Incident Communications

Prepared for Front Line Alerts Procedure group

Prepared by
Drew McConnell
Information Officer
IT Services
University of Glasgow

June 2007
Updated Jan 2011
# Contents

Summary ........................................................................................................................................... 4

Background ......................................................................................................................................... 5

Incident communication ...................................................................................................................... 6

Factors .............................................................................................................................................. 6

Incident sources ................................................................................................................................ 6

Audiences ......................................................................................................................................... 6

Channels for communication ........................................................................................................... 6

Message content .............................................................................................................................. 7

Current situation .............................................................................................................................. 7

Methodology .................................................................................................................................... 7

Current practice .............................................................................................................................. 7

Proposal ........................................................................................................................................ 8

A possible template for incidents .................................................................................................... 8

Unplanned incidents .......................................................................................................................... 8

Planned incidents ............................................................................................................................... 10

Closing an incident ............................................................................................................................ 10

Reviewing an incident ....................................................................................................................... 10

Areas for development ..................................................................................................................... 10

Documentation ................................................................................................................................. 10

Publicity ........................................................................................................................................... 10

Proposed roles and responsibilities .............................................................................................. 11

Staff cover ....................................................................................................................................... 11

Communication channels ............................................................................................................... 11
Conclusions................................................................. 12
References........................................................................ 13
Appendix 1........................................................................ 14
  Diary of an unplanned incident ...................................... 14
Appendix 2........................................................................ 16
Summary

Current incident communication methods require a review in order to ensure an accurate message is being given to the correct audience in a timely manner using the appropriate language.

The proposals are:-

- The Help desk will act as a single point of contact for reporting all incidents and changes.
- The Information Officer will be responsible for publishing information to the appropriate communications channels including the Service Alerts.
- The Incident coordinator (the person managing the incident investigation and fix activity) will communicate through the Information officer.

This will help to protect and improve IT Services (ITS) reputation as well as allowing service teams to work uninterrupted.

There are several areas that are in need of development. These are:

- Documentation
- Publicity
- Roles and responsibilities
- Communication channels
Background

An incident may affect one or more users. When an incident is expected to impact on a large number of users it is necessary to communicate this to them in an appropriate and timely manner.

IT Services currently has several difficulties in communicating to the user community in the event of a planned or unexpected major loss or disruption of service. These include channels of communication that are not well known to our audiences and ambiguous internal processes for utilising those channels.

The purpose of this report is to explore channels and methods of providing information to various University stakeholders in the event of a disruption or loss to a service provided by IT Services. The report will describe current internal and external communication procedures in the event of an incident, either planned or unplanned, and propose a template for incident communication management.

This report will focus on the communication process to the user and IT community. It will not define the types of service losses or on Business Continuity (BC) or Disaster Recovery (DR) processes.

Definitions:

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.

Incident Co-ordinator (IC) - the person responsible for managing an incident response. This person would normally be the team leader of the affected service or an ITS director depending on the scale and nature of the incident. In the event of an unidentified incident the Information officer or the Helpdesk may be the IC until the incident is identified and passed to the appropriate team.

Change Co-ordinator (CC) - the person responsible for managing a change.

IO – Information Officer or deputy

N.B For the purposes of this report a planned change will be considered as a type of incident.
Incident communication

Factors
There are several factors to take into account for the successful communication of an incident these are:

- Incident sources
- Audiences
- Channels for communication
- Message content

Incident sources
When there is an incident the initial notice may come from several sources:

1. Helpdesk
2. Other IT Services staff
3. Distributed IT community staff
4. Outside Source e.g. other member of staff, student etc

It is preferable that all reporting should be via the Helpdesk as the first point of contact. Note: only the Helpdesk or other IT Services staff may formally raise an Incident.

Audiences
The target audiences for communication include:

- IT Services staff
- Distributed IT support community
- Other staff
- Students
- Postgraduates
- Visitors
- General public
- Press

Channels for communication
The possible channels for communication currently include:

- Service Alerts
- Websites (Spotlight, Landing pages, news or equivalent)
- Supportworks
- Moodle
- RSS
• Telephone
• Telephone answering machine message
• University Voicemail broadcast
• Message of the day on Library CSCE Machines
• SMS text messaging
• Corporate communications (in the event that the press request information)
• Screen saver on Library CSCE machines
• Written publications e.g. University newsletter, mail shots etc

**Message content**
The language used in any communiqué should be appropriate for the target audience(s) and wherever possible in plain English i.e. no jargon, acronyms or cryptic references to network topology. The messages given need to be consistent, clear and concise.

**Current situation**

**Methodology**
The current methods used for communication are:-

1. **Service alerts system** ([http://alerts.gla.ac.uk](http://alerts.gla.ac.uk)) – Directed at Technical IT staff. This is inputted by IT Services operators at the behest of an Incident or Change Co-ordinator. There is also an e-mail list which sends a copy of all alerts to a number of IT Services staff and an RSS feed.

