FM

FOOD MOOD

FoodMood
Business Continuity Plan
GCU 2023

By Jesse Enriquez

Table of contents

Executive Overview

Please Read Carefully

This document lists the process that must be followed to maintain critical business operations. This is required to be read fully in order to enable full maintenance continuity for business even after the disruption.

***Critical* business operations have come to a halt for one of the following reasons:**

- Loss of access to parts or the entire facility (Fire, Flood, Strom, Etc.)
- Severe reduction of the workforce for outside reasons (Flue, Pandemic, sickness)
- Loss of service due to equipment failures or blockages (IT failures, systems failures, electrical grid failures, Hackers)

Evaluate Severity

This document serves as a template that must be followed to ensure that our company, Food Mood, can return to operations even after this disruption. Everything mentioned below must be considered. This document is meant to be navigated in the event of an emergency and must be treated as so. In the event that there is a disaster that is beyond the company's capabilities and requires immediate outside assistance, please contact local emergency services and refer to the company organizational chart to contact the correct help. If this is a matter of keeping the company active due to a malleable disruption please continue, and follow along.

Document Change Control

Date	Change/Review	Sig.

1. Introduction

Overview

The Business Continuity Team ensures that the plan in place ensures that the business will be in a functional state where the organization is performing its crucial business functions. These functions follow the company's mission statement *Come Consume With US, Let The Food Do The Talking*, and ensure our users are able to partake in the sharing portion of our application. The team also ensures that we comply with all legal requirements and support all safety regulations and local laws everywhere we have an impact. This includes if a disaster happens technologically or naturally within company grounds. All events that may result in company service being halted are included. The BCT is in charge of planning and preparing for an incident, and also ensuring critical business functions are not only running but improving as well.

Company Plan of Action

This Plan of Action Covers Food Mood. This plan is opposed when the life or safety of employees, users, or guests has been potentially compromised. In the event that our immediate facility has been or will be beyond our reach, this plan must be activatable during and post after hours without warning.

Plan of Action Objectives

The Food Mood Business Continuity Plan Objective is to coordinate the operations, functions, and technology of the company and ensure they are resuming at and in a timely and organized manner. This is to ensure the company is able to remain stable and viable. While ensuring this, it is crucial that the user base, guest, and employees' safety is considered first.

Primary Objectives:

- **Maintain Critical Business functions** (Most critical departments/business operations)
- **Ensure employees are able to access the site facility** (Ensure employees have a safe zone/area)
- **Protect Vital Documents** (They are accessible at all times)

Plan Assumptions

The listed assumptions were used while creating this list.

- Event occurs that affects operation hours
- Limited or no access to a company facility
- Documents or equipment are inaccessible
- Qualified personnel is not available to continue business operations

2. Risk Assessment

Part One: Risk Assessment

This Risk assessment involved an intense can that was run on all parts of our network that assist in the company's traffic and success. This scan was able to identify and give a synopsis of areas and their risk levels. Here at FoodMood, our customer's and employees' information is very valuable to us and these intense scans frequent our network and enable us to always be working on improving the overall security of the system. The results are reviewed and mentioned below

Two critically labeled systems can possibly impact the organization negatively if these vulnerabilities are found by potential attack vectors. The first critically labeled system is our Authentication application (MoodID). This is the login system and authentication process that passes or fails users as actual humans interacting with our login system or if it's a computer-generated bot trying to virtually enter our system. This system has there areas where a threat event can occur, Loss of confidentiality, loss of integrity, or loss of availability. Given the results of the risk assessment, all their areas came back with a high-risk level and graded the overall system as HIGH risk. The potential impact it can have on the company is graded high because of the potential people that can be affected. Our user base is directly impacted if a negative result occurs due to our negligence in fixing this issue. This can put many at risk of not having their information hidden well enough, not protected enough, and being unable to access it if all fails. This would result in all affected users' information being out for grabs where it can easily be used for other negative impacts that can result in a loss for our community. This would also result in the company losing the established trust of many users and a significant drop in users of our application which then affects companies greatest asset.

Our second system that is marked critical is our application with creator-produced content. This area of our system is intended for all physical content that creators post on our application is stored. When a creator creates and shares something with the world, it is our responsibility to keep it safe and give an area to be stored while being viewed. Once again all real can hack high risk and that is why this system is rated critical. If this system is attacked by an insider threat, users will then begin to question the safety of their public content, creators will then find our applications they feel their information is better kept and respected. This, similar to the above, creates a potential hole in company assets by losing users over time.

