+Record+Documentation)   * **Date / Time** – Use the start and end time from the CI Unavailability   record.  For more information see:  [Incident Ticket with CI Unavailability Record Documentation](https://confluence.jacksonnational.com/display/CPENABLE/05+-+Incident+Ticket+with+CI+Unavailability+Record+Documentation)   * **Outage Minutes on SLA Report –** Use the outage minutes from the   Detail Record.   * **Investigation Ticket Number** – Use the Investigation Incident ticket   number that has been created to investigate the  missed / breached SLA.   * **SLM CI Unavailability Incident Ticket Number** – Use the SLM Incident   ticket(s) number in which a CI Unavailability record is  attached.   * **Details that Feed the Monitor** – Paste the information from theMDD   spreadsheethere. See **Appendix** A for more  information.   1. Access the correct monitoring tool to view detailed information. The correct monitor to use will be found in the “Details that Feed the Monitor” section of the MDD spreadsheet. See ***Appendix A*** *&* ***B*** for more information. 2. Use the information from the monitoring tool to add data to the following sections of the Missed SLA Form:  * **Nagios Alerts** – Paste the alerts from the monitoring tool in this field. |
| 2 | Conduct research to attempt to find out why the SLA was missed:   1. Use information from the MDD spreadsheet and monitoring tools to perform searches within the following reports to incidents, changes, and problems that coincide with the time frame that the service outage occurred: 2. Review the following reports:  * [Non-Job Abend Tickets: Opened Since Last Business Day Report](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx" \l "/Daily%20Reporting/Forms/current.aspx) * Navigate to the current year * Click on “Incidents Opened in Cycle” * Navigate to the current month * Click on the “Production Infrastructure Non-Job Abend Report – Opened Since Last Business Day MMDDYY” report * [Production Problem Report: Opened Since Last Business Day Report](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx#/Daily%20Reporting/Forms/current.aspx) * Navigate to the current year * Click on “Problems Opened in Cycle” * Navigate to the current month * Click on the “Production Problem Report – Opened Since Last Business Day MMDDYY” report. * [Data Center Turnover Report](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx#/Daily%20Reporting/Forms/current.aspx?View=%7B1D5400F7%2DF40D%2D4DC8%2DAED7%2DCCDABECB8C2F%7D)   + Navigate to current year   + Click on “Data Center Turnover”   + Navigate to current month   + Click on the “MMDDYY AM Turnover” report. * [Weekly Change Control Report](https://sharepoint.jackson.com/sites/itsmsd/changemanagement/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fitsmsd%2Fchangemanagement%2FShared%20Documents%2FChange%20Control%20Meeting%2FWeekly%20Report&FolderCTID=0x012000138FEA7820874A4EAE91DC2929C0189D&View=%7B9A7534D2%2DA53B%2D4392%2D8E6A%2D40A96A04EFBD%7D)   + Click on “Change Control Meeting”. This report is created every Thursday and is a great assistance in searching for Changes that may have caused missed / breached SLAs over the weekend.  1. Use the BMC Remedy Incident search functionality:  * When performing a search, use the dropdown list in the “Services” field. This will show all incidents in which the service had an issue. * The most recent incident tickets will be at the top. * Try to match the dates and times to when the monitoring tool reported the outage.      1. If any incident, change, or problem tickets are found that match the time frame of the outage, add the information to the following field on the Missed SLA Form:  * **Research Results** – Type the incident, change, or problem ticket(s)   found. Include the summary of the problem, the  resolution, and any additional information that may  assist SIG or JTS with verifying or investigating the  outage. |
| 3 | Attach the Missed SLA form to the Investigation ticket.  For more information see:  [Create an Investigate Ticket for Missed / Breached SLA Procedure](https://confluence.jacksonnational.com/pages/viewpage.action?pageId=575465311) |
| 4 | **Save the Missed SLA Form**   1. The Missed SLA forms will reside at the following location while the Investigation tickets is still being worked.   [O:\share\Service Delivery\Service Level Management\SLA Reporting\SLA Working Spreadsheet\Missed SLA Forms](file:///O:\share\Service%20Delivery\Service%20Level%20Management\SLA%20Reporting\SLA%20Working%20Spreadsheet\Missed%20SLA%20Forms)   1. When the Missed SLA form has been completed and the Investigation ticket has been resolved, move the form to current month’s folder in the same location. 2. When all of the Missed SLA Forms for the month have been completed and moved to the current month’s folder, move the folder to the following location:   [O:\share\Service Delivery\Service Level Management\SLA Reporting\Reporting\YYYY\Daily SLA Report\Month\](\\\\jacksonnational.com\\SHARE\\hq\\vol3\\share\\Service Delivery\\Service Level Management\\SLA Reporting\\Reporting)   1. Publish all of the Missed SLA forms to SharePoint at the following location:   [Daily Reporting/SLM/YYYY/Daily SLA /Month/Missed SLA Form](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx#/Daily%20Reporting/Forms/current.aspx?RootFolder=%2Fit%2Fsites%2Frs%2FDaily%20Reporting%2FSLM&View=%7B1D5400F7%2DF40D%2D4DC8%2DAED7%2DCCDABECB8C2F%7D) |

