Applied Health Sciences Computing
Services Contingency Plan

Terry Stewart
Director of Information Technology
Applied Health Sciences

Version 1.1, February 2015

Contents

INTRODUCTION

It is the objective of Applied Health Sciences (AHS) Computing to mitigate the risk of system and service unavailability by focusing on efficient and effective recovery solutions. AHS Computing implements this policy in order to ensure that confidential and sensitive systems and information is adequately protected during a contingency event, and to ensure that the AHS community has its confidential and sensitive systems and information available when it is needed.

It should be noted that this document is not meant to replace the official University Emergency Policy, the University's Emergency Plan or IST's Disaster Recovery Plan but rather to supplement by focusing on services provided to stakeholders in AHS.

POLICY STATEMENT

It is the policy of AHS Computing to establish and implement (as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain confidential and/or sensitive electronic information. This document addresses:

- Risk-based scenarios that are likely to impact the provision of services to AHS stakeholders
- Outlining key processes in place and their critical operations
- Defining critical operational periods
- Documenting critical IT systems, applications, databases and network infrastructure monitoring
- Delineating critical data and the availability, integrity and completeness of backups and recovery times required
- Prescribing acceptable downtimes and data loss that would allow for minimal impact on the Faculty based on criticality

FRAMEWORK

This document addresses all services provided by AHS Computing and its service partner, Information Systems and Technology (IST). Services are broken down into 4 business impact categories: mission critical, vital, important and minor. Events can be categorized by the scope of the clients affected: campus-wide, Faculty/Department and user.

Business Impact Categories

Mission critical services are those that have the greatest impact on the Faculty and its constituents. These encompass both education and business-critical functions. Examples of

mission critical services include services such as the Learning Management System and file servers.

The mission-critical category also includes some underpinning services upon which many of UW's services are built. For example, the Identity Management System (IDM) provides authentication for almost all other services on campus. And even it is built on network services. These core services are often not understood and appreciated by clients or even management – at least as long as they are working.

Vital services are services that have a high impact on the Faculty and its constituents but are not necessarily mission critical. Examples of vital services include e-mail and administrative systems like Quest. It should be noted that at certain times of the year, services such as Quest may be deemed to be mission critical (e.g., at registration time).

Value-added services are those that have been developed to deal with smaller, recurring issues or minor business functions within the University. They probably won't not be missed in the near-term and can be shelved if other higher category services are down. They will, however, need to be recovered over the longer-term.

Client Impact Categories

Campus-wide impacts are those events that affect all users on campus. In this case, the event affects all of campus and possibly beyond. Examples of campus-wide impacts are e-mail shutdown, loss of connectivity to off-campus sites and login issues with the learning management system.

Group impact are those that only affect one Faculty, Department or Research Area (e.g. Propel Centre for Population Health Impact.) In this case, other units on campus are unaffected and only the unit in question is without service. An example of this might be a file server or network printer used by a research group.

Individual impact are events that affect one person. In this case, the service disruption is related to an individual's account or computer.

Client Service Response Priorities

Using the categories above enables one to set priorities for client service response.

Client Service Response Matrix

	Individual	Group	Campus
Value-added services	1	2	3
Vital services	2	4	4
Mission Critical	3	4	5

The Client Service Heat Map yields 5 levels of response from the highest: mission-critical service with campus wide impact to a Minor service affecting only an individual.

Service Provider Categories

IT Services are provided in AHS by two groups:

1. **AHS Computing**; these are services that AHS Computing provides to its faculty, staff, researchers and students. Examples of this would be networked printers, student labs, and research support.
2. **AHS/IST Service Partnership**; these are core services that responsibility is shared between AHS and IST. Generally, the core service is provided by IST and the end-user support is provided by AHS Computing. Examples of this are Learn, Connect, WCMS, etc.

