

Facilities Management

Business Continuity Plan

*October 2019*

By Harun Biswas

Assistant Vice President, Facilities Management

Essential Business Functions/Operations

Facilities Management

**What Does Continuity of Operations Mean to Us?**

We believe Continuity of Operations is an effort to ensure our University’s Facilities continues its performance of its most essential functions during a range of potential emergencies. To be successful, a COOP plan incorporates the development of plans, procedures, and provisions for people, resources, and processes.

Threat to an organization’s operations can come from many sources, such as:

* Cyber-Security Attacks
* Acts of Nature
* Accidents
* Terrorist Activities
* Technology incidents

Although people are essential, they cannot perform their duties without the right resources. Resources incorporate a wide variety of supporting infrastructure, technology, and other tangible elements required for a comprehensive plan.

Examples:

* Alternate Locations - IT Systems
* Utilities (water, power) - Vehicles
* Communications - Equipment
* Data and records

**Business Function – Facilities Management**

Facilities Management consists of multifaceted departments with a primary responsibility of the University’s asset management, while also playing a major role in supporting the University’s teaching, research, and student life activities through the formulation and implementation of all capital and renovation projects.

Additional responsibilities include: providing overall strategic direction for all major facility projects including master planning, design, constructions, and implementation; and directing the operations of the institute’s buildings, grounds, housekeeping, utilities, operations and maintenance to provide a safe and healthy environment. A total of 55 personnel are employed to carry out the Facilities Management’s mission.

**Priority: High**

**Employee in Charge: Harun Biswas**

**Employees/Position:**

Darren Thomas – Director, Facilities Management

404-520-3490 [dthomas@clayton.edu](mailto:dthomas@clayton.edu)

Charles Bridges – Assistant Director of Building Services

404-825-5187 [charlesbridges@clayton.edu](mailto:charlesbridges@clayton.edu)

Flordeles Brown – Night Shift Supervisor of Building Services

678-427-7228 [flordelesbrown@clayton.edu](mailto:flordelesbrown@clayton.edu)

Wen-Sue Lee – Budget Coordinator

678-466-4243 [wen-suelee@clayton.edu](mailto:wen-suelee@clayton.edu)

**Impact on University if Function Not Performed**

Many of the critical business functions of the University will be adversely impacted if infrastructure operations fall and/or are not maintained.

**CYBER SECURITY:**

Business continuity planning is a crucial part of cyber security, but our Facilities Managementhas a system that accounts for its four phases.

The threat of data breaches looms over all organizations. A significant incident could cause irreparable damage and attract the attention of regulatory authorities. This is why our Facilities Management established the following Business Continuity Plan to mitigate the disruption during Cyber Attack. The following a set of processes that will assist Facilities Management respond to [disruptive incidents](https://www.itgovernance.co.uk/blog/the-5-biggest-information-security-concerns-facing-organisations/), including cyber-attacks and other relevant threats such as power outages and adverse weather (that covered under other section).

BAP (Business Continuity Plan) contain four phases:

1. Initial response
2. Relocation
3. Recovery
4. Restoration
5. **Initial response**

The first thing we do after discovering a disruption is work out the severity of the damage. What systems and locations are inaccessible? Has any sensitive information been compromised?

Our BCP will list the actions that need to be taken in different scenarios, so all we need to do is align the damage with the appropriate response measures.

1. **Relocation OR Plan for the Work Continuity for the Following Items that May Affect Facilities Management**

The next step is to move affected areas of our business out of harm’s way. For example, if our infrastructure is damaged, we need to move equipment into another part of your office. The same is true for employees: if their workspaces are unavailable, we must find somewhere else for them to work.

As with the initial response, our BCP should include specific details based on each scenario. This will probably include things such as setting up temporary offices, or asking employees to share desks or work from home or identified remote locations.

Items to be planed before Cyber Security Breach:

* 1. Access to Work Order System:

Employees asked to work from home will be able to use remote/home WiFi or internet connection to access our Work Order System.

* 1. Archive or save completed work order in Separate File and System:

Completed work orders physical files are saved in the Facilities Management office and warehouse. These files are accessible to employees, as well as remote access to the work order system that contains all requests made through that system.

* 1. List of Phone Numbers

Main Campus On-Call Phone – (470)230-7708

Mohammed Khan – (404)353-8125

Darren Thomas – (404)520-3490

Harun Biswas – (470)848-3146

Public Safety – (678)466-4240

* 1. Additional Phone Access

There are additional employees that have access to and possession of University cell phones, which can be used for communications in the midst of a cyber-attack.

Priti Bhatia – (678)435-7539

Charles Bridges – (404)825-5187

Trent Johnston – (678)435-4910

* 1. Laptops

Several employees have access to University laptops, which can be used remotely to help in accessing work orders and emails.

