



Gonzaga University Information Technology Policy and Procedure

SUBJECT: Post Critical Incident Reporting

Policy Number	Date Issued	Date Reviewed
IT104		

PURPOSE:

This policy outlines a structured process and analysis to be undertaken by Gonzaga Information Technology Staff when a critical incident occurs. The purpose of this policy is to:

- Determine the root causes of a critical incident
- Reduce the likelihood of future critical incidents
- Recover from critical incidents rapidly
- Ensure appropriate communication and documentation around the event

SCOPE:

This policy applies to all critical incidents and those responsible to resolve critical incidents.

POLICY:

The manager(s) of the area(s) responsible for the service most significantly affected by a critical incident will submit a written report in a timely fashion.

The department director(s) will ensure that all corrective action is accomplished and will report the conclusions of the incident to the Chief Information Officer (CIO) in a timely fashion.

The office of the CIO will retain records of the actions and reports provided by the director.

DEFINITIONS:

Critical incident - is any incident that makes unavailable one or more services in the IT Service Catalog apparent to a significant number of users.

Corrective action – Steps taken to eliminate the cause of a detected critical incident.

Incident – any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in the quality of that service.

Manager – person who is primarily responsible for the area or service.

Preventive measures - Action taken to prevent a problem from occurring, based on an understanding of the product or process. Preventive action will address inadequate "conditions" which may produce critical incidents.

Root cause – The source or origin of an event, the most basic reason, which if eliminated, would prevent recurrence.

Service – those applications, resources, and connectivity directly or indirectly related to the information technology structure and infrastructure.

Upgrade – software that updates and upgrades a piece of software to a newer version while keeping the settings and data from the prior program.

User – Any person who uses a computer or related service.

PROCEDURE:

I. Reporting

- a. The manager of the area or service shall submit a written report to the department director within 7 days of the incident's resolution.
- b. The report shall include:
 - The root cause(s) of the incident (if possible)
 - An analysis of the department's response in restoring normal operations
 - Corrective action taken
 - Modifications, upgrades, or other changes that can reduce the likelihood of future occurrences of the incident

II. Corrective Action

- a. The manager submitting the report will meet with the area director and agree on preventive measures.
- b. The department director will submit the original report along with agreed upon preventive measures to the CIO.

III. Follow Up

- a. The department director will ensure that all corrective actions are accomplished.
- b. Once all corrective actions have been completed, the department director will record those actions and send that report to the CIO.
- c. Reports regarding the incident will be made available to the appropriate individuals or groups.

IV. Record Keeping

- a. The CIO's office will keep a record of all incidents in the appropriate shared folder.
- b. The CIO's office will also keep a record of successfully completed preventive measures.

ENFORCEMENT:

Any University personnel found to have violated this policy may be subject to disciplinary action, at the discretion of their supervisor, as described in the university's **Personnel Policies and Procedures Manual**.

Date:	President or Designee