



Technology Solutions – Incident and Outage Communications

Department: Technology Solutions

Procedure Name: Incident and Outage Communications

Procedure ID: TS-PROC-007

Effective Date: 01/21/2026

Last Reviewed: 01/21/2026

Owner: Chief Information Officer (CIO)

Applies To: All Technology Solutions staff

1. Purpose

This procedure defines the required actions, communication standards, ownership, and documentation expectations for incident and outage response within Technology Solutions. The objective is speed, clarity, accountability, and consistency during high-stress situations.

2. When This Procedure Is Used

This procedure is triggered immediately when any of the following occur:

- A system, service, or application is unavailable or unstable
- Multiple users report the same issue
- A security concern is suspected
- The cause of an issue is unknown
- There is potential campus-wide or institutional impact

If there is uncertainty whether an issue qualifies as an incident, it must be treated as an incident and this procedure followed.

3. Step 1 – Declare the Incident (No Analysis Yet)

As soon as an incident is identified, the following actions are required:

- Navigate to the Technology Solutions Microsoft Teams site
- Start a new post in the Incident Response channel
- Do not investigate first
- Do not start side chats
- Do not wait for confirmation

The initial post must include, at minimum:

- What is happening (plain language)
- When it started or was noticed



- Who or what appears impacted
- What is unknown

This step exists to initiate coordination, not to establish root cause or confirmation.

4. Step 2 – Leadership Assigns an Incident Owner

A Technology Solutions leadership member (Director, Executive Director, or CIO) will assign a single incident owner and confirm ownership in the Incident Response channel.

The incident owner is responsible for the entire incident lifecycle, including:

- Driving investigation activities
- Ensuring cross-team participation
- Maintaining communication updates
- Declaring resolution
- Completing post-incident documentation

5. Step 3 – Mandatory Cross-Team Investigation

Once an incident owner is assigned, every Technology Solutions team must investigate. Participation is mandatory and assumptions are not acceptable.

Each team must:

- Review systems under their responsibility
- Perform sufficient checks to confirm impact or rule out involvement
- Post findings directly in the Incident Response channel

Each team update must include:

- What was checked
- What was found
- A clear conclusion (impacted / not impacted)

Statements such as 'we don't think it's us' are not acceptable responses.

6. Step 4 – Active Incident Coordination

During an active incident, all communication must remain within the Incident Response channel. Side chats, emails, or texts are not permitted. The Incident Response channel serves as the single source of truth.

7. Step 5 – Resolution Declaration

An incident is considered resolved only when service is restored or stabilized, no further technical action is required, and stakeholders have been informed where applicable.

The incident owner must post a resolution message including:



- Date and time of resolution
- What resolved the issue
- Confirmation that monitoring is stable

8. Step 6 – Post-Incident Documentation (Mandatory)

Within 24 hours of resolution, the incident owner must complete the Incident Investigation and Root Cause Report using the approved Technology Solutions template.

The report must include:

- Incident timeline
- Team investigations
- Root cause
- Corrective actions
- Preventive recommendations

The report must be saved in Microsoft Teams under Incident Response → Files using the naming convention: **INC-YYYYMMDD-Incident-Title**.

9. Step 7 – Leadership Review & Closure

The completed incident report must be shared with Technology Solutions leadership. Leadership may require follow-up actions, preventive changes, or additional reviews.

10. Behavioral Expectations During an Incident

- Follow the procedure, not instincts
- Over-communicate in the Incident Response channel
- Investigate even when confident
- Document actions as they occur
- Remain calm and methodical

11. Compliance

This procedure is mandatory and governed under TS-PROC-001. Failure to follow this procedure may result in formal leadership review or corrective action.

12. Review Cycle

This procedure will be reviewed annually or as organizational or operational needs change.