When assessing the system, we also discover two high-risk findings but have included mitigation strategies. The first system is our server with PCI Data. This system is responsible for storing user payment information if saved for next time. Being labeled high-risk, puts customer information at risk and can possibly result in company assets loss. How we fix this by updating to the latest encryption system? Our current system is outdated and we intended on transitioning to the latest and safest when it comes to payment information. Our second high-risk area is the IT admin laptop. This is labeled risk for mainly being available for grabs by anyone. This system should never be available for anyone even if protected with passwords and other strategies. If for any reason, this system has to be left behind, it needs to be well hidden or locked which brings us to our mitigation strategy. If the IT admin tends to be busy and has to leave his personal space frequently, we must build or purchase a safe or locked cabinet that the admin can lock his system in when necessary.

Alternate controls are important to consider and should always be the instant band-aid to a system if the permanent change is going to take an extended amount of time to implement. For our first risk mentioned, we should enable a two-factor authentication application immediately, these are easy programs to implement and can easily be attempted instantly. For protecting creator content, we can enable a warning system that will suggest that all users save their information on their devices and even include some steps for having backups of your information. This risk will take an extended amount of time to refresh and this is a temporary fix to a major issue that saves the company short term. PCI data is some of the most important information to protect, the alternative control should be to remove any saved payment data from our system until the next one is established. Lastly, I feel the most alternative control before installing a system with a lock in the office space is a backpack with a small lock, this enables the admin to have the system on them and secure at all times.

Part Two: Contingency Plan

A contingency plan is vital to being able to re-establish a company if a disaster or loss of information occurs. There are four vital areas that we have built our plans around. These are business impact analysis, recovery strategies, plan development, and lastly testing exercises. These four areas cover all compliant areas in the business that are important to protect well enough to not only save the company but protect assets that could possibly be lost in the process of a disaster. In our case, the site has been rendered a disaster and we cannot access the business or assets on site.

A cost/benefit analysis is a process that must be done if a disaster occurs. Fortunately, the margins are clear and the financials are accounted for and paid for during safe times. Being a social media company, we must store our important information occasionally in more than one spot. Our greatest cost with the highest amount of benefit is our off-site storage systems. In a neighboring state, we have servers that save the information that is vital to the company's success if a disaster occurs, we could easily recover and re-establish at another site. This is a major cost for the company but does have its value. When the contingency plan is referred to, we will immediately refer to the offsite servers to ensure all the necessary information has been backed up and the company can stay protected and secured. This is why the emergency offsite servers are the most expensive and the most valuable on our analysis sheet.

An event that frequents the California area in which we are located is wildfires. These fires require all within a certain range of the fire to immediately evacuate as the fire grows. California has had some of the largest fires ever recorded which was followed up by tons of assets destroyed along the way. If this occurs, all physical controls immediately become useless due to the urgency of evacuation. Before vacating the premises, it is important we attempt to lock the space up to the best of our ability and we ensure all valuable assets are not accessible if looters were to gain control of the building. While we must always prioritize safety, it is important that we consider our live assets if possible.

Compensating controls is vital to ensuring the safety of our company and our users. We as a growing and hopeful Fortune 500 company are always looking for improvements on how we can ensure we are modern in our space, industry, and our security controls. With this logic, we are frequently running compliance tests and constantly reestablishing what compliance looks like in our space. This enables us to appear non-compliant with our standards whilst most other companies would be regarded as compliant. With this strategy, we are always building upon getting better and improving our infrastructure. When working with these non-compliant systems, we often start thinking of strategies that allow us to step back into that compliant area. We begin this process by analyzing what exactly makes our system non-compliant. When that information is collected, we then form strategies on how we can fix that weaker area. This begins by establishing an alternate control, this allows our system to be temporalty stronger as we work to fix and patch the issue. When the new system is ready to be installed, we quickly implement it into our network and re-test for compliance to ensure our initial goals have been met. If the system is worse or not up to our expectations, we use our previous system and re-install the old one until we have designed an appropriate system.

Experiencing a breach when having a compliant environment can be an interesting experience. The company and everyone in it are somewhat under the impression that they are very difficult to breach and damage. This is what results in it some of the largest breaches recorded in history. Some of the most damaging breaches have occurred over an extended amount of time and by the time they realize there's a mole in the network, they've already established themselves deep in the system. Having the logic of being indestructible, creates the threat of being hit harder than necessary when an attack does occur. This logic would also create an emerging risk, comfortability. Being cybersecurity professionals, we should never be comfortable with our work, we should always have a mindset of learning and improving if we want to remain compliant and secure. Creating a progressive environment tends to limit the number of threats that can occur and be created in a network.

