[2-2 Final Project Milestone One: The Executive Brief](https://bb.snhu.edu/webapps/assignment/uploadAssignment?content_id=_16810839_1&course_id=_125052_1&assign_group_id=&mode=view)

Name

IT-385

Professor: Christopher Doolin

Southern New Hampshire University

July 16, 2017

**Executive Brief**

This executive brief is to explain the process of the new security features that will replace our current security platform and system. The reasoning behind our change in security is to protect our customers and data within our system and to prevent security threats. This brief will contain the aspects of what all employees will be trained on, how the content will affect the needs of end users at various levels of technical proficiency. The manual will be all-inclusive and understandably systematized. Lastly, we will be revising an exemplar to demonstrate the training layout and provision method suitable for the target audiences.

**Key Features**

The key features that will be included in the standard training consist of weekly backups, informing on different phishing attempts and terminology of security threats, how to report the phishing attempts, the importance of strong passwords, and limited administrative options.

* Weekly backups will be conducted on the system to ensure there will be no data loss in the event of an attack or a natural disaster. The purpose of weekly backups is to ensure there is a reliable method for recovering data. Without weekly backups, there is a possibility that a loss of data can occur which would end in a terrible outcome for the company. (Keegan, 2013)
* Employees will be informed on the different phishing attempts and the terminology used to describe particular security threats. The terminology that will be defined and explained are Data Loss Prevention, Phishing, Social Engineering and Limited/Privileged Access. (Group, 2014)
* Employees will be trained on how to spot any security threats and how to report them. It is imperative that when a phishing attempt is first detected it should be reported right away, as we will have a dedicated team to block attempts made through email and also notifying employees on an alerting message to avoid any miscommunications with clicking on a mysterious link by mistake.
* Employees will be required to change passwords quarterly and will not be able to use the same passwords. It is important to change passwords frequently as this will limit data breaches and will be a better means of security on all levels.
* Limited administrative options on the computer will be in force as there will be a specific team that will handle all network issues that may arise. If there is a matter with a particular computer, the user must report to management and consult with the IT team as well.

**Users at Various Levels of Technical Expertise**

With the new security features that will be in force, it is important to have everyone on the same page. There may be employees who are more technical and knowledgeable in the areas of cyber security and others not so. Therefore, within the training manual, all users will fully understand what cyber security is and how to avoid threats to keep all of the data and information secure. Without proper training and knowledge on the safety, a person can put the company at risk. (Group, 2014) We want the process to be a smooth transition and a comfortable learning experience for all employees. This brief is designed to relate to different levels of experience to ensure that everyone and everything are protected and secured.

**Format and Delivery Method**

The method will be used in this training process will be Instructor led training as well as using interactive methods to keep all employees engaged and attentive. The advantages of having instructor led training with interactive methods include:

* It is personable
* Everyone will be involved, and questions will be answered in classroom setting
* Storytelling
* Group discussions and participations
* Case Studies
* Quizzes
* Demonstrations

The format and delivery method used in training will be great in ensuring that everyone is involved and understands the processes (training today, 2016)

Conclusion

In conclusion, we want all employees to be knowledgeable and understand the process of cyber security and how important it is on all levels of experience. With the proper training, everyone will be able to protect the data and information of the company to allow a smooth transition of the new security features.

# Works Cited

(2016). Retrieved from trainingtoday: http://trainingtoday.blr.com/article/most-effective-training-techniques/

Group, S. A. (2014, October). *PCI Data Security Standard (PCI DSS).* Retrieved from www.pcisecuritystandards.org: https://www.pcisecuritystandards.org/documents/PCI\_DSS\_V1.0\_Best\_Practices\_for\_Implementing\_Security\_Awareness\_Program.pdf

Keegan, C. (2013, July). *The importance of backup policies*. Retrieved from www.techtarget.com: http://searchdatabackup.techtarget.com/tip/The-importance-of-backup-policies