2. **Spotlight** – [http://www.gla.ac.uk/it/helpdesk](http://www.gla.ac.uk/it/helpdesk). Web information system directed at the main body of IT users. Various links exist elsewhere on the site that link to this page. E.g. [www.gla.ac.uk/it](http://www.gla.ac.uk/it) /for staff, as well as on the main student computing page.

3. **Email** - Some departments and teams will email their users to make them aware of upcoming changes or current problems with a particular service. This is usually, but not always, done in conjunction with the Service alerts and/or the Spotlight.

4. **News Content** – in some cases e.g. holiday arrangements, the news section of IT Services website ([http://www.gla.ac.uk/it](http://www.gla.ac.uk/it)) is used to communicate to users. The news section is mirrored in various locations throughout the site in an attempt to target the widest possible audience.

**Current practice**
At the moment alerts are raised as and when required. The subsequent actions e.g. Service alerts, mailing user groups etc, are picked up (or not) by IT staff on a fairly informal basis and rely solely on the practitioners rather than on a process. The language used is often terse and written for a specialist technical audience. (see appendix 1) In the case of emailing users it is not always possible to tell which users are receiving the message or if there are other affected groups who are not on the email list.
There are no systematic processes for informing end users of service outages or planned changes. Lack of information leads to user confusion and negative perceptions of IT Services even when a great deal of work is actually taking place.

Proposal

There are a large number of possible incidents ranging from relatively minor to catastrophic system failures. It is not possible to document procedures for each possible incident but the following is an attempt to create a procedural template which could be used and adapted for each eventuality.

A possible template for incidents

Unplanned incidents

When an unplanned incident occurs the Incident Manager (IM) or the person discovering the Incident should contact the IT Help Desk with the following information:

- What is the problem? (or the symptoms if problem is as yet unidentified)
- What is affected?
- Where is affected?
- Who is affected?

The Helpdesk as part of their incident procedures will inform the Information Officer of these details at the earliest opportunity. The Information Officer (IO) will raise an alert using the appropriate language for the various channels.
The IO may seek clarification from the Incident co-ordinator and communications should then proceed as per figure 1.

![Figure 1]

The IO should also consult with the helpdesk to determine the level of calls being received in relation to the incident. If the level of calls is very high the helpdesk manager may decide to stop logging calls but a record should be kept to monitor the levels of calls.

There may also be incidents where the problem is resolved very quickly. In this event the IO should be informed to determine in conjunction with the Help Desk whether any user group requires reassurance.

Any changes/developments throughout the course of the incident should be routed through the IO for further action on communication channels.

Any requests for information or updates during the incident, including management requests, should be made to the Information Officer who will liaise with the Incident co-ordinator to make an appropriate response. (Figure 1)

This process has the advantage of allowing the Incident co-ordinator and incident teams to work uninterrupted on the resolution of the incident as well as protecting and enhancing ITS’ reputation due to the fast response and correct and frequent information being circulated. (See figure 2)
**Planned incidents**
A planned incident (i.e. a change) should follow the same general process as an unplanned incident, with the obvious exception that it would be the Change Co-ordinator who would be responsible for informing the Help Desk. This should be done as far in advance as possible.

**Closing an incident**
An **unplanned** incident would be deemed to be closed when all of the following are met:-

- The Incident Co-ordinator has declared a fix is in place.
- The helpdesk are receiving no calls relating to the incident after the fix is declared. (Subsequent calls relating to the incident should be double checked as they may have originated from before implementation of the fix).
- Affected users agree the incident is resolved.

A **planned** incident would be closed when the planned change has been successfully carried out and tested.

**Reviewing an incident**
After an incident is closed a review of the communications procedures and events should take place using the following criteria:-

- Was every appropriate party informed in a timely and accurate manner?
- What lessons have been learned from this experience?

**Areas for development**

**Documentation**
Records or logs should be kept of incidents and changes and a system of keeping these records developed. A contacts list for both internal and external contacts should be created and maintained.

**Publicity**
Several of ITS’ channels of communication are web based. If the affected members of staff are unaware of
these web pages then they are of little use informing users during an incident. Best practice would indicate that the Helpdesk should be the single point of contact for users to approach IT Services and users should be made aware of this.

End users are becoming increasingly intolerant of downtime and tend to expect 24/7 ‘always on’ services. In any IT Infrastructure and certainly in one as complex as the Glasgow campus (which includes multiple remote sites), then some level of incidents is inevitable. Education of the end user of this fact should be a goal of any communication strategy.

**Proposed roles and responsibilities**

It is the responsibility of the:

- **Incident ‘discoverer’** to inform the helpdesk.

- **Helpdesk** to inform the Information Officer and any other appropriate staff.

- **Information Officer** to:
  
  - publish information about the change or incident using available communication channels in the appropriate language.
  
  - to solicit information from the appropriate expert (s) should that prove necessary.
  
  - ensure communications are taking place.
  
  - review the incident in conjunction with the ITS Director of user services.

- **Incident or change manager** to update the information officer of changes in the situation that may affect end users.

**Staff cover**

In the event of the Information Officer being unavailable 2nd and 3rd line deputies should be appointed. The deputies should be familiar with all procedures and practices relating to incident communications as well as have some skill in using the appropriate language to the target audience.