Part Three: Risk Assessment Table

Table 1 Note: *The following Table reflects the FoodMood Risk levels given the current operational security framework strength as of 2023.*

	Policy	Network	Endpoint/ Protection	Identity	RISK Priority
Identify	4. Highly	4. Highly	4. Highly	4. Highly	☐ High

	Likely 3. Likely 2. Possible 1. Unlikely	Likely 3. Likely 2. Possible 1. Unlikely	Likely 3. Likely 2. Possible 1. Unlikely	Likely 3. Likely 2. Possible 1. Unlikely	☐ Medium ☑ ~~Low~~
Business Environment	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	☐ High ☐ Medium ☑ ~~Low~~
Risk Assessment	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	☐ High ☐ Medium ☑ ~~Low~~
Governance	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	☐ High ☑ ~~Medium~~ ☐ Low
Protect	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	☐ High ☐ Medium ☑ ~~Low~~
Access Control	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	☐ High ☐ Medium ☑ ~~Low~~
Data Security	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	☐ High ☐ Medium ☑ ~~Low~~
Protective Technologies	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	☐ High ☐ Medium ☑ ~~Low~~
Detect	4. Highly Likely 3. Likely 2. Possible	4. Highly Likely 3. Likely 2. Possible	4. Highly Likely 3. Likely 2. Possible	4. Highly Likely 3. Likely 2. Possible	☐ High ☐ Medium ☑ ~~Low~~

	1. Unlikely	1. Unlikely	1. Unlikely	1. Unlikely	
Events/ Anomalies	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High ☑ ~~Medium~~ □ Low
Threat Intelligence	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium ☑ ~~Low~~
Detection Process	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium ☑ ~~Low~~
Respond	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium ☑ ~~Low~~
Response Planning	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium ☑ ~~Low~~
Analysis	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium ☑ ~~Low~~
Mitigations/ Improvements	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium ☑ ~~Low~~
Recover	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium ☑ ~~Low~~
Recover	4. Highly	4. Highly	4. Highly	4. Highly	□ High

Planning	Likely 3. Likely 2. Possible 1. Unlikely	Likely 3. Likely 2. Possible 1. Unlikely	Likely 3. Likely 2. Possible 1. Unlikely	Likely 3. Likely 2. Possible 1. Unlikely	□ Medium ☑ ~~Low~~
Improvements	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium ☑ ~~Low~~
Communications	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium ☑ ~~Low~~

Table 2 Note: *The below table can be completed based on the designee’s assessment of the current situation facing the company that is not included in Table 1. Though the impact and duration of hazards for your business may differ from this table.*

Table 2 FoodMood Mitigation Analysis

	Policy	Network	Endpoint/ Protection	Identity	RISK Priority
Identify	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Business Environment	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Risk Assessment	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Governance	4. Highly	4. Highly	4. Highly	4. Highly	□ High

	Likely 3. Likely 2. Possible 1. Unlikely	Likely 3. Likely 2. Possible 1. Unlikely	Likely 3. Likely 2. Possible 1. Unlikely	Likely 3. Likely 2. Possible 1. Unlikely	□ Medium □ Low
Protect	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Access Control	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Data Security	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Protective Technologies	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Detect	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Events/ Anomalies	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Threat Intelligence	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Detection Process	4. Highly Likely 3. Likely 2. Possible	4. Highly Likely 3. Likely 2. Possible	4. Highly Likely 3. Likely 2. Possible	4. Highly Likely 3. Likely 2. Possible	□ High □ Medium □ Low

	1. Unlikely	1. Unlikely	1. Unlikely	1. Unlikely	
Respond	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Response Planning	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Analysis	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Mitigations/ Improvements	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Recover	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Recover Planning	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Improvements	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low
Communications	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	4. Highly Likely 3. Likely 2. Possible 1. Unlikely	□ High □ Medium □ Low

3. Critical Business Functions

Overview

Food Mood is a social media platform that relies on the sharing of content with others. When content is not being shared, the creators and users are not consuming and creating content, when content watch times are impacted, revenue is impacted. It is important that we prioritize the safety of our employees. Without a staff, we are unable to provide our own mission statement. Without our employees, we are unable to perform critical business functions post-company disaster. It is important to prioritize the safety of our users. Without their trust, we are unable to operate as a company and once again provide what our mission statement is to the number of people we would like to reach.

Function

The ability to upload and view content by our users at all times.

Business Process to Complete

When content is uploaded and shared to Food Mood, users are able to share short videos of them enjoying their favorite dishes as well as their experience at a restaurant with others. This enables local restaurants as well as provides add revenue via restaurants paying to be promoted and minutes being consumed on the application. The more content shared, the larger variety that is created, which results in more content being consumed, which results in a growing user base. This creates a growing company.

