Incident Management Process

Version 3.0

PROCESS INFORMATION

This table should be completed by the responsible office and IT Risk & Compliance, as it provides general information about the process.

RESPONSIBLE OFFICES	ITS Enterprise Service Delivery (ESD) - Technology Support & Quality Management – Support Center
RELATED DOCUMENTS	• University Policy Number 1305, Reporting Electronic Security Incidents Policy • ITS.ITSO-PROC004, Security Incident Response Procedures • ITS.ESD-PRS003, ITS Unplanned Service Disruption Communications Process • DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
REFERENCE DOCUMENTS	None
DOCUMENT CONTROL NUMBER	ITS.ESD-PRS004
PURPOSE	The intent of this document is to provide effective incident management within Mason's Production ITS environment during an incident while simultaneously providing transparency to the root cause and lessons learned after the incident is resolved.
LAST REVIEWED DATE	5/2/2024

NOTE TO ALL USERS

REVISION HISTORY

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
2.0	08/11/2020	ITS-IT Process & Planning/Randy Anderson	1. Major Revisions – a. sentence deletions and rewrites in the Benefits Section b. updated definition of USDC Process in the Definitions Section 2. Minor Revisions a. updated process owners to Technical Support Services – Support Center b. fixed mechanics and syntax throughout the document c. updated process format to the current version (1.3)

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
			d. updated some KPIs in the Metrics Section
2.1	02/08/2021		Minor Revisions 1. Added DFARS Clause 252.204-7012 in the References section 2. Updated process to address DFARS Clause 252.204-7012 requirements for ITAR 3. Added Document Control Numbers in the Reference
3.0	04/30/24	Technology Support & Quality Management	Update to proper form, move documents in the Reference Documents to Related Documents since none of those documents were cited in the process, major edits to process to include Outage and Problem Management into Incident Management process, and addition of Appendix A (Ticket Priority Matrix).

PROCESS SCOPE

This document applies to the entire production environment and all ITS employees who manage assets or configuration items including all infrastructure, databases, applications, and endpoints where applicable. It is expected to be followed for all unplanned service disruptions. The communication requirements will be determined during each occurrence based on severity, existing or potential impact, and requests by management for updates.

The process…

1. ITS Incident Management is the process of identifying, triaging, and resolving incidents while, at the same time, communicating to the appropriate individuals and/or teams who have an interest in the status of the incident at any point in time. The process begins with the identification of an issue with any service or piece of infrastructure not functioning as expected. Typically, these issues are identified by customer inquiries, automated monitoring/alerting, or identification of an issue by an ITS resource.
2. The ITS Incident Management process's main goal is to resolve the issue efficiently while minimizing business impact, security impacts, risk, and cost. All ITS incidents that occur at Mason will be documented in the ITSM tool. To achieve this, the Incident Management procedure includes the following steps.

The process is applicable when:

1. A customer contacts an ITS representative with information regarding a service that is not working as expected.
2. An ITS representative during their work finds that a service is not functioning as expected.
3. An ITS Monitoring system shows that a service or asset, examples are a phone, server, database, router, etc. is non-functional and a member of the support group for that service or asset needs to determine what has caused the issue.

PROCESS INPUTS & OUTPUTS

Process Inputs

1. Contact from customer (email, phone, chat, or in person).
2. Technician sees alert in monitoring system.
3. Automated Email generated by a system is received by the ITSM Tool.

Process Outputs

1. Incident Ticket generated, manually or systematically based on input method.
2. Group assigned to work on Incident ticket.
3. SLA assigned to ticket based on Priority.

DEFINITIONS

ACRONYM/TERM	DEFINITION
Incident	A break/fix scenario. A service or asset is no longer functioning. Incidents could include Outage or Problem tickets, which are a higher level of Incident ticket.

Incident Ticket	A completed Incident form in the ITSM Tool.
Group	A selection of people assigned as pool of users that works on specific types of issues.
Service Level Agreements/SLA	Service Level Agreement. There are two forms of SLA associated with an Incident Ticket: 1. Respond By: this is the time limit based on the Priority of the Ticket that an ITS staff member should be contacting the customer to let them know the ticket has been received and a review of the issue has started. 2. Resolved By: this is the time limit based on the Priority of the Ticket by which the Incident should be fixed. SLAs do not include the time waiting for a customer or vendor response. The SLA Respond/Resolve times are explained in Appendix A: Ticket Priority Matrix
Dispatcher	The ITS staff assigned to review the ticket queue regularly during the workday and assign tickets to other members of the group or to another group if the ticket was assigned improperly.
Impact	This represents how many people are affected by the Incident. There are 7 levels: • Affects only ITS Service Operations. • Affects a single individual. • Affects a single building. • Affects a single department. • Affects multiple buildings. • Affects multiple departments. • Affects the entire University
Urgency	This represents how the customer is affected by the Incident. There are four (4) levels: • Work Stopped – No Workaround • Work Stopped – Workaround • Work Impaired • Work not Impaired
Priority	This is based on the Impact and Urgency according to the table in Appendix A: Ticket Priority Matrix
ITSM Tool	The current ITSM Tool used by ITS and other Departments/Units at Mason is TeamDynamix.
Service Owner	The ITS Director is responsible for a specific service.
Incident Manager	The ITS staff chosen by the Service Owner to be the main point of contact during the Incident, Outage, and Problem. The Incident Manager is responsible for all outgoing communication on an Incident ticket regardless of level of ticket (Incident, Outage, or Problem).
Outage	An issue has occurred to affect a service. The service could be partially impacted, service is available but is slower than normal, or completely unavailable.
Problem	An issue has occurred to affect a service. The service could be partially impacted, service is available but is slower than normal, or completely unavailable, but there is a workaround that can be put in place to mitigate the outage in a temporary fashion.

