**SECURITY PLAN PROPOSAL – We Deliver Logistics**

 **Student Name:** Abhishek Devulapalli

 **Professor:** Dr Jerome Olorunmaiye

 **Course:** Bus Cont Planning & Disaster Recovery Planning (ISOL-632-10)

 **Date: 03/15/2020**

Table of Contents

[Chapter 1: 3](#_Toc37583934)

[Purpose Of The Plan: 3](#_Toc37583935)

[Area Of Security: 3](#_Toc37583936)

[Control Measures/ Security Procedures: 3](#_Toc37583937)

[Exterior lighting: 3](#_Toc37583938)

[CCTV Cameras: 3](#_Toc37583939)

[Access criteria: 4](#_Toc37583940)

[Fencing: 4](#_Toc37583941)

[Site Maps: 4](#_Toc37583942)

[Chapter 2: 5](#_Toc37583943)

[Process Involved in Assembling a Recovery Plan 5](#_Toc37583944)

[Laying groundwork: 5](#_Toc37583945)

[Develop Departmental Plans: 5](#_Toc37583946)

[Combining Departmental Plans with overall Corporate Plan: 6](#_Toc37583947)

[Chapter 3: 7](#_Toc37583948)

[Emergency Operation Plan and Crisis Management Plan: 7](#_Toc37583949)

[Chapter 4: 8](#_Toc37583950)

[Significance of Policies and Procedures: 8](#_Toc37583951)

[Impact of Policies and Procedures: 8](#_Toc37583952)

[Steps of Building a Policy: 9](#_Toc37583953)

[Chapter 5: 9](#_Toc37583954)

[Layers of Security: 9](#_Toc37583955)

[References: 11](#_Toc37583956)

# Chapter 1:

## Purpose Of The Plan:

“We Deliver Logistics” is a newly established company which has partnered with Amazon to help fill the gap of Amazon’s delivery needs, as security administrator for this company I am going to come up with security plan. The use of a security plan is to align and stating the safety measures over the company’s assets (Lincle, 2015). If it contains an overview of the security program. It will help in enhancing and maintaining the security of the company through assessment and incorporation of the current security programs. The company has many assets, including personal and public data. These kinds of assets need security, as they are private for the company. Exposing this kind of information to anyone outside the company is inappropriate.

## Area Of Security:

Some places and spaces need security around a company. These areas hold sensitive information and hence are very critical. The risks posed to such regions are physical threats such as theft, damage, and arson. Computer security threats include spams on computers and viruses. Information threats also a problem to the private data held by the company and inherent risks that can lead to loss of delicate info such as earthquakes. The significant offices, stores, entry points, and the reception areas are among the areas that require enhanced security.

## Control Measures/ Security Procedures:

Control measures and security procedures involve the actions the company will take to reduce exposure to the company’s assets (Hulse, 2017).

### Exterior lighting:

Lighting the area strategically throughout the premises will help in highlighting perimeters, main gates, guard post points, entry points, and exit points in buildings. The installed lights activation is by motion or movement. The lighting will assist in monitoring movement in the area and the CCTV systems.

### CCTV Cameras:

The company will have CCTV cameras mounted on most of the sensitive areas. They will also be on the exterior places of interest. Through a fiber optic program, signals recorded 24/7 of the cameras reach the headquarters for monitoring. Observing frequent maintenance of the cameras and the CCTV systems will enhance the workability and reliability of the system.

### Access criteria:

This will involve the access of those authorized, for example, unit personnel, visitors, maintenance personnel, contractors, guards, and emergency response teams such as the police and medical services providers. The established permission control program will help in monitoring those who access the company. Issuing keycards with security passwords to the members will limit outsiders from getting to the premises. Coded name tags and badges with an identified area of work and inscribed photo of the owner will assist in identifying the members too. For the visitors, presenting an invitation or an appointment card will act as access for them. The same case will apply for the contractors and the maintenance personnel.

### Fencing:

Putting a wall around the premises will keep away intruders. Accessing the company becomes a challenge, and to receives services from the company following the proper protocol of entry becomes necessary. Imputing electronic barbed wires is an option to keep away those not authorized to be on the premises.