Supporting Activities

When content is uploaded, it relies on factors such as sharing and liking to gain popularity. Promoting the share icon and making it easy for the user base to share with others in multiple forms enables growth and once again results in an increase in company funds. Without the initial step of uploading occurring, this growth stops immediately.

Lead Point of Contact (POC) and Alternate

Chief Intelligence Officer: John Smith (123) 456-7890
Chief Risk Officer: Nancy Brown (000) 111-2345

Vendors and External Contact

Chief Legal Officer: Joey Carter (999) 777-2323

The Table below Mentions FoodMoods critical business functions, the table includes the points of contact if an issue

Company Asset	**Use of personal equipment on your company's network (BYOD)**
Issue Statement	By use of your personal equipment, you promise to abide by all safety sanctions and rules mentioned within the company manual provided. All rules must be followed on company property at all times. If failure to do so is proven, you are subject to discipline.
Statement of The Organization's Position	The organization's position on the use of BYOD is for a fair reason. There are many safety risks that can be spawned through the inappropriate use of BOYDs while within the company structure. We do understand that the intentions are not to harm the company while using personal tech, but please do understand that harm can still occur even without your consent through your personal devices.
Applicability	BYOD is occasionally used within our network, primarily for communication. Cell phones are the most applicable and essential for most. There is an overlap of personal use and company communication for almost all Boyds, but we ask that its use remain professional and safe while within the company infrastructure.
Roles and Responsibilities	Pristine communication is key for a high-functioning team, which is why the appropriate use of BOYD is important. The users are responsible for the respectful use of BOYD while maintaining excellent communication through personal devices.
Compliance	Is key because inappropriate use can lead to safety issues. If safety issues are created constantly through the use of BOYD, company regulations of personal devices would be certain to change.
Points of contact	Cybersecurity Department: Director: James Thanos Assistant Director: Jordan Goesin
Max Down Time Allowed	Three Hours/Zero Days
Criticality	☑ ~~High~~ ☐ Medium ☐ Low

Supplementary Information	Every BOYD device brought onto company property must be registered with the security team and given a unique certification that enables the team to know whose device is who.

Company Asset	**Internet Access**
Issue Statement	Internet use is essential to everyday work. By use of this service, you consent to appropriate work-related use only.
Statement of The Organization's Position	Internet use is used every single day when working. Our company revenue is created by the use of the internet, which is why it’s important to maintain respectable use of it when in company infrastructure. There will be restrictions that will not assist in the protection of company infrastructure.
Applicability	The entire company runs through an internet connection and we cannot function on a day-to-day basis without it. A majority of the roles at this company require internet use daily.
Roles and Responsibilities	The role and responsibilities are dense, we use internet access for everything, which includes communication with the team and our users. Every issue involves the internet and can be solved with it mostly as well.
Compliance	is essential within the company infrastructure. We can see all activity on work devices if necessary and inappropriate use of the service can lead to punishment and termination.
Points of contact	IT Department: IT Director: Scott Dickens Assistant Director: Jerry Terrosain
Max Down Time Allowed	5-8 Hours/ Zero Days
Criticality	☑ ~~High~~ ☐ Medium ☐ Low
Supplementary Information	N/A

Company Asset	**Personal use of company equipment**
Issue Statement	When issued a piece of company equipment, you vow to follow all rules that come with said piece of equipment at all times. Failure to do so results in immediate meetings regarding company asset use.
Statement of The Organization's Position	Company equipment is for the use of work responsibilities only. If found doing off-hand tasks or inappropriate activities may result in permanent termination.
Applicability	The use of company equipment is important in everyday activities. The company's main form of equipment would be your assigned company computer in which your daily tasks are all completed. The task cannot be completed without it and must be used daily.
Roles and Responsibilities	Maintain a safe and professional environment when accessing company equipment. Keep company safety in mind when referring to the use of said company device.
Compliance	Safety is our main priority at this company. When in use of these devices, it is essential to consider the safety of company infrastructure. Appropriate use is also necessary because you will have access to sensitive information as well.
Points of contact	IT Department: IT Director: Scott Dockens Assistant Director: Jerry Terrosain
Max Down Time Allowed	Zero Hours/ One -Two Days
Criticality	☑ ~~High~~ □ Medium □ Low
Supplementary Information	Devices are always subject to checking and can always be assessed by other departments if necessary.

Company Asset	**Removal of organizational equipment from your company's property**
Issue Statement	Removal of company equipment is essential when every member leaves the company or gets an upgrade. This process involves the IT team manually overseeing the process.

