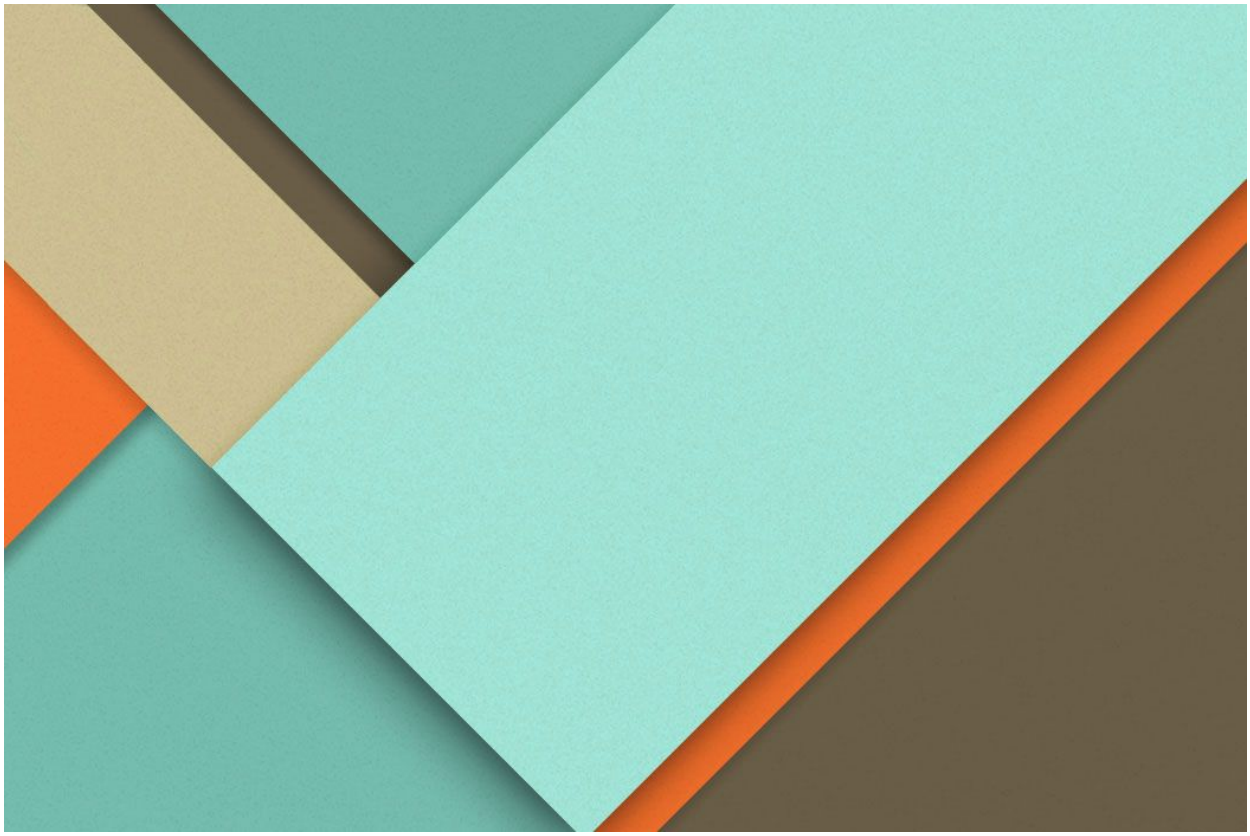

# Disaster Recovery Plan

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

# Water Damage

## Response

The first step is to determine if the water damage is coming from one location or if it is widespread in the room. The purpose of this is to relocate items into a safe and dry area until the damage can be repaired. For items that cannot be easily located such as large pieces of furniture or large computer systems, water proof as best as possible with plastic sheets or containers to catch the water. Dry off any items that were moved but are wet, and begin documenting what items were effected and when the incident occurred. Once the incident has been successfully contained and managed, it is now appropriate to contact Physical Plant to put a stop to the leak continuing.

## Backup

If the water is damaging equipment that is backing up information, then the information should be mirrored on the original device and a new backup should be created in case the water-damaged one fails. If computer systems are damaged and may contain sensitive or critical information than the hard drives should be pulled from these computers and put aside to dry to best ensure recovery.

## Recovery

During the process of documenting which items were damaged, their associated costs should also be documented so in the event that anything was damaged insurance can replace the items. Once the leak has been verified to be solved, it is safe to move equipment back to their original area. Anything that was water damaged and electronic should be tested as soon as it is dry in order to verify if it was damaged or if any data was lost for insurance reasons. If the area is considered a problem area, it may be worth considering relocating items completely away from this previous location.