### Site Maps:

The area maps will highlight the restricted areas and rooms. It will indicate the control measures in the areas. This can be electronically accessed points and guard posts. The site maps will only be for the employees for the company as they can offer crucial information to someone to break into the company.

# Chapter 2:

## Process Involved in Assembling a Recovery Plan

The method of developing and assembling a recovery plan starts with the documentation of the project in writing before implementing it in real life. It is merely a representation of what is to be done in the case when a disaster strike. When writing the plan, there are necessary steps that are followed to bring out an excellent outlook of the project, lay the background, develop departmental strategies and combine your departmental plans into an overall corporate plan (Mallery, 2015). This paper will put more emphasis on the mentioned steps and elaborate on how each one of the steps contributes towards the achievement of a disaster recovery plan.

### Laying groundwork:

In the laying of the groundwork, necessary decisions are usually made in this step. The decisions made are effect to the following; who will execute the plan? This guideline indicates that one should consider who to call in the case where an emergency happens, and you are not available. One should also find how obvious a particular problem is. This comes along with the introduction of detection devices for damages such as earthquakes. The plan should consider the number of warnings issued in the case where an inevitable disaster is expected, for instance, an incoming storm or floods. The project should also entail enough information that will hold or control the problem before help arrives.

In laying the groundwork, one should ask themselves; how soon must the process be restored? This is recognized as a "recovery time objective." The laid foundation should also outline other manual actions that can be implemented before the procedure is restored. The groundwork also should show precisely what has to have its plan. Some processes in a company when distorted bring about damage to a significant percentage of the entire company. They, therefore, require their unique project that will be used in their recovery. The word processing and documentation format are essential to be determined when laying the groundwork to have a presentable outlook of the plan hence easy to follow even by a different party.

### Develop Departmental Plans:

The departmental plan is the other basic guideline to follow in the process of assembling a disaster recovery plan. It involves the project itself, a post that entails the assets engaged in the department, the threats brought to the department's attention, the mitigation factors, and the steps to take with the occurrence of the disaster (Wallace & Weber, 2017). The departmental plan has three key components that include; immediate actions, well-explained containment actions, and the recovery actions to be taken. The elements should be incorporated with other factors to ensure the effectiveness of the disaster recovery plan.

The other factors to put into considerations are; the foundation documents of the company, which entails the asset list, risk assessment, critical process matrix, and essential process breakdown matrix. The other factor is the recall list of all the employees, list of the companies' vendors, processes whose workaround is manual, and also possible relocation activities that might be expected. The disaster recovery plan should simply contain enough information that will enable one to restore the function ability of the company to the acceptable minimum standard.

### Combining Departmental Plans with overall Corporate Plan:

In conclusion, writing a business recovery plan is always considered a big project, but it can somewhat be divided or broken down into small, more straightforward projects. Plans can be developed starting with the low departmental levels, which can, later on, be incorporated together to have a whole plan of the business. The program should be subject to amendment as risks and disasters strike at unknown levels; hence the frequent updating of the project is highly recommended. Again, this practice of changing the plan ensures or covers the ongoing growing business enterprise. All parts of the company are subjected to a recovery plan at all times if the practice is implemented.

# Chapter 3:

## Emergency Operation Plan and Crisis Management Plan:

In the case mentioned above, the main focus is on the creation of a security plan for the We Deliver Logistics Company. When it comes to the creation of such a plan, it is essential to consider the elements of the inclusion of the right activities and resources which in turn would promote the operations of the target firm from a security dimension. Two of the most common approaches that are used in the creation of a high-level security plan include emergency operations and crisis management. These two plans and strategies contain diverse activities which in turn help to create a platform for the achievement of the desired levels of the outcome. The primary reason for the creation of an emergency operations plan is to provide a platform for response and recovery of an organization from a given incident which happened in the workplace.