Statement of The Organization's Position	When a full removal is in process, feel free to remove any content that you would like to do manually before the IT team does it themselves. If this is an upgrade, the IT team will be responsible for all transferring and downloading of any necessary company programs and information the old machine obtained.
Applicability	This process is key when anyone leaves the company, we must ensure that all information is removed before being assigned to a new person. All traces of the last person's responsibilities will be removed prior to the machine being reassigned.
Roles and Responsibilities	The only role that said person with the device is to return it to the IT department's designated area for a full uninstallation process by the established due date. An identical process must follow for upgraded systems as well.
Compliance	Remaining compliant and following the exchange dates is important. This keeps the IT team on schedule and pace and also ensures you will get your upgraded system quickly if applicable.
Points of contact	IT Department: IT Director: Scott Dockens Assistant Director: Jerry Terrosain
Max Down Time Allowed	N/A
Criticality	☐ High ☐ Medium ☑ ~~Low~~
Supplementary Information	If company products with company information are not returned by an established date, They will be considered stolen and a police report will be ensured**.**

Company Asset	**Use of unofficial software**
Issue Statement	The use of unofficial software is a major risk to the company's infrastructure. If any questions or programs need to be assessed that are not official, please refer to the main points of contact to enable their use of them.
Statement of	Unofficial software can severely impact the company infrastructure.

The Organization's Position	Potentially malicious software can introduce security risks that put company information as well as user information at risk. The use of unofficial software that is actively harming the company found on a device can lead to permanent termination.
Applicability	There is no use of unofficial software nursery while on company time. If there is a program that can help or assist the efficiency of the company, get it registered as an official piece of software with the IT department.
Roles and Responsibilities	There are no responsibilities or roles unnecessary software has. If found on a device will lead to instant questioning of intentions.
Compliance	This is a very important rule that must be followed. This can harm the company and potential users if malicious attackers use the software as a key to company infrastructure. If not followed, immediate meetings within intentions with unofficial software will be had.
Points of contact	IT Department: IT Director: Scott Dockens Assistant Director: Jerry Terrosain Cybersecurity Department: Director: James Thanos Assistant Director: Jordan Goesin
Max Down Time Allowed	Zero Hours/Three Days
Criticality	☑ ~~High~~ □ Medium □ Low
Supplementary Information	If there is a new piece of software you feel will improve company efficacy, please contact the current Assistant director of the IT department.

4. Plan Activation Procedures

Operation: FIRE EVACUATION

Scope: All FoodMood Associates

Responsibility: All company Managers, All FoodMood Personnel

Purpose: **Outline fire evacuation plan within FoodMood building**

1. **PURPOSE**
   - This procedure aims to ensure the safety of all FoodMood staff and associates that work within the walls of the company/facility given there is an immediate evacuation due to a fire.

2. **RESPONSIBILITY**
   - The facility manager or facility safety manager will be responsible for establishing the fire evacuation plan. This is available at every facility at its designated spot
   - The staff of FoodMood is also responsible for being familiar with the established Fire Evacuation Plan

3. **PROCEDURE**
   - Every Facility has a fire evacuation map posted in areas such as entry doors and assessable fire extinguishers. The map will include a floor plan with all accessible exit points and other fire extinguishers in the given area. There will be arrows on the map which can be used to help guide people to the nearest and quickest exit route.
   - All staff will be trained and rehearsed where their closest exit is based on their assigned room. Staff will also be made aware of other points during orientation and the initial tour of the facility.
   - In the event of a fire alarm, the safety officer's immediate responsibility is to ensure all staff has safely evacuated company grounds. In the case that a member

refuses to leave, do not attempt to convince them, just note their exact location to inform responding firefighters.

- Ensure announce the rally point which should be located at least 100 feet from the building.
- Ensure every alarm is taken seriously.

Operation: Ransomware Attack

Scope: All FoodMood Associates

Responsibility: All company Managers, All FoodMood Personnel

Purpose: **To outline the procedure when facing a ransomware attack**.

---

1. **PURPOSE**
   - The purpose of this procedure is to establish a plan in case a ransomware attack occurs during operating hours.

2. **RESPONSIBILITY**
   - Chief security officer is responsible for establishing the ransomware attack plan that is posted and accessible in its designated spot.
   - It is the responsibility of the FoodMood staff to follow through with their part of a ransomware attack protocol.

3. **PROCEDURE**
   - Each key member should have the established plan document accessible near them or possibly on their computer if accessible. If not it can be found at the site's established location. This plan should map out what steps need to be taken and what precisely needs to be done.
   - Staff should be trained on exactly what steps need to be taken per their role. This solid be rehearsed and practiced as a team prior to the event.