**Appendix A – Metric Data Definition Forms / Details That Feed the Monitor**

Locate the correct [Metric Data Definition (MDD](https://sharepoint.jackson.com/sites/itsmsd/servicelevelmanagement/_layouts/15/start.aspx#/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fitsmsd%2Fservicelevelmanagement%2FShared%20Documents%2FPre%20December%202019%2FMDD%20Database%20Files&FolderCTID=0x012000C3EC5FEE7B19F646BACB9A57478C774E&View=%7B527EAB19%2D8D4A%2D47E6%2DACE1%2DCA631A3D99D0%7D)) spreadsheet in SharePoint.

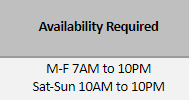
The Level (Bronze, Gold, Platinum, Silver) will already have been provided.

1. Access the correct spreadsheet in which the application falls under.

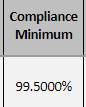


* + **ABD** – Aggregate Bronze Definitions
  + **AGD** – Aggregate Gold Definitions
  + **ASD** – Aggregate Silver Definitions
  + Metric Database CPI Data – Platinum definitions

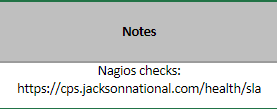
1. Locate the application in the spreadsheet.
2. Review “Column M” (Availability Required) on the specified application’s row. This is information is needed to determine if the outage occurred during the application’s availability window.



1. Review “Colum F” (Compliance Minimum) on the specified application’s row. This will be used to determine if the daily SLA compliance target was “missed” or “breached”.



1. Review “Column S” (Notes) on the specified application’s row. This information will be used for the “Details that feed the monitor” field of the Missed SLA form.



**Appendix B - Nagios Monitoring Tool**

Nagios is a [free](https://en.wikipedia.org/wiki/Free_software) and [open source](https://en.wikipedia.org/wiki/Open_source) [computer](https://en.wikipedia.org/wiki/Computer)-[software application](https://en.wikipedia.org/wiki/Software_application) that [monitors](https://en.wikipedia.org/wiki/Event_monitoring) [systems](https://en.wikipedia.org/wiki/System_monitor), [networks](https://en.wikipedia.org/wiki/Network_monitoring) and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services. It alerts users when things go wrong and alerts them a second time when the problem has been resolved.

<https://en.wikipedia.org/wiki/Nagios>

1. The Web Admin Nagios monitoring site is located at:

<https://webnagios.jacksonnational.com/nagios/>

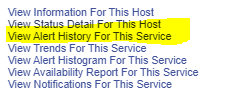
1. Type “SLM” in the “Quick Search” field.



1. The services that are preset to auto-create SLM Incident tickets with CI Unavailability records attached are listed.



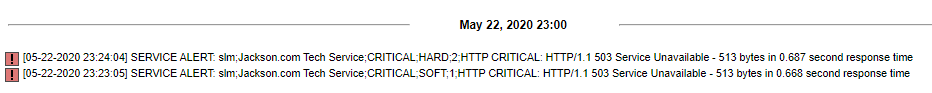
1. Click the Service name to access more information.
2. Click the “View Alert History for This Service” link near the top of the screen.



1. Click the “Earlier Archive” arrow to navigate backwards to the outage date that is being researched.



1. Look for information during the time frame in which an SLM Incident ticket with a CI Unavailability record was created. This data will be placed in the Missed SLA Form under “Nagios Alerts”.



1. The Windows Nagios site is located at:

<https://dc0xpnagv004.jacksonnational.com/thruk/#cgi-bin/status.cgi?hostgroup=all&style=hostdetail>

1. Type in the service name or a server name in the search field.



1. There are only a few services that are monitored for SLAs under the Windows Nagios site. These are not currently hooked up to Remedy to auto-create SLM Incident tickets with CI Unavailability records, but Nagios can be used to look up additional information when outages are discovered via manual monitoring.

For more information see:

[Manually Monitor Services Procedure](https://confluence.jacksonnational.com/display/CPENABLE/01+-+Manually+Monitor+Services+Procedure)

1. Follow c) through f) above.

**Modification**

The following associates can make modifications to this document:

* Manager, Service Level Management
* Director, IT Service Management
* Vice President, Service Delivery
* Chief Technology Officer, PGDS

|  |  |
| --- | --- |
| Service Level Management Process | |
| Responsible Party: Sharla Piepkow, Manager, Service Level Management Approving Authority: Rob Kolm Director, IT Service Management | Date Created: 02/09/2018 Last Modified: 05/26/2020 Last Reviewed: |