The primary elements contained in an emergency operations plan include communications, safety and security, utilities, clinical support tasks, staff roles and responsibilities and but not limited to the resources and assets. These elements play a crucial role in creating a reliable emergency operations plan for a given entity (Gouveia et al. 2017). This plan, however, is made up of a series of activities which are grouped into significant phases. The first phase is planning as well as preparations. This phase involves data gathering about the incidents in the context while at the same time promoting timely ordering of events. This stage is essential since it helps to create a high-level plan about responding and mitigating the effects of the occurred incidents. The next phase is the incident management. This phase introduces the elements of the best approaches to respond to a given incident. The main activities include the creation of a planning team, analysis of the capacities and risks, the creation of a plan and the implementation process.

From another dimension, a crisis management plan acts as a tool which is used in the creation of a platform for responding to the events that if they occur would bring about a negative effect on the operations of a company. Some of the most common activities that are involved in crisis management planning include a risk assessment. This process helps in the determination of the main risks that may arise in the course of operations which marks the first step in crisis management. The second activity includes the analysis of the potential impacts as far as the business operations are concerned (Eslamian, Khosravi, Sayahi & Haeri-Hamedani, 2017). There may exist numerous strategies which would be used to mitigate the effects witnessed in this context. It is essential to identify such alternatives to promote better outcomes. The third significant activity is the creation of the desired plan. This activity involves the building of the desired plan to support the underlying intentions. The last stage is sensitizing the users and the major stakeholders about the plan. This stage is essential because it helps to create awareness about the plan which promotes compliance.

# Chapter 4:

## Significance of Policies and Procedures:

In We Deliver Logistics, the need to have adequate policies and procedures cannot be understated. Firstly, it will ensure that there no inconsistencies in the process of executing the assigned mandate. In this instance, employees at We Deliver Logistics will know what to do in different work situations. As well, the policies and procedures will spell out the consequences of work behavior among the employees. Secondly, it will ensure that We Deliver Logistics is protected from legal suits and instances of employee fraud. Notably, in the case the company has taken disciplinary actions, the procedures and policies will be vital defending its stand (Wallace & Webber, 2004). So, in the instance the employee sues, the policies and procedures will be the defense.

Thirdly, the policies and procedures can be used as a tool for training new employees at We Deliver Logistics. In the situation the company has hired new staff members they will know where they fit in the organizational structure. Also, the employees will know where to go if they have any questions or concerns. Fourthly, employees at We Deliver Logistics will know of the constraints that are associated with their jobs without having to use the “trial and error” method, which is not cost-effective. Lastly, by having set policies and procedures, it will help the managers at the firm to exercise control instead of micro-managing the employees. Notably, micro-management leads to conflicts and is associated with a lot of time wastage.

## Impact of Policies and Procedures:

The business continuity planning policy is designed to ensure that the organization is resilient in the face of different challenges and also to ascertain that there is proper management of risk. Therefore, the policies and procedures will play a vital role in ensuring that the firm’s continuity policy is effective. Consequently, it will lead to a significant impact on the manner the company operates. To start with, they will lead to better employee performance, given that they will be used as a measuring tool in the organization.

Also, the procedures and policies will provide a guide that will be used in the process of making decisions, especially in disaster situations. In such cases, an employee will know what he or she is supposed to do and when to consult the upper management in the organization. In that way, We Deliver Logistics is not affected by the disaster negatively. Additionally, they will improve the process of communication in the firm (Tinti, Venelli-Costa, Vieira, & Cappellozza, 2017). For instance, there will be ease in the process of communicating critical information to the new workers, and hence they will not make mistakes that affect business continuity. As well, with improved communication, it implies that the occurrence of conflicts due to miscommunication will be avoided. Therefore, different processes at We Deliver Logistics will run seamlessly, and that will make the organization more resilient.

## Steps of Building a Policy:

At We Deliver Logistics, the process of building proper policies for business continuity will be composed of five steps. The first one is determining the objectives of the policy. In other words, what does the policy want to achieve? The second step will be to figure out how the objectives will be achieved. In this step, it will involve coming up with many options that are viable and can be used to actualize the objectives. Thirdly, it is assessing all the options that have been identified in the previous step and then choosing the best one. At We Deliver Logistics, this step will be achieved by taking a vote to ensure that every person feels heard in the decision-making process. The fourth step is publicizing the policy in the organization and then implementing it in line with the organizational structure that exists. Lastly, it will be the evaluation of the policy after implementation to identify is there is a need for any alteration.

