VCU Technology Services

Major Incident Communications Plan

October 2022 - Version 1.5

Goals and Objectives

The goals of major incident response communication are:

- Ensure that IT personnel, customers, and other stakeholders receive concise and consistent updates during an IT outage.
- Provide appropriate transparency throughout the process to those requiring information.
- Reduce conflicting messages and confusion about a major IT event.

The primary objective of this document is to define the process for handling communications during a major IT incident resulting in a critical/high system or service disruption or outage. Additionally this document:

- Outlines expectations for communications during a major IT incident.
- Provides guidance to identify key stakeholders, customers and IT partners across VCU that require communications and updates during a major IT incident.
- Documents what tools, templates and other communication resources are utilized to manage communications during a major IT incident.
- Documents communications frequency based on the classification of the incident per the Impact and Urgency Matrix in the TS Major Incident Response Plan.

Roles and Responsibilities

Incident Response Coordinator (IRC)- The Incident Response Coordinator is the on-call individual who is responsible for coordinating the response to a major IT incident. This role also acts as primary communications coordinator during a major incident, ensuring communications to all stakeholders are occurring to alert them of the incident, provide status updates, and resolution information when the incident has been resolved. The IRC does not have to send all communications, but must ensure they are being sent out from relevant parties to key stakeholders found on the Major Incident Communications Management Plan.

Incident Response Team (IRT)- The Incident Response Team are employees who respond to and assist in the remediation of an IT incident. During a major incident, they are responsible for communicating information to the Incident Response Coordinator timely, efficiently and accurately throughout the major incident process.

IT Support Center (ITSC)- The IT Support Center is the front line communication between VCU customers and the **Technology System/Service Owners** during an incident. They are responsible for managing all customer contacts related to an incident and providing up to date information related to the incident status and its estimated time of recovery.

TS ICT Members - The TS members who are responsible for acting as liaisons between the Incident Response Coordinator and the ICT are the CIO and senior directors. They will provide counsel and information to the ICT during a critical IT incident.

IT System/Service Owners - TS staff who are IT system and service owners. May or may not respond as part of the Incident Response Team depending on impact of incident.

Stakeholders - Stakeholders are members of the VCU community who are accessing a VCU TS owned IT system or service or who may be affected by an IT incident. This can include but is not limited to: VCU faculty, staff, students, researchers, distributed IT professionals, VCU Health System employees, etc.

Communication Oversight

The on-call person who assumes the Incident Response Coordinator role during a major IT incident (see TS Major Incident Response Plan) is responsible for ensuring that all internal and external communications occur during the lifecycle of an IT incident. Any communications sent to customers, IT personnel, and all other stakeholders must be vetted and approved by the Incident Response Coordinator.

> **IMPORTANT:** If an incident occurs and it is found to not be a major incident (determined to be a medium or low incident per the Impact and Urgency matrix), it is the responsibility of the TS system/service owner to coordinate communications to affected stakeholders.

All external communications about an incident or incident response to external parties ***outside*** of VCU are made in consultation with TS Leadership, ICT and University Relations.

Communications Process

The Incident Response Coordinator (IRC) must ensure appropriate communications are sent out during each step of the Major Incident Response Process:

Step	Activity	Communications
1	Detection and Activation	● A major incident is detected, and declared. ● On-call Incident Response Coordinator (IRC) responds to the major incident. ● The **IRC** assembles the preliminary **Incident Response Team (IRT)** to begin the response. This coordination occurs with a message sent to the TS Major Incident Chat Space. ● War Room activation is available for ease of coordination if needed.
2	Investigation	● **IRC and IRT** determine risk, scope, impact of incident. ● **IRC** determines whether to activate VCU ICT. ● Coordinate with TS ICT Members.

		• **IRC** coordinates initial and continued outage notifications to internal and external stakeholders with estimations for remediation/recovery occur.
3	Remediation	• **IRC** ensures status updates and/or recovery estimations are communicated to internal and external stakeholders.
4	Resolution and Recovery	• **IRC** ensures final status information is communicated to internal and external stakeholders.
5	Postmortem Report	• **IRC** creates and distributes copy of Postmortem Incident Report

TS Major Incident Chat Space

The primary communication tool used during incident response is the TS Major Incident chat space. All members of Technology Services staff have access to this chat space to track the incident and any and all updates in real time.

Chat Space Guidelines

- Use this space only during a major incident.
- Communicate clearly and professionally.
- This space is used to collaborate with colleagues with positivity and respect.
- All Technology Services can access this chat, so be mindful when posting or responding to information.
- If your system/service is not directly impacted by a Major Incident, please refrain from interjecting in the chat to ensure the space is used for those who need to respond/collaborate.

War Room Activation

In the event of an incident that is determined to be of Critical or High impact, a War Room is activated by sending a message to the TS Major Incident chat space. This will allow for the Incident Response Coordinator, the Incident Response Team, and all other applicable IT personnel to coordinate in real time.

The war room tool used for TS incident response is a standing virtual call. This virtual call is always available for activation and anyone with the link can access the room at any time. Incident Response Coordinators and TS Leadership all have co-host privileges for this virtual call. The War Room virtual meeting is set to record automatically and save the recording to the cloud. Connection details for this virtual call are as follows:

[Redacted for privacy reasons]

Stakeholders, Channels, and Frequency

Please see the following Major Incident Communications Management Plan document to view stakeholders, communication channels and communication frequencies.

Communication Standards and Tips

Communications during an IT incident must contain the minimum information necessary and be in terms digestible/understandable to the audience.

Internal Communications - Guidelines

- Communicate as soon as the incident is detected; acknowledging the issue, and providing as much known information so that system/service owners can determine "What-when-where-and who is impacted" quickly.
- Communicate often, providing updates regularly to keep IT personnel informed.
- Communicate consistently using primary communication channels when available and updates are relevant to stakeholder groups

External Communications - Guidelines

- Communicate early and quickly; reporting the issue as soon as customer impact has been verified.
- Communicate precisely, with honesty, clarity and transparency. Make sure the issue is explained in how it impacts different customers. Use relatable, customer friendly, and easy to understand terms. Be brief and to the point. Remove all technical jargon, language and IT references and instead describe the impact the customer will have related to the incident, rather than the cause/reason of the incident.
    - Examples:
        - Instead of *"CAS is experiencing intermittent outages, we are investigating the cause"* instead say:
            - *"Customers will experience issues with logging into the Central Authentication Service (CAS), which will prevent them from accessing systems such as Canvas, myVCU, eServices, etc."*
        - Instead of "*We are experiencing email delivery delays at our incoming Cisco gate*" instead say:
            - "*Customers will see delays in sending and receiving email."*
        - Instead of *"We are experiencing an issue with wireless authentication systems. This is impacting VCU SafeNet SSID access"* instead say:
            - *"Customers will experience issues in connecting to VCU SafeNet wireless."*
    - Utilize the templates to develop these communications. Provide an estimated time of recovery if possible, or estimated time of next update.

- If a temporary workaround is identified, provide a link to documentation for customers to refer to.
- Communicate often, providing updates regularly to keep customers informed.
- Stay consistent across all communication channels, make sure updates are consistent and relevant to the customer/stakeholder group.

Plan Access and Maintenance

Plan maintenance should include all activities required to keep the VCU TS Major Incident Response Plan current and up to date. This plan will be required to be reviewed during the annual Disaster Recovery Plan update cycle that occurs in the summer of each year.

Appendix

Major Incident Communications Management Plan

VCU TS Major Incident Response Plan

VCU TS IRC On Call Schedule and TS Emergency Contact Information

Incident Response Checklist Template