ROLES

AHS Computing is comprised of 1 IT Director, 3 IT Specialists and 1 IST Account Representative. The current contacts for these are kept up-to-date at https://uwaterloo.ca/applied-health-sciences-computing/about/people. Job assignments documented at: https://uwaterloo.ca/applied-health-sciences-computing/about-applied-health-sciences-computing/roles-responsibilities. Detailed roles are found on the internal R: drive at: R:\ AHS Computing\Position Descriptions\AHS Computing Committee Assignments.docx and for the IST Account Representative at: R:\ AHS Computing\OLA-SLA\AHS and IST Account Representative MOU.docx.

EMERGENCY CONTACTS

The Emergency Contact List for AHS Computing is maintained at: R:\ AHS Computing \Emergency Contacts\Emergency-Contacts.docx. For the sake of completeness, it is also included in Appendix A of this document.

SERVICES

The list of services provided to stakeholders in AHS is documented online at: https://uwaterloo.ca/applied-health-sciences-computing/services. Each service has: a description of the service, who the service is for, minimum notice required for service, average time to complete, cost and a contact.

SERVICE CONTINGENCY PLANS BY PRIORITIES

Using the five categories in the Client Service Response Categories above, this document outlines the contingency plan by category. Since the plan is expected to be similar for each category, an example response plan will be presented as a guide.

Category 5 – Mission-critical Service for Campus

Category 5 services are those that are mission critical and campus-wide. Examples of this are Exchange e-mail, network connectivity, Learning Management system, student printer accounting, etc. Since AHS Computing does not provide any mission critical, campus wide services, AHS Computing relies on IST to resolve the incident. Service Level Expectations are described at: https://uwaterloo.ca/information-systems-technology/about/organizational-structure/technology-integrated-services-tis/technology-integrated-services-core-service-level

As an example, let us consider the case of a shutdown of the Learning Management System (LMS). Our current LMS provider is Desire2Learn in Kitchener. When this is shutdown, the following procedure should be followed:

1. Report the shutdown to the contact in the Service Catalogue (hereafter referred to as the Contact); this should be done by referring to the contact in the Service Catalogue. (In this case, the Contact is lmshelp@uwaterloo.ca.)
2. Report the shutdown to the IT Director by phone, in person, e-mail or text. (In this case, Terry Stewart)
3. The IT Director will send an RT to the Request Tracking System.
4. The IT Director will send out an e-mail to ahs-all and ahs-grads informing them of the incident.
5. The IT Director in IST (in this case Andrea Chappell) will decide how to inform the UW community, most likely on the UW home page.
6. The IT Director will stay in contact with the IT Director in IST until the service is restored.
7. When the service is restored, the IT Director will inform the AHS community by sending an e-mail to ahs-all and ahs-grads.
8. A follow-up report from the IT Director in IST will be examined by the AHS IT Director and any changes to the service or the service response that will improve either will be implemented.

Exception

There is one particular exception to the above procedure. That is network connectivity. Almost all services rely on network connectivity. Communication surrounding the procedure is also affected. In this case, AHS Computing support staff should refer to the printed version of this document and the services catalogue that is stored in the IT Director's office. All communication above should be done either in person or by phone. The Chair or Director of each of the org units in the Faculty should be contacted by phone or in-person by IT Director to inform them of the loss of connectivity and to request that they arrange to contact their constituents.

Category 4 – Mission-critical Service for an AHS Group

This section describes the procedure for a sample mission critical service for an AHS group. Since most mission-critical services are provided centrally, except for research areas, this section will deal with an example from the Ideas for Health Group. Specifically it addresses InterRAIserv, which is the main analytical server for the InterRAI research group in AHS and headed by Dr. John Hirdes.

The server is set up as a Microsoft Server 2008 R2 Hyper-V host server and hosts 2 virtual machines that the group depends on daily. The first is a webserver*; InterRAIweb* and the second is Remote Desktop statistical analysis server; *InterRAIdata.* Both virtual machines are backed up weekly by AHS Computing using VEEAM. In addition, *InterRAIdata* is backed up nightly by IST's backup service Hoover.