USDC-L Listserv	Unexpected Service Disruption Communications list. This is a list of all managers and above level staff within ITS.
ITS Alert	This is a function completed by the ITS Support Center and the Facilities & Infrastructure Operations group. They receive request for alerts to be sent to the ITS Alerts Listserv during outage or Problem situation.

FLOWCHARTS

Provide an image of a Visio diagram to show process steps.

None

HIGH-LEVEL PROCESS OR STEP

Provide high-level process description along with the activity outputs for each process step.

PROCESS/STEP DESCRIPTION	Responsible Group	Output(s)
Formal Incident ticket created		
1. Customers contact ITS. This could be through various methods such as Phone, Email, Chat, In Person, or the TDX Client Portal Self-Service function.	Varies depending on issue and method of contact	Incident Ticket
2. ITS Staff member notices an issue due to monitoring service or while performing a normal job function.	Varies depending on issue and method of contact	Incident Ticket
3. Monitoring tools such as event monitoring platforms, sends a notification.	Varies depending on issue and method of contact	Incident Ticket
PROCESS/STEP DESCRIPTION	**Responsible Group**	**Output(s)**
Categorize and Prioritize the Incident		
1. Ticket is assigned to appropriate group	Varies based on type of incident	Ticket assigned to Group
2. ITS Resource (Dispatcher/Manager) for group performs triage on the Incident ticket to determine if the priority is correct and if this issue represents an Outage or Problem scenario.	Varies based on type of incident	Properly prioritized ticket.

3. If Incident is determined to be an Outage or Problem, the appropriate Outage or Problem Management process is invoked.	Varies based on type of incident	Invocation of Outage or Problem Management processes.
4. Incident Tickets are assigned to Technician	Member of Group	Assigned ticket
5. Assigned Technician reviews ticket, contacts customer to state ticket has been received and review has begun	Assigned Technician	Ticket status "In Process"
6. If Assigned Technician has questions for the customer or vendor, contact is made, and the ticket is placed on hold.	Assigned Technician	Customer/vendor contacted, Ticket placed in appropriate hold status: Wait Customer or Wait Vendor
7. Assigned Technician works on the issue to resolve it. Contacts customer that the issue should be resolved, and customer should test.	Assigned Technician	Ticket in "Resolved" status.
8. Customer responds issue is not fixed	Assigned Technician	Ticket moved to "Customer Responded" status. Work goes back to Step 5.
PROCESS/STEP DESCRIPTION	**Responsible Group**	**Output(s)**
Outage Management		
1. The Incident Manager and/or the appropriate team member(s) will engage, in the timeliest manner possible, to confirm the incident being reported is accurate and do an initial assessment to determine the impact and root cause. Once understood, those responding to the incident will work to resolve it as quickly as possible. Creation of the Outage ticket is completed. This is done following the guidelines shown in the Outage Management Knowledge Article.	Service Owner/ Technicians	Outage process initiated.

2. The Service Owner chooses the Incident Manager, which may be themselves or someone on one of their service groups. The Incident Manager will be separate from the team working on the issue, so they are available to speak with other groups or handle communications.	Service Owner	Outage Ticket assigned to Incident Manager
3. Based on the severity and complexity of the incident and a reasonable estimate of time needed to resolve, the Service Owner and/or Incident Manager must identify their communication plan to include the frequency of their communications and the audience that needs to be included. Ideally, this communication should be done through the Incident ticket itself where the audience is contained to ITS staff and a limited number of impacted users. For broader communications, ITS Alerts and/or the USDC-L email list should be used as needed. An email can be sent to the entire Mason Community, Senior Leadership and ITS Communications and Marketing will need to be involved.	Incident Manager /Service Owner	Email to specific customers, USDC-L, ITS Alerts, or E-Files Alert as appropriate
4. The Incident Manager must ensure that the Outage Ticket is kept up to date and contains a full accounting of the troubleshooting, findings and steps used to resolve the issue. If there are multiple incident tickets for a given incident, the Incident Manager will ensure all other tickets are identified as Child tickets and assigned to the Outage ticket. This is done following the guidelines shown in the Outage Management Knowledge Article. It is possible that the Outage Ticket be changed to a Problem Ticket if a workaround is in place while a permanent resolution can be identified and tracked. This is done by changing the Classification of the ticket. The Problem Management process would then be followed. Once email has been sent to either or both groups, regular updates should be sent on a schedule determined by the Incident Manager and Service Owner. Customer notifications should include when the next update will occur where reasonable	Outage Manager /Service Owner	Email to selected customer base
5. In some instances, resolution of the Incident may require one or more Emergency Request	Incident Manager / Technician	RFC creation