- In the event of the attack, it is the chief information officer's responsibility to inform the team that a ransomware attack is active and that the staff needs to begin their established duties.
- Regular meetings and updates need to be had, and there must be an established office/ meeting room that employees come to with progress updates.
- The serenity of the attack must be taken seriously, company information is at risk!

Operation: Power Outage

Scope: All FoodMood Associates

Responsibility: All company Managers, All FoodMood Personnel

Purpose: **Outline the event of a power outage within FoodMood**

1. **PURPOSE**
    - The purpose of this procedure is to establish a plan in the event that a power outage occurs within FoodMood facilities.
2. **RESPONSIBILITY**
    - The IT Director is responsible for immediately checking that all systems are legitimately powerless due to a building issue rather than a potential attack on company infrastructure.
    - The director of media user ability Immediately drafts an explanation to staff and potential users who can now not access some capabilities that were once accessible prior to the outage. This should mention the reason is due to a temporary power outage.
3. **PROCEDURE**
    - Team members are directly responsible for making sure there are risks of hazards once power is re-enabled. This includes making sure only essential devices are initially plugged in.

- There will be A list of essential items that should only be plugged in and read out loud by management. If there is a team member missing that is unable to perform their duties, announce it to a nearby team leader.
- In the event of an overnight power outage, please repeat the steps listed above and ensure the devices are left there once you leave the premises.
- Expect regular updates on the status of the power outage via personal mobile device.
- Power Outages must be taken seriously and posted steps must be followed in order to prevent damages during the re-enabling of power.

Operation: Pandemic Situation

Scope: All FoodMood Associates

Responsibility: All company Managers, All FoodMood Personnel

Purpose: Outline the protection of FoodMood faculty's health

1. **PURPOSE**
    - The purpose of this outline is to enable and ensure that all faculty that are present in FoodMood facilities can exit the premises safely in the event that the building must shut down due to a pandemic situation.
2. **RESPONSIBILITY**
    - The facility manager or facility safety manager will be responsible for establishing the Pandemic Situation plan. This is available at every facility at its designated spot
    - The staff of FoodMood is also responsible for being familiar with the established Pandemic Situation plan.
3. **PROCEDURE**
    - Every Facility has a Pandemic situation map, if not found please refer to the fire evacuation map posted in areas such as entry doors and assessable fire extinguishers. The map will include a floor plan with all accessible exit points and

other fire extinguishers in the given area. There will be arrows on the map which can be used to help guide people to the nearest and quickest exit route.

- All staff will be trained and rehearsed where their closest exit is based on their assigned room. Staff will also be made aware of other points during orientation and the initial tour of the facility.
- In the event of a Pandemic situation, the safety officer's immediate responsibility is to ensure all staff has safely evacuated company grounds. In the case that a member refuses to leave, do not attempt to convince them, just not so consequences can be taken later.
- Ensure that everyone exits calmly with the penalty of space between themselves and navigates directly to their means of transportation.
- Pandemic situations should be taken seriously, and the health of employees and their loved ones is at risk.

5. Internal Communications Procedure

Staff Accountability

Once all staff, guests, and customers have safely exited the building, they should meet at the primary assembly point and await further instructions from the appointed leader

Once at the Assembly point, please perform the following steps:

- Initiate a role call and ensure a proper headcount is taken given the staff, guest, and potential that is expected to be present
- Ensure that all accounted people are uninjured or need any sort of assistance, if so, reallocated resources to assist them
- Report said insured or sick to ownership or designee and ensure the proper information is given to first responders

Employee Communication Methods

1	*Staff work email; located in Personal information folder page 3*
2	*Staff work mobile phones, Numbers located in staff personal information folder page 6*
3	*Staff Personal email and mobile phones; located in employee personal information folder page 9*

6. Alternate Facilities

Overview

An alternate facility provides a backup location for a company to safely transfer activities in the event that the main facility becomes unusable due to a loss of access to any part of the facility or the entire facility. the use of replacement Facilities and telework options, when accessible, increases organizational resilience during COOP emergencies.

Alternate Facility Selection

An organization must ensure that, in the event that the primary facility is made worthless for whatever reason, the appropriate and efficient alternative facilities provide the means and competence to execute its stipulated core business responsibilities. Alternative facilities may, without restriction, consider the following elements:

- Suffienicent millage from the original facility
- Availability of critical resources, equipment, and supplies that can assist in the preparation of the business continuity plan within 24 hours of its activation.
- An updated understanding /agreement with the point of contact for facility managers
- Moderate levels of physical and information security

Telenetwrok As An Alternate Site

Telenetworking is the process of establishing a line of communication from the supervisor to the employees, during disaster circumstances, this s usually performed from home networks or another non-traditional assessable location to all. This is not always an option nor should it be an expected resource, but should be utilized when available.