In the event that InterRAIserv went down and was unrecoverable, AHS Computing would be able restore the VM's by doing the following:

1. Create new VM's on another host server. This server could be an AHS host server or, if that option is not available, IST's VM service could be utilized. In this case, *ahs-vmhost* is selected.
2. Restore VEEAM backups for each of the two InterRAI VM's to these newly created VM's.
3. In the case of *InterRAIdata*, restore the latest data backup from Hoover to the newly restored VM.
4. Test each of the restored VM's to ensure they are working correctly.

The estimated time for restoration of both VM's would be 1 -2 days.

Category 4 – Vital Service for Campus

There are a limited number of vital services for campus that are hosted in AHS. The WSUS server is one of those. This example shows the restoration of the WSUS server in the event of a service interruption. *ahswsus-v* is a VM hosted on *ahsvm-host*. It is backed up using VEEAM on ahscoserv (located in BMH 2302C).

1. Create new VM's on another host server. This server could be an AHS host server or, if that option is not available, IST's VM service could be utilized. In this case, ahscoserv is selected.
2. Restore VEEAM backups for *ahswsus-v* to ahscoserv. Instructions for restoring a VEEAM backup are described in the shared R: drive under the Procedures section.
3. Test each of the restored VM to ensure they are working correctly.
4. Forensic analysis of what caused the service interruption would begin.

Category 4 – Vital Service for an AHS Group

Network printing is a vital service to AHS Faculty and Staff that is managed by AHS. AHS "rents" Xerox printers through Retail Services and AHS Computing manages them. They are accessed via print queues set up on the server: *ahscoserv.* In the event that *ahscoserv* is down, the following actions would be undertaken:

1. For any critical printing, the user would be routed to the printer directly via IP printing.
2. A new VM would be created and the VEEAM image of *ahscoserv* would be restored to the new VM as per the section above.
3. Testing and forensic analysis of the cause of the service interruption would begin.

Category 3 – Mission-critical Service for an Individual

There are no services in this category at this time for an individual that don't apply to the campus or an AHS group.

Categories 1-2 – Other Services

Value-added services for individual services will be deal with as time and circumstance permit in the time frames as outlined in the Service Catalogue.

SUMMARY

This document is a framework for restoring services in the event of an interruption. As such, it outlines broadly measures that should be taken when a service is interrupted. It is not intended to be nor should it be a "cookbook" for explicit details on every service and every contingency plan. Doing such would be repetitive. With skilled IT Specialists on staff, it is Management's opinion that there is no need for such a detailed approach.

APPENDIX A

Note: Personal information on this page is intentionally redacted on the online version of this document for privacy reasons.

IT Director

Name: Terry Stewart
Office: BMH 1632
Phone: x35415
Home Address: [redacted]
Home Phone: [redacted]
Cell Phone: 519-950-9512
E-mail: stewart@uwaterloo.ca

IT Specialists

Name: Craig McDonald
Office: BMH 1626
Phone: x6148
Home Address: [redacted]
Home Phone [redacted]
Cell Phone: 519-590-9524
E-mail: cjmcdona@uwaterloo.ca

Name: Lowell Williamson
Office: BMH 1631
Phone: x32326
Home Address: [redacted]
Home Phone [redacted]
Cell Phone: 519-590-9528
E-mail: llwillia@uwaterloo.ca

Name: Brent Clerk
Office: BMH 1627
Phone: x36354
Home Address [redacted]
Home Phone: None
Cell Phone [redacted]
E-mail: bkclerk@uwaterloo.ca

AHS/IST Account Representative

Name: Cassandra Bechard
Office: BMH 1037
Phone: x33010

Home Address [redacted]
Home Phone: [redacted]
Cell Phone: 519-807-8339
E-mail: cbechard@uwaterloo.ca