for Change be created and implemented. Change Management policies and procedures should be followed as needed. Change tickets can be created following the steps provided in the Creating an Request For Change Knowledge Article.		
6. If communication was sent to customers, the Incident Manager will send either a resolved/all clear type message that explains in general terms for the public what caused the issue and how it was resolved.	Incident Manager	Email sent to customer base
7. Once the Incident is resolved, the customers affected by the outage will be contacted to ensure they see that the Incident is resolved.	Support Center	Closed Child Tickets
8. Once all Child tickets are closed, the Outage ticket can be closed.	Outage Owner/ Service Owner	Closed Outage Ticket
9. Once an Incident is resolved, the Incident Manager will be required to complete an After-Action Review form, be available for discussions with management and/or peers to share lessons learned or speak to a broader audience to ensure transparency of what caused the incident, how it was resolved, and what measures can/will be taken to prevent it from recurring.	Incident Manager & Technician	After Action Report created and submitted for posting.
PROCESS/STEP DESCRIPTION	**Responsible Group**	**Output(s)**
Problem Management		
1. Problem Management follows the same steps as Outage Management with one exception: the communication of the workaround. If a workaround is determined, this will be communicated as quickly as possible with the affected users. This is done following the guidelines in the Problem Management Knowledge Article.	Service Owner, Problem Manager, Technician	Problem Ticket used instead of an Outage Ticket.
2. The Problem ticket will be closed when a permanent fix is in place.	Incident Manager/Service Owner	Closed Problem Ticket
3. Once an Incident is resolved the Incident Manager will be required to complete an After-Action Review form, be available for discussions with management and/or peers to share lessons learned or speak to a broader audience to ensure transparency of what caused the incident, how it was resolved, and what	Incident Manager & Technician	After Action Report created and submitted for posting.

measures can/will be taken to prevent it from recurring.		

ARTIFACTS

ARTIFACT	PURPOSE
Outage Ticket	A higher-level Incident ticket that can be used when multiple users are affected by the same issue. This ticket can have Child tickets assigned to it, so the overall effect of the Outage can be known. Outage tickets are never assigned directly to a customer but to an Incident Manager.
Problem Ticket	A higher-level Incident ticket that can be used when multiple users are affected by the same issue. Problem tickets can have a workaround that is put in place to bypass the issue while a permanent fix is found. This ticket can have Child tickets assigned to it, so the overall effect of the Problem can be known. Problem tickets are never assigned directly to a customer but to an Incident Manager.
Incident Ticket	This ticket is used when a single user is reporting an issue.
After Action Report	A report explaining what the Initial Symptoms, Root Cause, Prevention, Resolution, what ITS Teams worked on the issue, what effect the issues had on customers, and what systems/services were affected by the issue.
Request for Change	A ticket that states what work needs to be done to implement a change in a configuration.

TIMETABLE FOR REVIEW

This process will be reviewed annually.

APPROVALS

ROLE	NAME & ORGANIZATION	SIGNATURE	DATE
ITS ESD Technology Support & Quality Management Director	David Lutz	DocuSigned by: David Lutz 184177D2DB924A6...	5/7/2024

Appendix A

Ticket Priority Matrix

SLA Clock Runs		Target Response	Impact Level: Critical • Entire University Affected			Impact Level: Major • Multiple Departments Affected • Multiple Buildings Affected			Impact Level: Minor • Single Department Affected • Single Building Affected			Impact level: Small • Outside of Service's operating hours • Affects only ITS Service Operations • Single Individual		
Priority														
Version 1		Target Resolution												
Urgency: Work Stopped - No workaround			24x7		15 minutes	24x7		1 hour	24x7		1 hour	Business Hours		8 hours
			Emergency Outage Management			High			High			Standard		
					4 hours			8 hours			8 hours			16 hours
Urgency: Work Stopped - Workaround available			24x7		1 hour	24x7		1 hour	Business Hours		8 hours	Business Hours		8 hours
			High Problem Management			High Problem Management			Standard			Scheduled		
					8 hours			8 hours			16 hours			32 hours
Urgency: Work Impaired			24x7		1 hour	Business Hours		8 hours	Business Hours		8 hours	Business Hours		8 hours
			High			Standard			Standard			Scheduled		
					8 hours			16 hours			16 hours			32 hours
Urgency: Work not Impaired			Business Hours		8 hours	Business Hours		8 hours	Business Hours		8 hours	Business Hours		8 hours
			Standard			Scheduled			Scheduled			Scheduled		
					16 hours			32 hours			32 hours			32 hours