It is also essential to create and maintain contact lists of

- **Key IT Services staff and functions**
- **Distributed IT Managers**

**Communication channels**

---

1 IT Infrastructure Library Service Support
The communication channels ITS use at the moment are either web or email based. In the unlikely event of a failure of both of these services we would be unable to communicate information about the incident. It is advisable to develop as a minimum a telephone network and/or a voluntarily subscribed-to SMS text service to communicate with the Distributed IT Community in particular. A further development would be the installation of a static web server in the disaster recovery suit serving up one web page at www.gla.ac.uk which we could use to communicate with staff, students and the rest of the world. There appears to be no email ‘alerts’ list to the distributed IT community and the creation of a voluntarily subscribed-to list should be a priority.

Conclusions

There is a need to improve our current processes to:

1. Maintain and improve IT Services’ reputation- good incident response would reduce any negative reactions and focus on quick reaction time.

2. Assist in business continuity by keeping our users informed.

3. Allow Internal ITS staff to be more effective through better use of their time -The teams would not be spending time answering users requests for information or assistance. The Information Officer would be the single point of contact for external and internal communications and so we would, in effect, be creating a buffer between the ITS staff and the user community.

Our current methods are not as widely known as would be desirable. This is an obvious problem and some thought needs to be given to the channels we actually want to use as and some efforts made to publicise and utilise these.

There are clear areas that require development and a plan should be created and acted upon to implement these.
References

Contingency Planning Guide for IT Systems - National Institute of Standards and Technology (US Department of Commerce) June 2002

IT Infrastructure Library (ITIL) - IT Service Management Forum 2007

Good Practice Guidelines - Business Continuity Institute 2007

Communicating in a crisis - Communications for Management inc. 1996
**Appendix 1**

**Diary of an unplanned incident**

This is an example based on an actual incident. Notice the difference between the technical language and the ‘broadcast’ language.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:50</td>
<td>Unidentified Network Service Issue</td>
</tr>
<tr>
<td>09:54</td>
<td>Service alert issued</td>
</tr>
<tr>
<td>09:55</td>
<td>Spotlight posted</td>
</tr>
<tr>
<td>10:06</td>
<td>Update from Incident co-ordinator</td>
</tr>
<tr>
<td>10:07</td>
<td>IO Called helpdesk</td>
</tr>
<tr>
<td>10:15</td>
<td>Service alert updated</td>
</tr>
<tr>
<td>10:18</td>
<td>Spotlight updated</td>
</tr>
<tr>
<td>10:28</td>
<td>IC Informs IO incident resolved</td>
</tr>
<tr>
<td>10:30</td>
<td>Service alert updated</td>
</tr>
<tr>
<td>10:30</td>
<td>Spotlight updated</td>
</tr>
<tr>
<td>Time</td>
<td>Event Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>11:15</td>
<td>Called helpdesk</td>
</tr>
<tr>
<td></td>
<td>Zero calls relating to the incident since fix implementtion</td>
</tr>
<tr>
<td>11:25</td>
<td>Service alert archived</td>
</tr>
<tr>
<td>11:30</td>
<td>Spotlight removed</td>
</tr>
<tr>
<td>11:31</td>
<td>Incident closed</td>
</tr>
</tbody>
</table>
Appendix 2

1. end users

**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.

---

**I think I have discovered an Incident**

Check the SPOTLIGHT section of http://www.gla.ac.uk/helpdesk

---

**There is nothing about the incident on that page**

**It's a known Incident**

I have more information about the incident

Keep checking SPOTLIGHT for updates

---

**Inform the Helpdesk**

- What is the problem? (or the symptoms if problem is unidentified)
- What is affected?
- Where is affected?
- Who is affected?

0141 330 4800
helpdesk@it.gla.ac.uk
www.gla.ac.uk/it/helpdesk/
2. ITS staff

**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.

I have discovered an Incident

Inform the Helpdesk

- What is the problem? (or the symptoms if problem is unidentified)
- What is affected?
- Where is affected?
- Who is affected? **If known**

0141 330 4800
helpdesk@it.gla.ac.uk
www.gla.ac.uk/helpdesk/its

Investigate/repair/fix Incident

Update as available

**Information officer**
1. 0141 330 8532
2. 014 330 8796
3. 0141330 8099
4. 07971676904
its@it.gla.ac.uk
3. Information Officer

**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.

![Diagram of incident handling process]

- **Helpdesk**
- **Other source**

- I have been informed of an Incident
  - • Start log
  - • Raise Spotlight?
  - • Issue service alert?
  - Other channels?

- **Service Alert**
  - Contact Net ops
  - Network@it.gla.ac.uk
  - Telephone: (+44) 141 330 4843
  - Fax: (+44) 141 330 4850

- **SPOTLIGHT**
  - [www.gla.ac.uk/it/helpdesk](http://www.gla.ac.uk/it/helpdesk)

- Require more information/been updated/incident closed?
  - • Update spotlight and service alert
  - • Update log

- COMMUNICATE with helpdesk and Incident manager/team(s)

**Review Incident**
Where people appropriately informed?
What could we do better?