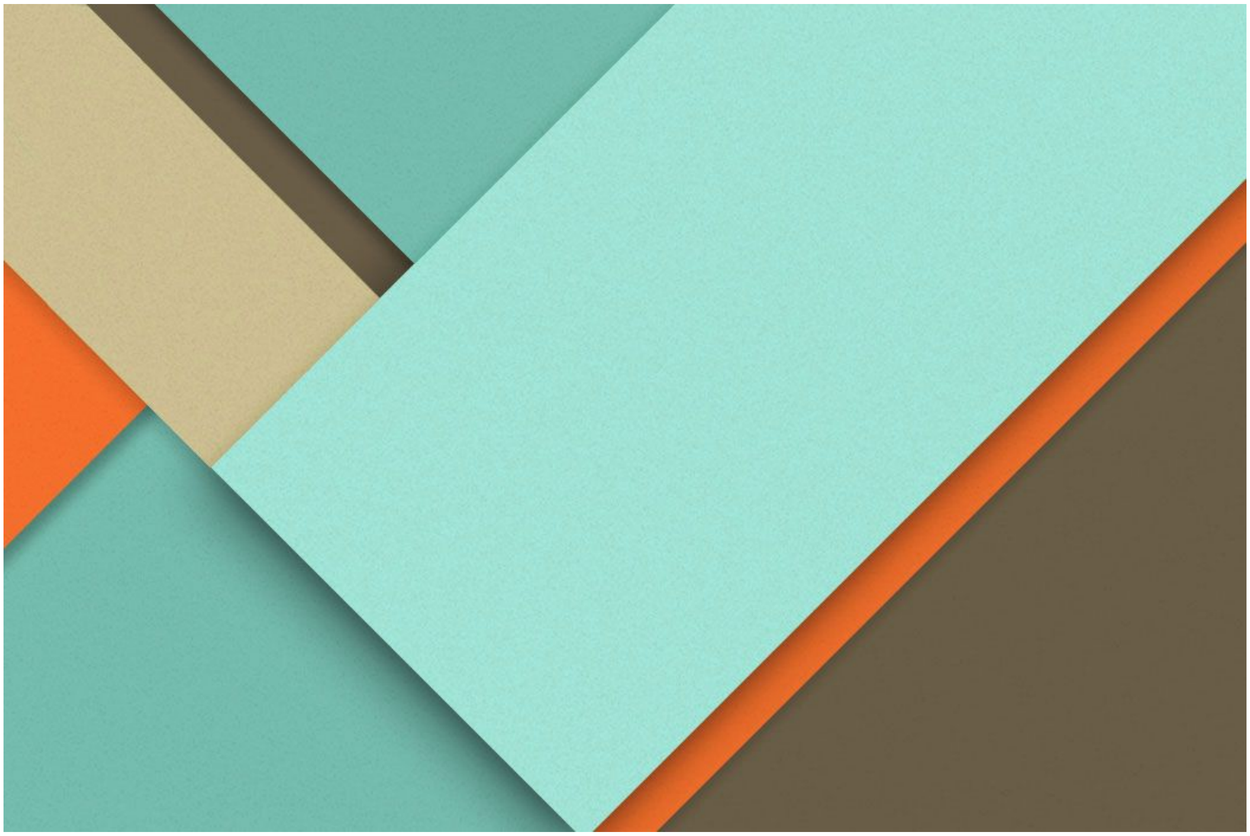

Business Continuity Plan

11.20.2016

Tyler Wilding
Algoma University - Computer Science Department - TAs/RAs
1520 Queen Street East
Sault Ste. Marie, Ontario
Canada P6A 2G4

Table of Contents

Introduction

There are many different types of incidents that can occur in any business setting, some minor and some major. For example, an incident could be as simple as a failing computer or as complex and serious as widespread water damage. This Business Continuity Plan's purpose is to both identify and rectify these incidents as best as possible.

This BCP was developed by Tyler Wilding and specifically targets Algoma University's Computer Science Department's employees including but not limited to Teaching Assistants and Research Assistants. The BCP is comprised of the following sections:

- Risk Assessment
- Business Impact Analysis
- Strategies

In the risk assessment section we examine any and all possible threats from malicious to natural to technical incidents and identify their likelihood of occurring. But the assessment also details the probability of each incident occurring as well as the impact on employees and students.

In the business impact analysis section, we examine all of the critical functions for productivity to continue and describe their allowable downtime and who is responsible for remedying the problem.