# Chapter 5:

## Layers of Security:

In the case of We Deliver logistics defense in depth will provide the best way through which valuable information and data can be protected. Notably, defense in depth will encompass having many layers of protection which will ensure that an intruder does not get through. The main advantage that is associated with defense in depth is that data is protected from many angles, and there are limited vulnerabilities (Aydos, Vural, & Tekerek, 2019).

There are different layers of security that will be instituted by We Deliver Logistics, each with its types of defense. To start with, it is the internet gateway which can be termed to be the connection of We Deliver logistics to the outside world (Wallace & Webber, 2004, p.335). An example of security measures that will be used in this instance is a firewall. Such a measure will restrict the flow of traffic to the network system according to rules that have been defined by We Deliver logistics. So, in the case, a specific type of data is considered to be malicious; it will be blocked by the firewall.

The second layer of security will deal with emails, print, and application servers (Wallace & Webber, 2004, p.335). In this situation, it will ascertain that messages which have been sent through emails do not harm the computer system at the firm. An example of a protection that will be used in this case is email filtering. It will involve sorting out of all the emails into different categories to identify those that are malicious. As well, there will be the installation of an antivirus program which will ensure that all of the emails are safe, and they do not harm the entire system of We Deliver logistics. Also, the antivirus program will be tasked with ensuring that the servers at We Deliver logistics are safe. Notably, for an antivirus program, it will have to be updated regularly so that it can deal with the most recent threats.

As for the third layer it will deal with the notebook personal computers (PCs) and standard desktop which are connected to the different servers at We Deliver logistics (Wallace & Webber, 2004, p.335). The security measure that will be implemented in this instance is the end-user protection. Consequently, it will ensure all the technological devices that are connected to the server are not used as the entry point for an attack on the We Deliver logistics system. Apart from the end-user protection, all the notebook personal computers and standard desktops will have antivirus protection installed to prevent any form of attack.

The last layer will consist of all the devices in the organization that share data, for example, standard PCs and mobile devices (Wallace & Webber, 2004, p.335). In this instance, different forms of data protection will be instituted to ensure that the process of sharing information is safe, and there are no breaches. Given that, an example of a protection that will be implemented is data encryption. Using this method, when attacks happen, all data in the We Deliver logistics system will be rendered to be unreadable and hence the hacker cannot exploit it at the expense of the company.

All the layers above mean that We Deliver logistics information is secure and protected from every corner. As well, such security measures will ascertain that We Deliver logistics does not have to incur considerable costs in the process of restoring normal operations after an attack happens. In the end, We Deliver logistics will be able to execute its functions without having to worry about cyber-attacks.

#

# References:

Hulse, S. A. (2017). *Control measures: If you've lost control, it's time to get it back*. Gold Rush Publishing.

Lincke, S (2015). *Security planning: An applied approach*. Cham: Springer.

Mallery, M. (2015). Technology Disaster Response and Recovery Planning: A LITA Guide.

Wallace, M., Weber, L. (2017). The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets. AMACOM

Eslamian, S., Khosravi, B., Sayahi, M., & Haeri-Hamedani, M. (2017). Crisis Management Planning and Drought Management Plans. In Handbook of Drought and Water Scarcity (pp. 293-305). CRC Press.

Gouveia, J., Gouveia, C., Rodrigues, J., Bessa, R., Madureira, A. G., Pinto, R., ... & Lopes, J. P. (2017, June). Microgrid energy balance management for emergency operation. In 2017 IEEE Manchester PowerTech (pp. 1-6). IEEE.

Tinti, J., Venelli-Costa, L., Vieira, A., & Cappellozza, A. (2017). The impact of human resources policies and practices on organizational citizenship behaviours. Brazilian Business Review, 14(6), 636-653. doi:10.15728/bbr.2017.14.6.6

Aydos, M., Vural, Y., & Tekerek, A. (2019). Assessing risks and threats with layered approach to Internet of things security. Measurement and Control, 52(5-6), 338-353. doi:10.1177/0020294019837991