MAJOR INCIDENT COMMUNICATIONS

IT services require timely communications during emergency situations.

Stanford | University IT

IMPACT LEVELS	CRITICAL SC1 **Service Criticality 1 (SC1): Mission Critical Services** require continuous availability.	MAJOR SC2 **Service Criticality 2 (SC2): Business Critical Services** require continuous availability for effective business operation.	MODERATE SC3 **Service Criticality 3 (SC3): Business Operational Services** contribute to efficient business operations.
Risk 1 Impact: Widespread (location or service outage) **Risk 2 Impact:** Limited (3-50 users) **Risk 3 Impact:** Localized (1-2 users)			
Priority 1 P1	Initial client notification is required within 15 minutes of activation. Healthcare updates required every 30 minutes. Non-healthcare updates required every 1 hour.	SC2 services do not qualify for P1 process.	SC3 services do not qualify for P1 process.
Priority 2 P2	Initial client notification is required within 2 hour of activating major incident. Healthcare updates required every 30 minutes. Non-healthcare updates required every 2 hours.	Initial client notification is required within 1 hour of activating major incident. Healthcare updates required every 30 minutes. Non-healthcare updates required every 2 hours.	If an SC3 service is experiencing a widespread impact, they can be promoted for Major Incident and will follow P2.
Priority 3 P3	No major incident communications are required.	No major incident communications are required.	If an SC3 service is experiencing a widespread impact, they can be promoted for Major Incident and will follow P2.

SERVICE CRITICALITY 1: Mission Critical Services

- Email
- Oracle Financials
- Paging Services
- PeopleSoft
- Phone Services
- ServiceNow
- SUNet Backbone
- Web Authentication and Authorization
- Zoom

SERVICE CRITICALITY 2: Business Critical Services

- Cardinal Print
- FASA
- Jira
- Reporting Applications
- Slack Grid
- Workgroup Manager

SERVICE CRITICALITY 3: Business Operational Services

- Authority Manager
- Enterprise Datawarehouse
- My SQL Form Builder
- Smartsheet
- Tableau
- Qualtrics

MAJOR INCIDENT PROCESS

The Major Incident Process can be viewed here.

For questions regarding communication procedures, please contact:
Mike Dimaano, ITOC Manager: mdimaano@stanford.edu
Marty Dart, ITOC Technical Lead: mldart@stanford.edu

NOTIFICATIONS AND ALERTS

After major incident activation notifications, automated notifications are sent to: CI Service Owner, Technical Operations Owner, Service Manager, UIT Service Desk, and ITOC.

Service alerts and planned outage notifications can be found on uitalerts.stanford.edu.

Internal UIT collaboration for Major Incident and DOC response is initiated in the #itoc Slack channel.