Alternate Site Ranking Table:

#	Site Adress	Distance from Primary Facility	Facility POC	Required Equipment	Parking/ Public Transit AcessabiltY	ADA Compliant
1						
2						
3						
4						

7. Orders Of Succession And Deligation Of Authority

Overview:

Orders of succession are created to define senior leadership responsibilities in the event that the people now holding these positions, whether they are management or decision-making roles, are not accessible. A delegation of authority gives successors the power to carry out certain tasks and represent important positions within an organization.

Orders Of Succession:

These lists of senior leadership positions are written by position rather than by name and are official and sequential lists. In the case that the incumbent is unable to do so, they are meant to demonstrate who is qualified to replace the office. The adverb inaccessible means that the office holder is unable to carry out the duties of the position owing to absence, a handicap, infirmity, or other circumstances. Identifying the orders of succession in advance is crucial for maintaining effective leadership after an occurrence that interferes with business operations.

Dedication Of Authority

The ability to legally act on behalf of important positions within an organization for particular goals and responsibilities is known as a delegation of authority. When a circumstance arises that calls for the activation of a business continuity plan, employees who

serve in important senior leadership roles must establish and uphold pre-delegated authority for policy decisions as necessary. The delegation of authority should include the sort of authority being transferred, such as a signature or credit card authorization for purchases, as well as the transferred authority's restrictions. When the incumbent cannot exercise that authority for any reason, all of the responsibilities of each senior leader are transferred to the position in the orders of succession, including but not limited to:

- **Absence**
- **Illness**
- **Leave**
- **Death**
- **Termination**

Each authority is also revoked upon the incumbent's return. Predelegated powers are essential because they guarantee that important tasks or authority may be completed in the event that the principal position is unable to carry out its assigned responsibilities.

The pre-delegated powers must be maintained by key employees through effective cross-training and succession exercises.

*******The Next page contains the positions of succession if in question***

Positions Of Succession

Chief Executive Officer Jesse Enriquez (111) 222-333 JE@FoodMood.com
Chief Financial Officer Jordan Myers (888) 555-2222 JMEeyer@FoodMood.com
Chief Intelligence Officer John Smith (555) 667-7777 JonnyS@FoodMood.com
Chief Information Security Officer Mary Wolf (444) 323-5677 WolfMary1@FoodMood.com
Chief Operations Officer Tommy Grant (777) 777-6644 Tomthecoo@FoodMood.com

8. Plan Deactivation

Overview

This process must be followed while transitioning from the alternate facility to the primary facility where all critical business functions are resumed. This may be the prior facility or a newly established primary facility if the prior is unable to handle necessary business functions. The goal of the plan deactivation is not to be fully operational with unlimited resources similar to our previous facility but to transition to an area that can now handle our full critical business functions and eventually evolve into what the space once was. If necessary, hire and backfill the necessary staff that is needed to compare the transition and initially re-establish it-infrastructure and vital records. When notified that the COOP activation has closed, all personnel should be notified that they may return to performing normal operations.

Criteria For Plan Deactivation

The Designee will determine based on information received from first responders and local input received if staff and other entities can now return to the restored facility or temporary facility that has now been re-established and when critical business information and functions have been transferred to the newly established zone.

Critical business functions must be restored in a priority sequence that has been pre-established below. The following functions are completed prior to the plan deactivation unless informed otherwise.

- Acquire or purchase supplies and equipment, arrange travel needed for resumption process

- Pause or temporarily suspend functions that are considered non-critical, fully support resumption process and efforts
- If applicable and available, utilize personnel available from other sites to perform resumption efforts

Business Function Resumption/Plan Deactivation

#	Function	Supplies	Required Resources
1	**Use of personal equipment on your company's network (BYOD)**	Personal devices; Cell phones, laptops, tablets, keyboard, Bluetooth devices, etc.	All are personally owned and carried by the person.
2	**Internet Access**	Routing system, multiple cables, a safe area established by IT team	Bandwith availability, secure space, IT team, electricity
3	**Personal use of company equipment**	(PCs, printers, sound devices, etc.)	Access to company supplies/space.
4	**Removal of organizational equipment from your company's property**	All supplies are to be returned if in the necessary situation	Access to employee/company loan policy
5	**Use of unofficial software**	Personal device/equipment or company device /equipment	unsolicited/ downloaded software

9. Employee Contact List

Employee Name	Title/Responsibility	Home/ Cell Number	Personal Email Address

10. Vendor Contact List

Vendor	Resouce/Service	Contact Information

11. Family Emergency Plan

Employee emergency contact list/information?

