Jesse Enriquez

M.S Project

Business Continuity Plan Phase Three

Part One: Issue Specific security Policies

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 BOYD's 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 are 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
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 Dockens Assistant Director: Jerry Terrosain
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
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
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 The Organization's Position	Unofficial software can severely impact the company infrastructure. 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

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.

Part Two: Legal Standard Operating Policy and 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 of 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.

Part Three: Incident Response Plan

https://www.egnyte.com/blog/post/8-essential-elements-for-an-incident-response-plan

Adverse Event	**Ransomware attack on one PC/user, Power failure, or ISP failure**
Mission Statement	**"To share and create moments with food around the world"**
Formal Documentation of Roles and Responsibilities	**Computer Emergency Response Team (CERT):** Quickly deploy as a unit and begin a pre-established plan for a given situation. This should include a step-by-step process that must be executed efficiently. **Company Legal Team:** Be accessible for any immediate questioning barring a potential private information leak via a ransomware attack. **Public Relations Team:** Prepare a statement that informs faculty of the severity of the situation and remind them if they are a part of an emergency team. Prepare statements for users so they can be informed of the state of their information and the application. **Executive Management:** Prepare to lead and answer any difficult questions asked by other leaders.

	Have the final say in any matters that are company-altering.
Cyberthreat Preparation Document	Given the strength and connections our security team has, we will not make any initial ransomware payments. Our team and staff go through cybersecurity awareness training and practice the “See Something Say Something” logic. When classifying the severity of the event, please refer to the incident classification form where more detail will be found.
Incident Detection Documentation	Detection is key and identification is key when incidents are active. Our main intrusion systems are our IDS and IPS. These must be referred to when checking what exactly is occurring. We must also have log managers check the logs for any unapproved access or changes. If nothing is found, it must be a basic power outage or ISP failure. If escalation builds, this is where we refer to our cyber threat document mentioned above and we follow the exact steps for the given threat vector.
Incident Response Threshold Determination	*Criteria For said Adverse Events* Ransomware attack: Attack that locks our system or prevents our use of vital machines and programs. Said Attack also requires some kind of service or fee by an attacker to enable our services to be reestablished Power Failure: Electricity is fully non-existent on the floor or floors of the facility. No devices are operational and all active operations are halted. ISP Failure: Internet Connection is non-existent in parts or the entire facility. Operations that rely on an internet connection are non-operational and service can not be provided via the internet.
Management & Containment processes	Multiple steps must be taken to enable the containment process. The process includes unplugging any impacted machines from your surrounding area, Isolate all systems, objects, and applications that have been in contact with the event, Set up a meeting space where information and updates and be received and updated, Gather and interviewing all impacted teams, Deploy CERT team and begin initial mitigation process, Decide if the business continuity plan needs to be deployed for the said situation, put mitigation strategies and ideas into place.
Fast, Effective Recovery Plans	● Test compromised systems multiple times before re-enabling ● Bring back systems online safely as quickly as possible ● Announced the closure of active incident ● Contact technical writers and document the events and the procedures that were executed
Post Incident Review	● Run a post-incident evaluation to determine the entry of the attack ● Update/Patch infected systems ● Bloc all suspicious activity and URLs ● Incorporate any feedback was given during response process that

	would enable a more effective deployment ● Apply all lessons from the incident to current infrastructure

<u>*If a disaster renders the current business location unusable for an extended length (with no alternate site):</u>

Works Cited

8 essential elements for an incident response plan. Egnyte Blog. (n.d.). Retrieved October 14, 2022, from https://www.egnyte.com/blog/post/8-essential-elements-for-an-incident-response-plan

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-61r2

Disaster Recovery Guide & Tips | the Hartford. (n.d.). Retrieved October 20, 2022, from https://www.thehartford.com/claims/business-disaster-recovery-guide

Keary, T. (2022, May 7). *The Colonial Pipeline Ransomware attack a year on: 5 lessons for security teams*. VentureBeat. Retrieved October 16, 2022, from https://venturebeat.com/security/colonial-pipeline-ransomware-attack/

Rose, S. (2021). Developing cyber resilient systems. https://doi.org/10.6028/nist.sp.800-160v2r1-draft

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency planning guide for federal information systems. https://doi.org/10.6028/nist.sp.800-34r1