# Physical or Data Theft

## Response

Once an item has been noticed and verified missing, whether physical or digital it should be reported immediately to the head of the Computer Science department as well as the Security staff. Any security footage available should be reviewed as soon as possible and efforts should be taken to narrow down the timeframe in which the theft could have occurred and by who. It may also be a good idea to contact ITS as they may be able to view the door card reader logs to see who entered and left. If the item that was stolen compromises the integrity of school assignments in any way, the assignments should be changed; the same would be done for any academic related materials. If the owner of the item is known they should be contacted and informed of the theft as well and it is then their responsibility not the Computer Science Department's.

## Backup

Any digital data should be stored and backed up on some sort of encrypted media in case this occurs. The same cannot be said for physical items, however if the item stolen was something more simplistic like a computer monitor than if possible a new one should be temporarily brought out to take its place until the original is found or is replaced.

## Recovery

After going through all necessary means, the item may be recovered or not. In the event that the item is not recovered or it is recovered in a damaged condition then a new replacement must be ordered. If the item was digital than this is not an option. Future digital items should be stored in a safer manner on encrypted storage and any compromised uses for the data should be modified to limit the impact of the theft.

# Power Outage

## Response

The first step is to determine the it is intermediate power issues, or if it will be one sustained power outage.  In it is intermediate power issues, unplug any sensitive devices such as servers from their outlets to minimize potential damage.  If it is one sustained blackout than the building will be closed and essentially evacuated.  In this case, ensure that nothing is left in the room as it will be inaccessible once you leave, take all possessions and leave the room.  If there are any possessions in the room that do not have their owner present, do not lock them up for safe keeping as this will absorb the responsibility onto the Computer Science Department.

## Backup

Any sensitive devices should be ran through an uninterruptable power supply and this will negate any harmful effects and data loss caused by the power outage.  On devices that do not have the luxury of an UPS make sure you save often to prevent any data loss or corruption.

## Recovery

Test all devices after power is restored to ensure that they have not been damaged, report any devices that are damaged to the head of Computer Science.  Recommend the purchase of UPSes for any devices that could have caused a large impact if they failed due to the power outage.

# Network Related Issues

## Response

The first thing to do is to diagnose the problem and identify if it is a physical connection problem or if it is a logical networking configuration problem. To see if it is a physical connection several troubleshooting steps can be performed such as trying new cables, trying plugging the same device into another computer, the same port into another computer likewise. Through deduction it can be determined what is the source of the error and then a more concise ticket can be created for ITS to solve the problem. If it is a logical configuration problem such as un-opened ports, verify that this is the case by trying to access the same services on other computers. You can also run port scans to verify the ports have not been opened, and ensure that the servers are listening on said ports. This information can and will be useful to ITS during the ticket process.

## Backup

If network availability is absolutely required, attempt to find some sort of temporary fix. This could include running a cable from another port to this computer, or accessing the network resource from another network entirely to bypass the firewall restrictions. Some of the information acquired during this troubleshooting can be backed up and documented so the next time the problem occurs it can be solved more quickly.

## Recovery

Once network access appears to be restored, verify that it truly was a fix but also ensure to check that nothing new was taken down in the process of fixing this one issue.

# HVAC Issues

## Response

Heating and cooling requirements are important to be maintained for both health and safety reasons but also productivity reasons. The first step is to confirm suspicions that something is wrong with the heating and cooling systems of the room. To do this, attempt to set the thermostat to one extreme and if the temperature makes no noticeable adjustment than something is most likely wrong. An addition step that can be done is to go into adjacent rooms as often they will be suffering from the same issues. In the event that a problem is identified, contact Physical Plant with a description of the problem and the room numbers you have verified there to be a problem.

## Backup

You should backup the ticket message that you drafted up for this problem, as you may be sending this multiple times in the future.

## Recovery

Once the system is claimed to be restored, verify that it is working correctly by repeating the steps used to identify the problem in the first place.

# Aggressive Students in Lab(s)

## Response

If there are aggressive students in the lab whether it is being physically aggressive or not, they are being a disturbance to the room and it is a serious situation that must be dealt with.  You should begin by trying to remedy the situation while maintaining a calm and pleasant demeanor throughout.  If the situation begins to escalate the student needs to be asked to leave and if necessary Security should be contacted.  Throughout this process notes should be taken of what the student is saying as well as the overall timeline of the situation; these notes may help out later if the student tries to complain.

## Backup

Ensure the notes taken are backed up and kept for into the future, as well as they should be stored in a confidential and private manner and not publically shared.

## Recovery

If the incident was related to course work, then the professor should be contacted of the students behaviour with a transcript of what happened.