Employees with access to laptops include:

Darren Thomas

Wen-Sue Lee

1. **Recovery**

With the affected area of our organization isolated, it’s time to fix the problem. We can deal with some disruptions ourselves, but there are times when we might need to bring in experts for the access of data or operation during cyber security breach.

During the event of a cyber-security breach, Facilities Management would rely heavily on the HUB for safe data access. The HUB would be asked to ensure that email access through the SWAN is safe. They would also be asked for tips to keep our remote workers and equipment safe from interruption.

1. **Restoration**

Once the recovery process is complete, our organisation can return to business as usual. Our first need, to confirm that the recovery was successful, which can be done by performing a test. If that goes well, we can move everything and everyone back onto the premises and resume work.

Once IT gives the clear for us to resume business as usual, final testing will occur. Testing that our work order system is intact and operational on both our end and the user’s. After testing, notifying the end users of the restoration and offering tips on how to avoid cyber-attacks will be sent via email.

**Concept of Contingency Operations:**

The purpose of the concept of Contingency Operations Plan is to protect lives and property. Whenever an emergency affecting the campus reaches proportions that cannot be handled by routine measures, the President, or designee, may declare a state of emergency and these contingency guidelines will be implemented. This plan identifies policies, procedures, organizational relationships, and lines of responsibility and communication necessary to minimize the loss of life and destruction of property. This plan is to offer an effective, rapid, and orderly recovery from an emergency.

Facilities Management is responsible for returning the campus to its pre-disaster condition. That activity will involve all members of the staff from housekeeping, to landscape management, to repair of facilities, bother temporary and permanent, to demolition, reconstruction of buildings, and utilities and other structures.

Also, Physical Plant personnel are responsible for the following:

1. Inventory necessary items and equipment (fuel reserve, chainsaws, batteries, flashlights, plywood, caution and masking tapes, etc.) and secure logistical requirements to include emergency generators, fuel, water, etc.
2. Testing of items such as generators.
3. Shutter or board up windows where possible (otherwise tape).
4. Request volunteers for “Watch Teams.”
5. Secure power to emergency operations center (if necessary).
6. Secure all HVAC chiller plants and mechanical equipment.
7. Secure flammable storage lockers.
8. Secure mattresses, blankets, and pillows from storage, alone with food provisions and eating utensils.
9. Cluster all University vehicles adjacent to Physical Plant Maintenance building.
10. Health services will be placed on alert so that they may inventory medical supplies and personnel and formulate plans for alternate emergency care site.
11. Academic, Administrative, Information Technology and College Affairs will be notified.
12. The emergency storerooms located at ABL Food Services, custodial housekeeping and each trade shop will be inventoried to ensure that necessary emergency items are available.

**Maintenance Operations**

After 5:00 PM and weekends – Contact campus Public Safety (678)466-4050. Skilled workers are available from the Physical Plant at all times during normal business hours and on short notice at other times. They are capable of providing the following minor emergency services:

* Utilities – Repairs to water, gas, electric, mechanical equipment, and sewage systems
* Equipment – Portable pumps, generator, lighting, air compressors, tractors, and other miscellaneous equipment.

**External Resources**

Critical Function: Electric

Name/Contact: Georgia Power

1-888-850-4551 BIN#78401 (this will be asked for)

Critical Function: Water

Name/Contact: Clayton County Water Authority

770-960-5200

Critical Function: Gas

Name/Contact: Gas-South

770-907-4231

Critical Function: Sewer

Name/Contact: Clayton County Water Authority

770-961-2130

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Critical Equipment**  **Needs/Supplies** | **Availability** | **Replacement Cost** | **Vendor** | **Quantity Needed** | **Related Business Function** |
| Emergency Generator | 1 | 500 | Home Depot | 3 | Temporary Power |
| Water Pump | 1 | 350 | Home Depot | 1 | Pumping water during flood |
| Battery Powered Flood Light | 2 | 1900 | Grainger | 3 | Provides needed light with no electricity |
| Chainsaw | 1 | 500 | STHIL | 2 | Clearing trees/limbs |
| WetVac | 2 | 300 | People’s Janitorial | 2 | Mitigating flood water |

**Conclusion**

To continue in our operation during an emergency we have discussed the following questions for corrective measures and posed ourselves to mitigate/address the problem if we ever face any catastrophe.

1. Do we know all of the threats to our organization?
2. Do we understand the impact to our organization in a disaster?
3. Will we have alternate facilities from which to operate?
4. Will we be able to effectively communicate with our people?
5. Have we documented all of our critical processes?
6. Do my people know where to report?
7. Do we know who will do what and when in an emergency?
8. Will we have access to all our vital records and data files?
9. Do we have a Business Continuity Plan?
10. Have we learned from the past and corrected ourselves to tackle the future emergencies of such?