Name	DoB	Social Security #	Home Cell #	Work #	Home Adress	Emergency Contact
Jeff Green	**xxx**	**xxx**	**xxx**	**xxx**	**xxx**	**xxx**
Mary Sorana	**xxx**	**xxx**	**xxx**	**xxx**	**xxx**	**xxx**
Tony Xin	**xxx**	**xxx**	**xxx**	**xxx**	**xxx**	**xxx**

Basic Disaster Supplies Kit

1. Additional Items to Consider Adding to an Emergency Supply Kit___.
2. Prescription medications and glasses ___.
3. Infant formula and diapers ___.
4. Pet food, water, and supplies for your pet ___.
5. Important family documents such as copies of insurance policies, identification, and bank account records in a portable waterproof container ___.
6. Cash and change ___.
7. Emergency reference material such as a first aid book or information from www.ready.gov Sleeping bag or warm blanket for each person. Consider additional bedding if you live in a cold-weather climate ___.
8. Complete change of clothing including a long-sleeved shirt, long pants, and sturdy shoes. Consider additional clothing if you live in a cold-weather climate ___.
9. Fire Extinguisher ___.
10. Matches in a waterproof container ___.
11. Feminine supplies, personal hygiene items, and hand sanitizer ___.

12. Insurance Considerations

1. Do you have coverage for a flood?

No, Unnecessary given the company's geographical location

2. **If you are located near the coast or a river, is "storm surge" classified as "flood" or as "windstorm"?**

The coverage for a flood may be different than the coverage for a hurricane. In most cases, the storm surge that spawns as a result of a hurricane is classified as a "flood"; in more cases, it is classified as a "windstorm."

3. **Do you have coverage for Business Interruption?**

Yes, Foodmood is fully covered if a business interruption occurs. This is a very important coverage that we have at FoodMood because we are a technology company that relies on the internet.

4. Do you have coverage for Service Interruption?

Service interruption is always a consideration. We are a technological company that some people are targeting to strictly limit or deny service to our potential users or in an effort to stop the potential profitability of the company.

5. Are the limits under your policy sufficient?

There are reasonable limits to our insurance for service interruption, we get 48 hours of coverage before we are officially financially responsible for all thats lost during the outage.

6. What is the deductible under your policy for windstorms or flood?

Our insurance policy covers a single dollar deductible (e.g. $30,000 per occurrence) for losses. Be sure to check our current deductible when available.

7. If you have any key customers or suppliers, do you have Contingent Business Interruption coverage?

FoodMood Business Continuity Plan CONFIDENTIAL Document for Internal Use Only What would the impact on your business be if one of your key suppliers or customers is impacted by a significant incident, such as a hurricane, a fire, or an explosion? If a significant portion of your revenue is dependent upon a key supplier or a key customer, you should consider Contingent Business Interruption coverage.

8. Do you have any assets that have a long lead time and may take significant time to replace should a loss occur?

All of our assets are media-based and backed up onto information-holding devices in multiple locations across the united states.

9. If you have more than one location, have you considered how an incident at one location will impact the other location?

For some businesses, a significant loss at one location can result in additional losses to another location due to interdependencies. For other businesses, if one location suffers a loss, another location can help to mitigate the loss by shifting employees and other resources. It can be very helpful to think through how a catastrophic loss at one location can impact other locations.

Contact your insurance agent or broker to discuss these and other questions about your business insurance coverage and needs.

Refrences

Essential tools and resources for Business Continuity Planning. (2021). *Business Continuity Planning*, 179–180. https://doi.org/10.1016/b978-0-12-813844-1.09995-4

Incident response guidelines. (2015). *Business Continuity Management*, 201–283. https://doi.org/10.1002/9781119202929.ch5

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data Breach Management: An integrated risk model. *Information &amp; Management*, *58*(1), 103392. https://doi.org/10.1016/j.im.2020.103392

Rise of the chief intelligence officer (CINO). Anomali. (n.d.). https://www.anomali.com/blog/rise-of-the-chief-intelligence-officer-cino

Scarfone, K. A., Grance, T., & Masone, K. (2008). *Computer Security Incident Handling Guide*. https://doi.org/10.6028/nist.sp.800-61r1

Settanni, G., Skopik, F., Shovgenya, Y., & Fiedler, R. (2016). A collaborative analysis system for Cross-organization Cyber Incident Handling. *Proceedings of the 2nd International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0005688301050116