Finally, the strategies section attempts to identify ways in which these described incidents can be resolved, however the separate DRP will go into further details.

Risk Assessment

Threats can take on many forms and be malicious, natural or technical disasters. Each threat is examined from the perspective of the impact on the intuition and its employees as well as its clients. The likelihood and the probability of each threat occurring is detailed below as well. While some threats may have a very low chance of happening in the event that they did they could potentially cause very crippling damage and as a result they should be considered regardless.

Threat	Likelihood of Occurrence	Probability of Occurrence	Impact on Institution	Impact on Students
Power outage	Very Likely	High	High	High
Loss of data	Very Likely	Medium	Medium	Medium
Physical Theft	Very Likely	Medium	High	Medium
Data Theft	Very Likely	Low	Medium	Low
Localized Water Damage	Likely	Low	Medium	Medium
Widespread Water Damage	Likely	Low	High	High
Equipment Failure	Very Likely	Medium	Medium	Medium
Active Shooter	Unlikely	Low	High	High
Hostage Situation	Unlikely	Low	High	High
Extreme Weather	Very Likely	Medium	High	High
HVAC Failure	Very Likely	High	Medium	Medium
Workplace Harassment	Very Likely	High	Low	Medium
Aggressive People	Very Likely	Medium	Low	Low

Threat	Likelihood of Occurrence	Probability of Occurrence	Impact on Institution	Impact on Students
Network Failure	Very Likely	High	High	High
Workplace Injury	Likely	Low	Low	Low
Compromised Privileges	Very Likely	High	Medium	Low

Business Impact Analysis

The business impact analysis will be subdivided into two categories:

- Category A - Critical functions that impact the health and safety of all involved parties.
- Category B - Critical functions that do not impact health and safety but impact business continuity and productivity.

Category A

Critical Function	Allowable Downtime	Estimated Recovery Capability	Department Responsible
Power System Functionality	24 hours	N/A	Municipal Services
HVAC System	72 hours	12 hours	Physical Plant
Cleaning Services	1 Week	1 Day	Physical Plant
Door Scanners	12 hours	12 hours	Physical Plant
Security Services	6 hours	6 hours	Security
Seating	24 hours	1 hour	Physical Plant

Category B

Critical Function	Allowable Downtime	Estimated Recovery Capability	Department Responsible
Locked Cabinets	24 hours	6 hours	Computer Science
Computer Systems	48 hours	12 hours	Computer Science
Printer Services	24 hours	12 hours	ITS
Internet Access	48 hours	24 hours	ITS
Server Availability	72 hours	48 hours	ITS / Computer

			Science
Critical Function	**Allowable Downtime**	**Estimated Recovery Capability**	**Department Responsible**
Course Management System	24 hours	12 hours	ITS
Software Availability	48 hours	24 hours	Computer Science
Email Access	24 hours	12 hours	ITS

Strategies

Contact List

ITS Email - ryanandrose@algomau.ca / Danny.Reid@algomau.ca

Security Staff - 705-949-2301, ext.4444

Registrar - registrar@algomau.ca

Computer Science Department Head - Simon.Xu@algomau.ca

PUC Power - 705-759-6555

Shaw Internet - 1-888-472-2222

Bell Internet - 1-866-301-1942

Types of Events to Trigger BCP

Disruptions in Category A incidents will immediately trigger an incident response while Category B incidents will only trigger a BCP response after their allowable downtime. A BCP Response is described for general incidents below, and for a more detailed description of the response, backup, and recovery of said system, the DRP should be consulted.

General Recovery Procedure

When the incident is first discovered it should be reported to the relevant department that holds responsibility over maintaining and recovering said system immediately. The department at this time will need to make the distinction on whether or not the incident warrants a DRP response. An event would warrant a DRP response if the department feels as though it cannot be recovered within the allowable downtime period / the monetary impact is exceedingly larger than usual. The DRP should then be consulted for that particular incident and used as a guide to recover the system, which may include setting up temporary backup systems. Otherwise if the event is not as severe the department should follow standard procedures to get the system recovered in the allowable timeframe and notify all relevant parties periodically on the status of the system. If at any point something changes that would make the timeline change this must be notified to all parties. Once the system is successfully recovered all parties should be notified and an internal review should be conducted in order to identify the cause of the incident. This will reduce the likelihood of the event occurring again, but it will allow preventative measures to be put into place.